EUROPEAN PARLIAMENT

Mass Surveillance

Part 2 - Technology Foresight

ANNEX

Science and Technology Options Assessment

EPRS | European Parliamentary Research Service

Scientific Foresight (STOA) Unit

PE 527.410

Mass Surveillance

What are the risks for the citizens and the opportunities for the European Information Society? What are the possible mitigation strategies?

Part 2 – Technology foresight, options for longer term security and privacy improvements

Annex

IP/G/STOA/FWC-2013-1/LOT 4/SC1

January 2015

PE 527.410

The STOA project "Mass surveillance – Part 2: Technology foresight, options for longer term security and privacy improvements' was carried out by Capgemini Consulting, part of Capgemini Netherlands BV.

AUTHORS

M. van den Berg
P. de Graaf
P.O. Kwant
T. Slewe

The authors acknowledge and would like to thank the following experts for their contributions to this report: *Mr. Axel Arnbak, University of Amsterdam (NL), Mr. Brent Bilger, Vice-President Solutions Architecture at Vidder (USA), Mr. Caspar Bowden, independent privacy researcher (UK), Dr. Christian Doerr, University of Delft (NL), Mr. Rickey Gevers, forensic investigator at Digital Investigations (NL), Ms. Monika Maglione, Mr. Michael Palmer and Ms. Cecilia-Joanna Verkleij (EC-DG Home), Mr. Gopal Padinjaruveetil, Chief Security and Compliance Architect Capgemini US (USA) Mr. Rejo Zenger and mr. Hans de Zwart, Bits of Freedom (NL).*
Also we relied on the insights of the Capgemini Cyber Security Community of Practice, in particular: *Mr. Jule Hintzbergen, Mr. Cees de Kuijer, Mr. Guido Voorendt, Mr. Jan Willem de Vries and Mr. Jack van 't Wout.*

STOA RESEARCH ADMINISTRATOR

Peter Ide-Kostic
Scientific Foresight Unit
Directorate for Impact Assessment and European Added Value
Directorate-General for Parliamentary Research Services
European Parliament, Rue Wiertz 60, B-1047 Brussels
E-mail: peter.ide-kostic@ep.europa.eu

LINGUISTIC VERSION

Original: EN

ABOUT THE PUBLISHER

To contact STOA or to subscribe to its newsletter please write to: STOA@ep.europa.eu
This document is available on the Internet at: http://www.ep.europa.eu/stoa/

Manuscript completed in January 2015
Brussels, © European Union, 2015

DISCLAIMER

The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. It is addressed to the Members and staff of the EP for their parliamentary work. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

PE 527.410
ISBN 978-92-823-5538-1
DOI 10.2861/984037
CAT QA-06-14-229-EN-N

Abstract

This document contains the Annex to the Study on Mass Surveillance, commissioned by the STOA Office of the European Parliament. This Annex contains detailed information on the four subthemes defined in the invitation to tender.

The motivation for providing this Annex separate to the Study is to provide the reader with a means to delve deeper into relevant information concerning the questions posed in the tender of the Study.

TABLE OF CONTENTS

Theme 1: Technological initiatives to redesign the Internet

This theme contains several subjects concerning improving the Internet as it is in order to decrease the risks for privacy and security attached to illegitimate mass surveillance. Topics covered are redesign of HTTP, programs like CRASH and PROCEED, the Internet as corporate network, anonymization techniques and technology prospects in encryption.

1. Redesign HTTP

This annex pursues to answer the following questions:

"What is the legitimacy and credibility of initiatives taken by the Internet Engineering Task Force (IETF) to redesign HTTP and other Internet protocols to enforce encryption by default for all communications and hence attempt to solve hampering technical interoperability issues of today? What are the risks of backdoors in the new designs? What are the technical drawbacks of using systematic encryption for all communication, in terms of processing power but also caching & buffering issues over data transport networks?"

1.1. Introduction

One of the main ways to secure internet communications is to encrypt all traffic, preferably by default, to improve usability and prevent insecure communications by manipulating settings. To facilitate this on the Internet, some protocols must be redesigned. In the past IPv6 and DNSSEC have been designed to increase security.

The Internet Engineering Task Force (IETF) is the forum in which network operators, hardware and software implementers and researchers discuss future protocols and standards to improve the technical working of the Internet. It is the forum where basic standards like HTTP, email and IP are set and maintained. One of the most important redesign projects currently done is HTTP2 (Hypertext Transfer Protocol).[1]

1.2. Goals of HTTP2

The goals of HTTP2 are to make HTTP more robust in the face of pervasive passive monitoring (mass surveillance) and to limit the potential for active attacks. The mechanism provided should have a minimal impact upon performance and not require extensive effort to configure.

Some argue though that HTTP ought to be replaced by HTTPS always, as a solution for protecting digital data in transit on the Internet.[2]

HTTP2 does not replace HTTPS however, which is a combination of HTTP and security standards TLS/SSL. HTTPS has its drawbacks that HTTP2 tries to solve partially. HTTPS is for instance less easy to configure than HTTP and requires certificates, for which costs have to be made. Besides, advertisement networks and content delivery networks for video and other high bandwidth data providers need to get to client computers efficiently. Encryption slows down their networks (see also Annex 2).

1.3. How will HTTP2 work?

The design document on HTTP2 is work in progress, so everything said here is limited to the version studied. That said, the current document proposes to use opportunistic encryption to secure HTTP. Opportunistic encryption means that computers (clients, servers) attempt to encrypt the communication channel, but if that is not possible, have an integrated fallback to unencrypted communications. There is no need for a pre-arranged set-up between the systems communicating (unlike HTTPS for instance, which requires an authenticated certificate on the server side).

[1] IETF (2014) 'Opportunistic Encryption for HTTP URIs', draft-ietf-httpbis-http2-encryption-00, expires December 14, 2014. http://tools.ietf.org/html/draft-nottingham-http2-encryption-03 Accessed July 21st 2014

[2] Tom's Guide (2014), HTTP Must Die, Security Experts Tell Hackers, http://www.tomsguide.com/us/http-must-die,news-19188.html, Accessed July 21st 2014

Other deployments of opportunistic encryption include STARTTLS for SMTP[3] (email – upgrade plain text SMTP connections to encrypted connections) and the FreeS/WAN, Libreswan and Openswan projects.[4] Libreswan, for instance, is a free software implementation of the VPN protocol based on IPsec and the Internet Key Exchange (IKE). https://www.libreswan.org/

1.4. Advantages and disadvantages

Opportunistic encryption can prevent passive surveillance, forcing an active approach if the monitoring agent wants to keep collecting data. More potent agencies ought to be capable to do so and set up a man-in-the-middle attack, but might not want to risk the chances of detection. A man-in-the-middle attack enables the attacker to pose as the assumed end-server, meanwhile monitoring all traffic going through. Under some unauthentic encryption methods, like the Diffie-Hellman key exchange, the attack would be detected. This is not the case for all unauthenticated encryption methods though. The additional costs and loss of performance for mass surveillance on opportunistic encrypted communications are limited, according to several experts.[5]

1.5. Backdoors

A "backdoor" in computing is a method of bypassing the normal method of authentication. Backdoors are usually inserted into a program or algorithm before it is distributed widely. They are often hidden in part of the design of the program or algorithm. In cryptography, a backdoor would allow an intruder to access the encrypted information without having the correct credentials. The backdoor would either a) allow the intruder to guess the access key based on the context of the message or b) allow the intruder to present a skeleton key that will always grant him access.[6] Government agencies have been known to insert backdoors into commonly used software to enable mass surveillance. Backdoors can be built into software, hardware, or even built into the design of an algorithm.[7]

Not everyone in the HTTP Working Group is satisfied with the state of the HTTP/2 draft, and some of the criticisms run deep. Some people believe that the draft is not ready for a Last Call. The protocol allows data to be included in HTTP headers which can be exploited by malicious parties to unfairly monopolize a connection. It is argued that pushing out HTTP/2 would waste the time of numerous implementers, as well as introduce code churn that may carry unforeseen security risks.[8] With so many concerns these days about whether telecom companies can be trusted not to turn our data over to third parties that haven't been authorized, one would assume that a plan to formalize a mechanism for ISP and other "man-in-the-middle" snooping would not be proposed. But apparently the authors of IETF Internet-Draft "Explicit Trusted Proxy in HTTP/2.0" (14 Feb 2014) haven't gotten the message. What they propose for the new HTTP/2.0 protocol is nothing short of officially sanctioned snooping. The proposal expects Internet users to provide "informed consent" that they "trust" intermediate sites

[3] IETF, (2002) RFC 3207, "SMTP Service Extension for Secure SMTP over Transport LayerSecurity", http://tools.ietf.org/html/rfc3207 , Accessed July 21st 2014

[4] https://www.libreswan.org/ , Accessed July 21st 2014

[5] Mattsson, John (2014), 'Is Opportunistic Encryption the Answer? Practical Benefits And Disadvantages' STRINT Workshop Paper, https://www.w3.org/2014/strint/abstracts.html, accessed on July 31st 2014 and Caudill, Adam (2014) On Opportunistic Encryption, https://adamcaudill.com/2014/02/25/on-opportunistic-encryption/ , accessed on July 21st 2014.

[6] Stanford (undated), 'Encryption Backdoors', http://cs.stanford.edu/people/eroberts/cs201/projects/ethics-of-surveillance/tech_encryptionbackdoors.html , accessed on July 31st 2014

[7] Ars Technica (2014) 'How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer' http://arstechnica.com/security/2014/01/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/, accessed on July 31st 2014

[8] Willis, Nathan (2014), 'Should the IETF ship or skip HTTP 2.0?', http://lwn.net/Articles/600525/ , accessed on July 31st 2014

(e.g. Verizon, AT&T, etc.) to decode their encrypted data, process it in some manner for "presumably" innocent purposes, re-encrypt it, then pass the re-encrypted data along to its original destination.[9]

1.6. Technical Drawbacks

There are practical obstacles to this approach (extensive use of encryption with strong authentication), including a lack of reasonable tools and understanding of how to use the technology, plus obstacles to scaling infrastructure and services with existing technologies.[10]

1.7. Alternatives

HSTS: in 2012 HTTP2 was preceded by an earlier mechanism to improve protection of internet traffic against eavesdropping. This mechanism, HTTP Strict Transport Security (HSTS), enables web sites to 'declare' themselves only accessible via secure (HTTPS) connections and/or convert any insecure links into secure links.[11] For instance http://example.com will be modified to https://example.com. This happens before accessing the server. Or, if the security of the connection cannot be ensured due to lack of authentication, an error message is shown and access to the web site or web application is disallowed. The HSTS request is implemented in the HTTP header (just like HTTP2), but only through HTTPS. HSTS headers over HTTP are ignored.

HSTS improves privacy by enforcing secure, encrypted communications over HTTPS, but only if (strong) authentication is possible. HTTP2 takes this one step further.

HTTPS plug-ins: several browsers (eg FireFox) and web platforms (e.g. Wordpress) provide HTTPS plug-ins that support users in automatically selecting HTTPS. Such plug-ins might have an impact on performance. Just like HSTS this solution only works if authentication of the addressed server is possible. And likewise it is not really an alternative for HTTP2. It does provide a higher level of protection though, compared to manually selecting HTTPS over HTTP.

1.8. Conclusion

Opportunistic encryption like HTTP2 in the end does not stand up against active attackers but provides a higher level of protection for Internet users against (lesser capable) passive threats. It eliminates a class of attacks against low costs.

However experts fear that opportunistic encryption may lead to a false sense of security and might abstain from 'real' security, like HTTPS or other forms of strongly authenticated encryption on communication channels.

Recommendation is that this form of encryption is only used when there is at least some form of weak authentication available. Concepts of context sensitive security could also be used: less options available for users without proper encryptions. Also naming and implementation should not suggest to users a better security than it offers.[12]

[9] Weinstein, Lauren (2014), 'No, I Do not Trust You! -- One of the Most Alarming Internet Proposals I've Ever Seen', http://lauren.vortex.com/archive/001076.html, accessed on July 31st 2014

[10] Roberts, Phil (2014) 'Pervasive Internet Surveillance – The Technical Community's Response (So Far)', http://www.internetsociety.org/blog/tech-matters/2014/06/pervasive-internet-surveillance-technical-community-response-so-far , accessed on July 4, 2014

[11] IETF (2012) RFC 6797, 'HTTP Strict Transport Security (HSTS)', final, http://tools.ietf.org/html/rfc6797 , accessed on July 31st 2014

[12] Mattsson, John (2014), 'Is Opportunistic Encryption the Answer? Practical Benefits And Disadvantages' STRINT Workshop Paper, https://www.w3.org/2014/strint/abstracts.html, accessed on July 31st 2014

2. DARPA initiatives

This annex pursues to provide answers to the following questions:

"What is the legitimacy and credibility of the "Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH)" project initiated by the DARPA agency in the US?

Is the initiative related to Programming Computation on Encrypted Data (PROCEED) a solution that is credible for the future of a totally encrypted Internet without backdoors?"

2.1. Introduction

From the very start of the internet, US government-related agencies have been tied to its development. In fact, the Defense Advanced Research Projects Agency (DARPA) – in an earlier incarnation as ARPA, was the creator of the internet, by the development of the ARPANET, and more lastingly, the development of Transmission Control Protocol/Internet Protocol (TCP/IP).[13]

These agencies are still working on the forefront of developing new technologies. DARPA develops an array of research programs, oriented at developing new technologies and systems, including developing robots, satellite technology, rockets and traditional weaponry, besides information technology.

2.2. CRASH Project

The announcement for the CRASH (Clean-slate design of Resilient, Adaptive, Secure Hosts) research project was made on June 1, 2010. It was initiated by DARPA, according to the idea that all vulnerabilities are the result of a failure to enforce basic semantics, the rules that govern software language, in particular the inability to distinguish instructions from data, to recognize different types of data, and to restrict operations to those that make sense for specific data.[14] The aim of the project is to design new computer systems, in terms of both hardware architecture, software(operating system and other system software), programming languages and development environments, that are resistant to cyber-attacks, can adapt and repair after an attack as well as continue to provide services and learn from previous attacks to tackle future attacks.[15] It takes inspiration from the biological immune system, which has two parts: an innate system that responds quickly but only to a known set of pathogens and an adaptive system that is slow but can learn to recognize new adversaries. Similarly, the new systems will be able to remove existing vulnerabilities as well as adapt to and eventually get rid of future faults. If the program succeeds, it can provide avenues for new technologies to better protect government and private computers from attacks and also give them ability to self-repair the damage. The program explicitly aims to develop 'revolutionary advances in science, devices, and/or systems'. Under the program, hardware is designed that enforces semantic constraints on all operations, software that allows better access rights and operating system that are more modular.

The first results of CRASH are now coming into view of the general public. Researchers at SIFT (Smart Information Flow Technologies, a research and development consulting company specializing in

[13] Waldrop, Mitch (2008), 'DARPA and the Internet Revolution', http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2554, accessed on August 3, 2014

[14] Breaking Defense (2012) 'DARPA's CRASH Program Reinvents The Computer For Better Security', http://breakingdefense.com/2012/12/darpa-crash-program-seeks-to-reinvent-computers-for-better-secur/, accessed on August 3, 2014

[15] DARPA, landing page CRASH program, http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_(CRASH).aspx, accessed on August 3, 2014

Human Factors and Artificial Intelligence, under the CRASH program are developing FUZZBUSTER, to provide adaptive immunity against cyber-attacks.

2.3. PROCEED Project

The announcement for the Programming Computation on Encrypted Data (PROCEED) project was made on July 6, 2010. It was also initiated by DARPA, and is concerned with research on what is sometimes called the 'holy grail of cryptography': computing on encrypted data, without having to decrypt it first. At the moment, this is theoretically possible[16], but the computational time needed to do this is at the moment too great to make it practically usable.

The program plans to support research in mathematical foundations of fully homomorphic encryption (FHE), secure multiparty computation, optimized hardware and software implementation, and programming languages, algorithms and data types.[17] The goal of the project is to speed up the homomorphic encryption algorithm by a factor of 10 million - which is not an easy optimization factor to achieve. [18]

Galois (a US-based company that applies cutting edge computer science and mathematics to solve difficult technological problems) is serving as the research integrator for the PROCEED program. DARPA has awarded $5 million to Galois as initial funding for the project and it plans to invest $20 million over 5 years to contractors and academic research teams as part of PROCEED.[19]

2.4. Conclusion

CRASH and PROCEED have different aims. CRASH aims to develop new hardware and software designs and operating systems for computer systems to improve resistance to as well as learn from cyber-attacks, while PROCEED promotes research that allows computing on encrypted data. However, on a bigger level, both projects intend to improve security (of data and systems) and enhance user confidence.

Assessing the credibility and legitimacy of these initiatives provides a challenge, mainly because the results of the programs are not public yet, nor are the terms under which parts of it are awarded to companies such as Galois.

Historically, DARPA has an extensive track record with regards to delivering cutting-edge technology. In this sense, its credibility is indeed quite large. Its legitimacy in this instance is harder to asses. In essence, it can be argued that the need for data security has arisen mainly as a result of a growing need for cyber security, because of the increase in snooping by all sorts of governments. Since the DARPA programs are funded by one of these very same governments, doubts can be raised as to the conditions under which the work here will be performed. Who has access to the products delivered? Who is the end user? What will be the legal regime under which the products will operate? More openness is needed to ensure that the products delivered can be assessed by independent experts. Overall, however, DARPA has a very good reputation of delivering state-of-the art

[16] Gentry, Craig (2009), *A fully Homomorphic Encryption Scheme*, http://crypto.stanford.edu/craig/craig-thesis.pdf, accessed on August 3, 2014

[17] DARPA, landing page PROCEED program, http://www.darpa.mil/Our_Work/I2O/Programs/PROgramming_Computation_on_EncryptEd_Data_(PROCEED).aspx, accessed on August 3, 2014

[18] Armstrong, Alex (2011), 'DARPA spends $20 million on homomorphic encryption ' http://www.i-programmer.info/news/112-theory/2330-darpa-spends-20-million-on-homomorphic-encryption.html, accessed on August 3, 2014

[19] Forbes (2011) 'http://www.forbes.com/sites/andygreenberg/2011/04/06/darpa-will-spend-20-million-to-search-for-cryptos-holy-grail/

technology and the research that is done by universities and independent research facilities should be scrutinized under normal scientific standards.

With regards to the question of whether these products can contribute to a ‘totally encrypted Internet without backdoors’, it can be said that only PROCEED is aimed at encryption, and in that case only of cloud data. Under Theme 4, the research turns more in-depth towards encryption.

3. Similar initiatives to CRASH and HTTP 2.0

This annex pursues to answer the following questions:

"What similar alternative initiatives to the two mentioned above exist, especially open source ones, at the moment? Who works on what projects?
How do they all compare with each other and what are their respective advantages and disadvantages from a technological, security, economic and organisational perspectives?
What is the level of implication of the EU in these different projects?"

3.1. Related programs by DARPA

3.1.1. Mission-Oriented Resilient Clouds (MRC)

Security implications of concentrating sensitive data and computation into computing clouds have yet to be fully addressed. The Mission-oriented Resilient Clouds (MRC) program from DARPA aims to address some of these security challenges by developing technologies to detect, diagnose and respond to attacks in the cloud; effectively building a 'community health system' for the cloud. MRC also seeks technologies to enable cloud applications and infrastructure to continue functioning while under attack. It aims to use the connectivity of clouds as a defensive machanism, by sharing information about potential attacks and redirecting resources to defend the attack. To achieve these goals the program will research development of innate distributed cloud defenses, construction of shared situational awareness and dynamic trust models, and introduction of manageable and taskable diversity into an otherwise homogeneous cloud, as well as development of mission aware adaptive networking technologies. MRC also aspires to develop resource allocation and optimization techniques that orchestrate interactions between components that maximize effectiveness while accounting for potential risk from perceived threats.[20] The self-evaluating mechanisms and platforms needed for this, could be drawn from in DARPA's CRASH program (see also Annex 2).

3.1.2. High-assurance Cyber Military Systems (HACMS)

Embedded systems form a ubiquitous, networked, computing substrate that underlies much of modern technological society. Such systems range from large supervisory control and data acquisition (SCADA) systems that manage physical infrastructure to medical devices such as pacemakers and insulin pumps, to computer peripherals such as printers and routers, to communication devices such as cell phones and radios, to vehicles such as airplanes and satellites. Such devices have been networked for a variety of reasons, including the ability to conveniently access diagnostic information, perform software updates, provide innovative features, lower costs, and improve ease of use. Researchers and hackers have shown that these kinds of networked embedded systems are vulnerable to remote attack, and such attacks can cause physical damage while hiding the effects from monitors.

The goal of the HACMS program is to create technology for the construction of high-assurance cyber-physical systems, where high assurance is defined to mean functionally correct and satisfying appropriate safety and security properties. Achieving this goal requires a fundamentally different approach from what the software community has taken to date. Consequently, HACMS will adopt a clean-slate, formal methods-based approach to enable semi-automated code synthesis from executable, formal specifications. In addition to generating code, HACMS seeks a synthesizer capable of producing a machine-checkable proof that the generated code satisfies functional specifications as

[20] DARPA, Landing page Mission-oriented Resilient Clouds (MRC), http://www.darpa.mil/Our_Work/I2O/Programs/Mission-oriented_Resilient_Clouds_(MRC).aspx , accessed on August 4th, 2014

well as security and safety policies. If successful, HACMS will produce a set of publicly available tools integrated into a high-assurance software workbench, which will be widely distributed for use in both the commercial and defense software sectors. HACMS intends to use these tools to (1) generate open-source, high-assurance, and operating system and control system components and (2) use these components to construct high-assurance military vehicles.[21]

3.2. Other initiatives

3.2.1. Security and Privacy Assurance Research (SPAR) Program - IARPA

SPAR is a program from the Intelligence Advanced Research Projects Activity (IARPA). The goal of the SPAR program is to develop and demonstrate practical techniques for exchanging data that protect the security and privacy interests of each party. For example, a database server must not learn what information was requested by a client, and yet still have the assurance that the client was authorized to have the information that was sent. Prototype systems will implement protocols that are demonstrably efficient and provide a range of security and privacy assurances relevant to a chosen data exchange scenario.

The data exchange scenarios that will be addressed in the SPAR program are: complex database queries, publish/subscribe systems, message queue/mailbox systems, and outsourced data storage systems. In addition, the SPAR program will explore efficient homomorphic encryption techniques to implement these data exchange patterns by evaluating the relevant functions and circuits on encrypted data.[22]

3.2.2. Global meshnet project - /r/darknetplan community

Its objective is to create a versatile, decentralized network built on secure protocols for routing traffic over private mesh or public internetworks independent of a central supporting infrastructure.[21] This project hopes to supplement the current infrastructure to create a secure, independent network that can operate under any condition including natural disaster or general failure of existing infrastructure. An Internet where every packet is cryptographically protected from source to destination against espionage and forgery, getting an IP address is as simple as generating a cryptographic key, core routers move data without a single memory look up, and denial of service is a term read about in history books. Finally, becoming an ISP is no longer confined to the telecoms, anyone can do it by running some wires or turning on a wireless device.[23]Project Meshnet is still in its alpha stages and is available for testing purposes to its users. The future aim of the project is to use a combination of hardware (called mesh islands) and software (called CJDNS) to set up a decentralized Internet. CJDNS is a routing engine which helps us communicate over the mesh network. Right now, the communication happens over the current Internet infrastructure over a network called Hyberboria (http://hyperboria.net/). The future aim of the project is to set up its own hardware across the globe through which the communication will take place.[24] The aim of Project Meshnet is to build a

[21] DARPA, Landing page High-assurance Cyber Military Systems (HACMS) http://www.darpa.mil/Our_Work/I2O/Programs/High-Assurance_Cyber_Military_Systems_(HACMS).aspx, accessed on August 4th, 2014

[22] FedBizzOps (2011), Security And Privacy Assurance Research (SPAR) Program Broad Agency Announcement (BAA) https://www.fbo.gov/index?s=opportunity&mode=form&id=c55e38dbde30cb668f687897d8f01e69&tab=core&_cview=1 , accessed on August 10 2014

[23] http://projectmeshnet.org/ , accessed on August 10 2014

[24] Infosec Institute (2012),' Defending the Internet with Project Meshnet' http://resources.infosecinstitute.com/project-meshnet/ , accessed on August 10 2014

decentralized Internet that will enable users to exchange information easily without a central authority like an ISP, which can block or filter traffic.

As such, Project Meshnet is completely open-source, so anyone can contribute as much as they would like in any area of expertise.[25] Project Meshnet was established in December 2011 by Daniel Supernault. After Supernault became aware of the increasing trend of uncertainty and lack of organization within the subreddit /r/darknetplan, which these ideas originated from, Project Meshnet was formed.[26]

3.2.3. CRYPTECH.IS Initiative - loose international collective of engineers

CRYPTECH.IS is a loose international collective of engineers trying to improve assurance and privacy on the Internet. It is funded diversely and is administratively situated outside the US. Recent revelations have called into question the integrity of some of the implementations of basic cryptographic functions and devices used to secure communications on the Internet. There are serious questions about algorithms and about implementations of those algorithms in software and particularly hardware. We are therefore embarking on development of an open hardware cryptographic engine that meets the needs of high assurance Internet infrastructure systems that rely on cryptography. The open hardware cryptographic engine will be of general use to the wider Internet community, covering needs such as secure email, web, DNS, PKIs, etc. The intent is that the resulting open hardware cryptographic engine can be built by anyone from public hardware specifications and open-source firmware. Anyone can then operate it without fees of any kind.[27]

The project is hosted by the Swedish University Network (SUNET) in collaboration with its subsidiary NORDUnet A/S that provides financial and administrative support for the project. Hosting for the project is provided by RHnet, the Icelandic Research & Education network.[28] Cryptech and the team that has been assembled could significantly help to alleviate these specific concerns by producing open-source hardware designs that can be directly used or re-implemented by others. A significant benefit of that is to provide confidence that the design and implementation is as free from potential nation-state or other interference as can be. While it may never be possible to achieve 100% confidence in that, it is definitely technically possible (though non-trivial) to do far better than we have to date – today we essentially have a choice between pure software cryptography or commercial hardware products for which it is impossible to see what's "under the hood. The Cryptech effort began in late 2013 with a small group of engineers at a side meeting at IETF 88 in Vancouver. The project has strong support from the IETF and IAB chairs but the project is not limited to IETF participation. While early use cases included IETF protocols such as RPKI and DNSSEC, there was also interest from Certificate Authorities, the TOR Project, and others. Cryptech is aimed at those processes requiring a very high degree of assurance – normally provided by purchasing a Hardware Security Module (HSM) – but in this case they will replace the closed box with an open one.[29] Cryptech's work aligns with Internet Society goals (a) to advance the work of open standards bodies such as the IETF and W3C, (b) to strengthen the Internet, (c) to limit the corrosive effects of mass surveillance, and (d) to improve privacy on the Internet. This group is developing open source tools for cryptography that are used as building blocks for Internet communications. The initial projects are an open crypto chip design and

[25] Zhang, Melody (2012), 'A Censorship-Free Alternative to the Global Internet?' https://opennet.net/blog/2012/08/censorship-free-alternative-global-internet , accessed on August 10 2014

[26] https://wiki.projectmeshnet.org/FAQ , accessed on July 4, 2014

[27] https://cryptech.is/ , accessed on July 4, 2014

[28] https://wp.cryptech.is/organization/ , accessed on July 4, 2014

[29] Lynch, Lydia (2014) 'The Black Box Paradox – How to Trust a Secret on Today's Internet', http://www.internetsociety.org/blog/tech-matters/2014/07/black-box-paradox-%E2%80%93-how-trust-secret-todays-internet , accessed on July 4, 2014

prototype(s), and an assured tool chain (basic elements such as compilers, operating systems, and hardware design tools). The intent is that the resulting open-source hardware cryptographic engine can be built by anyone from public hardware specifications and open-source firmware.[30]

3.2.4. CurveCP – Daniel Bernstein

CurveCP is similar to TCP but uses high-speed high-security elliptic-curve cryptography to protect every packet against espionage, corruption, and sabotage. The cryptographic tools used in CurveCP are the same as the cryptographic tools used in DNSCurve. CurveCP was announced at the 27th Chaos Communication Congress on 28 December 2010. The first CurveCP implementation, incorporated into the Networking and Cryptography library (NaCl), entered public alpha testing on 21 February 2011. CurveCP software isn't ready for users yet but is ready for experimentation and development by interested programmers. CurveCP was designed by Daniel J. Bernstein (University of Illinois at Chicago). Bernstein's work was funded by the US National Science Foundation, grant number 1018836, Higher-Speed Cryptography.[31]

3.3. EU Involvement in initiatives

The EU has a limited profile with regards to projects relating to clean-slate design or any other of the mentioned directions. There are examples of projects relating to the future of the Internet - for instance the Future Internet Research & Experimentation (FIRE) program[32], but these lack a specific focus on security issues. The Horizon 2020 program (an €80 billion research and innovation program), does have a section devoted to 'quantum key distribution systems and networks for long-term security by design'[33], and other sections on security and privacy. The broader aims for these programs are however sometimes in conflict with demands for security[34].

[30] Roberts, Phil (2014) 'Pervasive Internet Surveillance – The Technical Community's Response (So Far)', http://www.internetsociety.org/blog/tech-matters/2014/06/pervasive-internet-surveillance-technical-community-response-so-far , accessed on July 4, 2014

[31] http://curvecp.org/ , accessed on September 10, 2014

[32] http://cordis.europa.eu/fp7/ict/fire/, accessed October 3, 2014

[33] http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-fet_en.pdf, accessed October 3, 2014

[34] For instance, demands for platform-independent solutions can conflict with the demand to incorporate platforms in designing and evaluating security

3.4. Conclusion

There is a general misconception about cryptography, i.e. that it is secure if the key cannot be recovered without brute force within a reasonable time. This is generally not true. Many schemes have been published for breaking cryptographically protected resources by using various attack strategies, that do not depend on brute force attacks or that significantly reduce the effective key length. In addition to that several protection schemes are vulnerable to **social engineering attacks.** Cryptographic protection only is secure if all of the following conditions are met:

1. The protocol can mathematically proven to be secure against all known attack strategies;
2. The implementation of the protocol is free of errors;
3. Key management, key exchange and key initialization use mathematically secure trapdoor functions;
4. The key length is chosen such that a pseudo random key cannot be distinguished from a true random key within a lifetime even with current global computing power;
5. It can mathematically proven that the implementation cannot be distinguished from the formal scheme within a lifetime even with current global computing power.

Cryptography algorithms will always be attacked and will eventually be broken if the mentioned conditions are not met. New improved algorithms will be designed which will be harder to crack. Organizations need to be aware that they have to periodically check their algorithms and may have to replace them.

The biggest threat for algorithms is expected from quantum computing but it will take more than 5 years before this threat is imminent. The EU's role in these is limited, although several initiatives are based in EU Countries.

4. Large-scale deployment of security solutions already in use by private companies

This annex pursues to provide answers to the following questions:

"What would be the advantages and disadvantages of massively deploying on the Internet the type of security solutions already in use by private companies to secure their global private IP networks, for instance for exchange of financial transactions between banks, and other financial critical infrastructures such as clearing houses and central banks?
This includes but is not limited to:
(i) systematic use of encryption for all communications using very long "key length" using for instance RSA and VERISIGN-like technologies,
(ii) use of tamper-resistant hardware security modules (HSM) for cryptography processing, such as for instance the technologies commercialized by UTIMACO and ENTRUST,
(iii) implementation of auditable security standards and baselines,
(iv) security supervision by a central authority in combination with local national regulatory bodies."

Multinational corporations and networks of corporations (including supply chains) or institutions (including the EU itself) secure their internal digital communications over (mostly) IP networks with a varying stack of security controls. These solutions involve organization, people, processes and technology. One of the key objectives is to achieve a minimum level of trust required to collaborate within the network (identities, malware free traffic, integrity of data etc.) and with external parties.

Typically controls applied derive from a security strategy, based on a periodic risk assessment. This strategy is translated into several more specific policies, e.g. on communication channels, end point protection, identity & access management, monitoring, awareness & training, privacy et cetera. Security baselines help to reduce the effort in translating inside and outside risks into controls. A baseline sets out the basic measures that should be in place anyhow, for any data and any ICT network in the organization. Only ***high risk assets*** receive additional attention and investment.

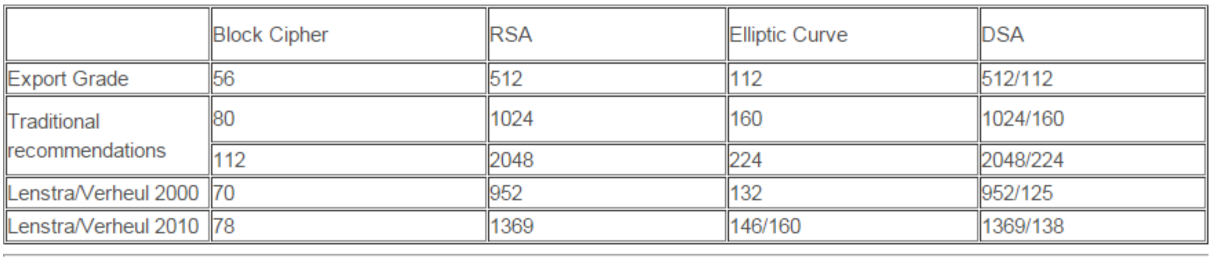
That is a trivial observation to make as security measures can be costly. In this chapter we describe several security measures that are in use for high risk processes, with the exception of security baselines. The latter is extensively explored in chapter 10.

4.1. Systematic encryption with long key lengths

Size matters?

In cryptography, key size or key length is the size measured in bits of the key used in a cryptographic algorithm. An algorithm's key length differs from its cryptographic security, which is a logarithmic measure of the fastest known computational attack on the algorithm, also measured in bits. This is always smaller than its key length. A larger key in general offers better protection against brute force attacks.

Key length is not the whole story, the algorithm is a major factor too. Symmetric and asymmetric keys provide the same level of security at different key lengths for instance. RSA considers its 1024 bits RSA key equal in strength to 80-bit symmetric keys for instance, 2048 bits RSA to 112 bit symmetric and 3072-bit RSA keys to 128-bit symmetric keys. NIST suggests that 15360-bit RSA keys are equivalent in strength to 256-bit symmetric keys. See the examples in the table below:



	Block Cipher	RSA	Elliptic Curve	DSA
Export Grade	56	512	112	512/112
Traditional recommendations	80	1024	160	1024/160
	112	2048	224	2048/224
Lenstra/Verheul 2000	70	952	132	952/125
Lenstra/Verheul 2010	78	1369	146/160	1369/138

Table 2. Minimal key lengths in bits for different grades.

Table: minimal key lengths for symmetric, asymmetric, elliptic curve and DSA[35]

The actual degree of security achieved over time varies, as more computational power and more powerful mathematical analytic methods become available. For this reason cryptologists tend to look at indicators that an algorithm or key length shows signs of potential vulnerability, to move to longer key sizes or more difficult algorithms.

However other factors determine how long a specific key is secure enough for use. This is period is called the cryptoperiod. In general short cryptoperiods are better for security. Other factors are for example:

- How the encryption mechanism is implemented;
- The operating environment (e.g., a secure limited access facility, open office environment, or publicly accessible terminal);
- The volume of information flow or the number of transactions;
- The security life of the data;
- Key management functions (like re-keying, key update processes);
- The number and distribution of copies of a key;
- Personnel turnover (e.g., CA system personnel);
- The threat factor to the information (e.g., whom the information is protected from and their resources).

Advantages and disadvantages

Basically a long key length ensures enhanced security, but at the cost of lower performance (increased decryption time). How long the key needs to be, depends on risk assessment and (perceived) benefits. High value network traffic between datacenters is for instance currently encrypted with 2048 bit RSA keys, but longer keys are in use.

But what is considered secure now, can become obsolete in a few years. Due to ever increasing computational power, key lengths have to grow too, in order to offer a sufficient level of security. Key management is therefore more than an operational activity. It requires periodic updates of all applications, devices and infrastructure components utilizing cryptokeys.

[35] RSA Laboratories, 4.1.2.1 What Key Size Should Be Used?, http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/key-size.htm, accessed November 20th 2014

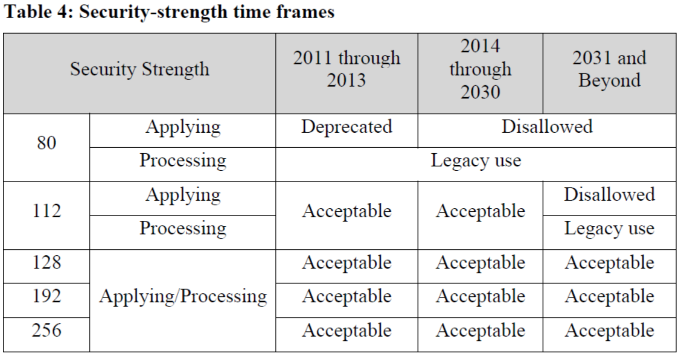


Table 4: Security-strength time frames

Security Strength		2011 through 2013	2014 through 2030	2031 and Beyond
80	Applying	Deprecated	Disallowed	
	Processing	Legacy use		
112	Applying	Acceptable	Acceptable	Disallowed
	Processing			Legacy use
128	Applying/Processing	Acceptable	Acceptable	Acceptable
192		Acceptable	Acceptable	Acceptable
256		Acceptable	Acceptable	Acceptable

Figure: example of NIST advisory to US federal government on key sizes[36]

In general, where strong cryptography is employed, other risk factors become more important to monitor, like physical, procedural, and logical access protection. Attackers may be able to access keys through penetration or subversion of a system with less expenditure of time and resources than would be required to mount and execute a cryptographic attack.[37] Also, an insiders threat can shatter the strong defences of a long cryptokey.

4.2. Tamper-resistant hardware security modules (HSM)

A Hardware Security Module (HSM) is "*a piece of hardware and associated firmware that usually attaches to the inside of a PC or server and provides at least the minimum of cryptographic functions. These functions include (but are not limited to) encryption, decryption, key generation, and hashing. The physical device offers some level of physical tamper-resistance and has a user interface and a programmable interface*." [38]These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server.[39]

HSM can also be found with names like Personal Computer Security Module (PCSM), Secure Application Module (SAM), Hardware Cryptographic Device or Cryptographic Module.

HSM are typically certified, for instance to the FIPS 140-2 Level 3 standard[40]. Organizations in financial services, defense and government have long made use of these tamper-resistant devices to secure their high risk communications.

Generally HSMs are implemented for the following uses:

- key generator and safe key storage facility for a Certificate Authority.
- tool to aid in authentication by verifying digital signatures.
- accelerator for SSL connections
- tool for securely encrypting sensitive data for storage in a relatively non secure location such as a database.
- tool for verifying the integrity of data stored in a database.
- secure key generator for smartcard production.

[36] NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General (Revision 3), 2012

[37] NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General (Revision 3), 2012

[38] SANS Institute, An Overview of Hardware Security Modules, 2002, http://www.sans.org/reading-room/whitepapers/vpns/overview-hardware-security-modules-757.

[39] http://en.wikipedia.org/wiki/Hardware_security_module

[40] NIST, FIPS PUB 140-2 - Security Requirements For Cryptographic Modules, 2001

Figure: NCipher nShield F3 Hardware Security Module in the form of a PCI card

The overall advantages of an HSM are increased security for the creation, storage and use of cryptographic keys, accelerated cryptographic performance, and an industry standardized hardware platform from which to design a suitable security set-up for an organization.

Vendors of HSM's include Thales, IBM, SafeNet, Futurex, HP, Ultra Electronics AEP and many others.

Figure: Cryptosec Banking Hardware Security Module - FIPS 140-2 Level 3 - rack mounted HSM by Ultra Electronics AEP.

Disadvantages:

The main drawback of using HSMs is cost. These devices can range in price from $500 each to $10,000 or more, depending on the level of functionality and security that is required. The cost of the device can be partially offset by reducing the need for more servers to support the increased need for cryptography. A large scale development at the level of a European Internet Subnet would still require very substantial investments.

HSMs should be tamper-resistant as one of their core functionalities. They should "zeroize" themselves (erase all sensitive data), in the event they detect physical tampering, for example, by means of physical penetration, anomalous electrical activity or anomalous temperatures. This is to prevent an adversary who has gained physical access to the card from retrieving the keys protected within. This is not always good enough: it depends on the self detection of tampering. Really secure tamperproof hardware must automatically self destruct on tampering e.g. by releasing a corrosive charge.

With the vendor documentation it is often hard to assess the true level of security, as vendors typically withhold information about how their security products work.[41] The FIPS standard is the easiest way to verify the security of a given HSM.

[41] SANS Institute, An Overview of Hardware Security Modules, 2002, http://www.sans.org/reading-room/whitepapers/vpns/overview-hardware-security-modules-757

Another disadvantage of HSMs is the difficulty in upgrading. If, for example, a weakness is exposed in a cryptographic algorithm, a new cryptographic software module can be plugged into a well-designed architecture with relative ease. This is typically not the case with HSMs. This means that even if HSM improve the efficiency of encryption in network environments, it still means that HSM lifecycle management can be labor-intensive when deployed on a European scale. Each upgrade will be a substantial but manageable effort, as long as it is clear what is where (asset management).

4.3. Implementation of auditable security standards and baselines

The subject of security baselines is addressed in this Annex in chapter 10.

4.4. Security supervision by a central authority in combination with local national regulatory bodies

Supervision on security management can currently be seen in roughly two varieties:

1. Supervision on a voluntarily basis, e.g. ISO 2700x audits to renew the company's certificate
2. Obliged supervision on a regulatory basis, e.g. in the financial sector (by national banking authorities) or in the payment industry (based on PCI-DSS).

The level of supervision can vary too: from detailed technical inspection to evaluation of the security management processes. In relation to security baselines the current practice tends more towards the higher level processes. If the security management processes function, then technical, organizational and human factor controls ought to be effective.

The scope is another dimension. The primary focus should be on the wider Critical Information Infrastructure, but in fact every organization handling personal data feeds the surveillance engine. Data Protection Authorities already have a supervisory role, which may be enforced by the coming EU Data Protection regulation.

There is no technological reason why the concept of supervision on adherence to security baselines could not work on an EU scale. That said, the scale is the issue itself in terms or organization required and administrative burden on society. Policy options can therefore range from stimulate voluntarily and market driven audits & certification to obliged supervision as part of the future NIS directive.

From our own perspective we see that more and more public and private organizations adopt security baselines and agree to some form of supervision on a semi-voluntarily basis. Either market conditions force them (to stay in business with clients who demand high security levels), or larger agreements within groups of companies or public organizations. This growth indicates that there is a basis to work on, and that regulation with forced can remain the big stick for a while.

See furthermore chapter 10 in this Annex.

5. Anonymization services

This annex pursues to provide answers to the following questions:

"Are anonymization services a good way of protecting privacy of end-users, for egovernment systems but also more generally for the protection of their meta-data? Can it be defeated?

What are examples of anonymization services and to which extent can they protect citizens, what is the future of this technology? What is the limit of what can be done?"

5.1. Introduction

Generally, anonymization makes it possible for users to surf the internet anonymously and unobservably. Without anonymization, the website that one visits, the internet service provider (ISP), or any eavesdropper on the internet connection can determine which websites the user of a specific computer visits as well as other personal data.[42]

Anonymizers act as a man in the middle while browsing the Web, handling communications between the device and the website being visited anonymously. If everything is configured well and works correctly, the target website only sees information from the anonymizing service, so it cannot identify the user's IP address or other personal information.[43]

Another way in which anonymization can be used is by the provider of certain services. Anonymity in this context means that citizens can use a service without being identified, i.e. the subject is not identifiable within a set of subjects.[44]

5.2. Examples of Anonymization Services for Users[45]

In the broadest sense, anonymization services for users can be structured according to the complexity of the tools used and the amount of encryption involved.

Tools used in anonymization:

- Simple Anonymization Proxies
- Network Address Translation (NAT)
- Virtual Private Networks (VPNs)
- Overlay-based anonymity approaches

5.2.1. Simple anonymizing proxies

Use of simple anonymizing proxies allow users to access servers without allowing information to be gathered about which servers they access and without allowing the accessed servers to gather information about the user. These proxies provide some measure of endpoint privacy, but require

[42] Homepage 'Project: AN.ON - Anonymity.Online', http://jap.inf.tu-dresden.de/index_en.html , accessed on July 4, 2014

[43] PC World (2012) 'How (and why) to surf the web in secret' http://www.pcworld.com/article/2013534/how-and-why-to-surf-the-web-in-secret.html, accessed on July 4, 2014

[44] Jacobi, Anders et al (2013) Security of eGovernment Systems, http://www.europarl.europa.eu/stoa/cms/cache/offonce/home/publications/studies;jsessionid=064C72F4A6DC5DEAC8CBE544E382B31F?reference=IPOL-JOIN_ET%282013%29513510, accessed on july 4th, 2014

[45] Mendonca, Marc et al., (2012) 'A Flexible In-Network IP Anonymization Service,' http://yuba.stanford.edu/~srini/papers/icc-sdn12.pdf , accessed on August 4, 2014

trust in the proxy. Additionally, there are overhead costs (in terms of computing power) as well as time delays.

5.2.2. Network Address Translation (NAT)

Traditional network address translation (NAT), in which individual IP addresses are channeled (or 'masqueraded') behind a router, also provides a certain degree of privacy. However, this method still allows for the public IP address to be traced back to end users, or at least ISPs. Additionally, NAT provides no privacy benefit to intranet work communication behind the NAT infrastructure.

5.2.3. Virtual Private Networks (VPNs)

Virtual Private Networks are another popular solution used to hide network identity from the opposite endpoint. A VPN extends private network settings across public networks, such as the Internet. It enables devices to send and receive data across shared or public networks as if they were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. VPNs exist both as free and paid services for individual and corporate users. While widely supported and deployed, VPNs have similar drawbacks as anonymizing proxies - the user must trust the VPN service provider and traffic must flow through the provider network, which may not be the most efficient route to the destination.

5.2.4. Overlay-based anonymity approaches

In recent years, anonymization based on overlay has seen increased popularity. Especially the Tor-network has received increased attention, due to its widespread use by users as diverse as hackers, activists, criminals and government officials seeking increased anonymity.

These overlay-based approaches include Onion routing (e.g. Tor), JonDo (which uses fixed shared routes known as cascades), and P2P-designs such as Tarzan. While they are considered "low-latency" connection-oriented approaches[46] compared to lower message-based anonymity systems, they still considerable issues with usability, in the sense that they require 'overhead' (separate installation and some amount of knowledge) and noticeable delay. This issue has, in the case of Tor, to some extent been addressed by developing the Tor Browser.

In the case of Tor specifically, there is no control over who runs the Tor servers over which private data travels. In the past, there has been ongoing suspicion that criminals and intelligence agencies exploit the Tor network in order to secretly attain information like passwords, bank accounts and credit cards. Researchers have shown in a number of cases how easily somebody can set up a spying Tor exit node to collect private information.[47]

5.3. Allowing users anonymity

Another way in which anonymization can be used is by the provider of certain services. In this way, the provider of a service only knows the specific information needed to apply a certain rule, without it being necessary for the person to reveal their complete identity. In this context, much scientific work is being done on so-called 'attribute-based' access to systems, that provides dynamic, context-aware and risk-intelligent access control. Users only reveal a certain aspect (for instance their age), in order to identify themselves to a system. In this way, users can control the way they disseminate information further. Research into attribute-based access can provide new ways to allow for access to e-

[46] Dingledine, Roger et al (2014) 'Tor: The Second-Generation Onion Router ' (draft version 1), http://www.cl.cam.ac.uk/~sjm217/papers/tor14design.pdf, accessed November 1, 2014

[47] Homepage 'Project: AN.ON - Anonymity.Online' http://anon.inf.tu-dresden.de/index_en.html, accessed on August 4, 2014

government services[48], but also for other regulatory identification procedures (for instance: proving that one is adult at liquor or cigarette shops).

5.4. Future of Anonymizing Services

Providing a usable anonymizing network on the Internet is an ongoing challenge for those interested in privacy and security of online communications.

Security and usability do not have to be at odds: As Tor's usability increases, it will attract more users, which will increase the possible sources and destinations of each communication, thus increasing security for everyone. This very development will provoke attempts to reduce the (sometimes malicious) possibilities anonymity offers. Ongoing trends in law, policy, and technology are at odds with a desire for anonymity, with the right to free speech in this case being at odds with demands for security. Increased surveillance and undermining of anonymity can however also undermine national security and critical infrastructure, by making communication among individuals, organizations, corporations, and governments more vulnerable to analysis.

Other tools have also have proven to be working and are in some places gaining in popularity.[49]

	Other examples of anonymity tools
Share	A closed source file sharing application from Japan. It is developed by an anonymous engineer, because file sharing applications are illegal in Japan. It implements a large virtual distributed hard drive.
FreeNet	One of the most used anonymous networks. Unlike Tor, it does not allow anonymous communication with the network outside FreeNet. Instead, all users contribute with their own disk space to store encrypted information for others to access. A similar system is called Entropy.
GNUnet	A system that supports direct downloading of files through anonymous tunnels similar to those used in Tor, but also supports diffusion of data as in Share.
I2P	A computer network layer that allows applications to send messages to each other pseudonymously and securely, by using end-to-end encryption.

5.5. Conclusion

The development of more and better encrypted anonymization tools has proved a breakthrough in privacy-oriented internet use in the last years. However, anonymization in and of itself will not be a sufficient way of ensuring privacy to users. Anonymization techniques namely work retrospectively: identities have probably already been exposed before and cannot be concealed completely to adversaries who have already harvested sensitive personal data in the past.[50] There are also numerous ways to enable tracing of users, and examples of this abound.

[48] Work on this is being done for instance in the Access eGov initiative, http://www.access-egov.info/, accessed on August 4, 2014

[49] Erkonnen, Henrik and Jonas Larsson (undated) 'Anonymous Networks: Onion Routing with TOR, Garlic Routing with I2P', http://www.cse.chalmers.se/~tsigas/Courses/DCDSeminar/Files/onion_routing.pdf , accessed on August 4, 2014

[50] That is, if the legal framework applicable permits harvesting, storing and processing such personal data for this purpose for a longer period.

In order for current users to regain some measure of anonymity, large-scale adoption of users and governments of anonymization tools would be needed. However, this needs to be complemented by extensive measures in the domain of identity management in order to prove effective. Even then, due to existing dissemination of harvested personal data, it would take another generation before any such scheme would take effect.

Research into anonymization is however, proving to be a fruitful means of reacting to surveillance. As usability, reliability and availability of anonymization tools increases, so could future use. But any measures to be implemented will take much more than ten years to become fully effective.

6. Latest technology prospects related to encryption

This annex pursues to answer the following questions:

"What are the latest technology prospects related to the use of elliptical-curve encryption to reduce CPU consumption, quantum-based technology to increase the quality of pseudo random number generation, homomorphic encryption to allow some processing on encrypted data? What realistic progress can be expected in the area of encryption in the next 10 years and how will it improve security of the Internet and end-user data privacy?"

Elliptical Curve Cryptography[51]

The best assured group of new public key techniques is built on the arithmetic of elliptic curves. It has been argued that elliptic curves are a foundation for future internet security, given the relative security and better performance of these algorithms. While at current security levels elliptic curves do not offer significant benefits over existing public key algorithms. Elliptic curve cryptosystems (ECC) are more computationally efficient than the first generation public key systems, RSA and Diffie-Hellman. As one scales security upwards over time to meet the evolving threat posed by eavesdroppers and hackers with access to greater computing resources, elliptic curves begin to offer dramatic savings over the old, first generation techniques.

For protecting both classified and unclassified National Security information, the National Security Agency has decided to move to elliptic curve-based public key cryptography. The United States, the UK, Canada and certain other NATO nations have all adopted some form of ECC for future systems to protect classified information throughout and between their governments.[52] ECC helps to establish equivalent security with lower computing power (battery) resource usage, and it is becoming widely used for mobile applications.[53] With all the advantages, ECC will replace the RSA in some areas, such as PDA, mobile phones, smart card applications, and become the general public key encryption algorithm. Many international organizations for standardization (government, industry, finance, business, etc.) have all kinds of elliptic curve cryptosystem, as their standardization documents issued all over the world.[54]

Researcher are optimizing the performance of ECC by reducing the cost of group operation (e.g. by using a different curve representation), reducing the number of group operations or by using special instructions. Intel has added in its processor architecture special instructions for optimizing ECC (PCLMULQDQ – PC Carry-Less Multiplication Quadword).[55]

Quantum-based technology

Researchers have devised a new kind of random number generator which is cryptographically much better, inherently private and certified random by laws of physics and it is based on quantum technology. At present, the process of random bit generation is slow, but speedups by orders of

[51] Bos, J.W. et al., Fast Cryptography in Genus 2, Microsoft Research Workshop on Elliptic Curve Cryptography, 2013. https://www.cosic.esat.kuleuven.be/ecc2013/files/joppe.pdf. Jankowski, K. et al., Intel Polynomial Multiplication Instruction and its Usage for Elliptic Curve Cryptography, 2012. http://www.intel.co.kr/content/dam/www/public/us/en/documents/white-papers/polynomial-multiplication-instructions-paper.pdf

[52] NSA (2009), http://www.nsa.gov/business/programs/elliptic_curve.shtml, accessed on August 4, 2014

[53] http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography, accessed on August 4, 2014

[54] Klanke, Dan et al (2013), 'Elliptic curves and public key cryptography', https://www.projectrhea.org/rhea/index.php/Walther453Fall13_Topic13_paper, accessed on August 4, 2014

[55] Jankowski, Krzysztof et al. (2012) 'Multiplication Instruction and its Usage for Elliptic Curve Cryptography', http://www.intel.com/content/www/us/en/intelligent-systems/wireless-infrastructure/polynomial-multiplication-instructions-paper.html, accessed on October 5, 2014

magnitude are expected in the coming years.[56] Today's (pseudo-)random-number generators which are used by encryption schemes are not truly random- their output is not verifiably unpredictable. In some cases the output of a not-truly-random generator can be encrypted with a sufficiently long key, so it cannot be distinguished from the output of a true random generator. However, quantum technology has the potential to generate completely random numbers and it is proposed that in the near future, a practical device based on this principle can be devised.[57]

Homomorphic Encryption

IBM recently claimed that one of its researchers has made it possible for computer systems to perform calculations on encrypted data without decrypting it (the idea behind fully homomorphic encryption). According to it, the breakthrough would let computer services store the encrypted (confidential) data of others and process it without knowing the content of the data., as well as many other potential applications.[58]

However, this implementation requires immense computational effort and is not practical. For example, performing a Google search with encrypted keywords would multiply the necessary computing time by around 1 trillion according to estimates.[59] According to Moore's law, it would be 40 years or more before homomorphic search would be as efficient as a simple search today, and that is also an optimistic estimate.[60]

6.1. Future of encryption

For AES (Ryndael), a 128-bit security symmetric key length should be the minimum requirement for new systems being deployed. However a key recommendation is encryption algorithms and key lengths should be periodically be evaluated. Encryption algorithms that are no longer secure enough should be phased out. In selecting key sizes the recommendations by ENISA can be used.[61]

Experts anticipate an alternative computing technology, quantum computing, that may have processing power superior to current computer technology.[62] It can still take over 10 years before this technology is mature enough. It is expected that quantum computing can be used to crack the keys for certain types of encryption schemes in the coming years.

Recommendations for coping with increased computation power and the corresponding required increased key length can be found on www.keylength.com. Note that no recommendation from an EU authority for key lengths has been found.

In the field of cloud computing, Microsoft expects to have measures in place for encrypting data in transit between customer locations and its data centers, and while in transit between its own data

[56] University of Maryland (2010) 'Random, but not by chance: A quantum random-number generator for encryption, security' www.sciencedaily.com/releases/2010/04/100414134542.htm, accessed on August 4, 2014

[57] Bienfang, Joshua (2012) 'Truly Random Numbers -- But Not by Chance', http://www.nist.gov/pml/div684/random_numbers_bell_test.cfm, accessed on August 4, 2014

[58]Computerworld (2009), 'IBM touts encryption innovation', http://www.computerworld.com/s/article/9134823/IBM_touts_encryption_innovation?taxonomyId=152&intsrc=kc_top&taxonomyName=compliance, accessed on August 4, 2014

[59] Forbes (2009) 'IBM's Blindfolded Calculator', http://www.forbes.com/forbes/2009/0713/breakthroughs-privacy-super-secret-encryption.html, accessed on August 5, 2014

[60] Schneier, Bruce (2009) 'Homomorphic Encryption Breakthrough', https://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html, accessed on August 5, 2014

[61] ENISA (2013) 'Algorithms, Key Sizes and Parameters Report', https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, accessed on August 5, 2014

[62] http://en.wikipedia.org/wiki/Quantum_computer

centers by the end of 2014. Like Google, Microsoft says it plans to encrypt all stored data in the cloud. Several other cloud services providers, like Dropbox, Sonic.net and SpiderOak, have announced support for similar data encryption programs, and for features like 2048-bit key lengths and the "*Perfect Forward Secrecy*" method for future-proofing encrypted data. Experts say such measures are vital to protecting data traveling between customer companies and cloud service providers.[63] However, without rigorous proof of the absence of backdoors, these vendor claims should be regarded with extreme skepticism.

The focus today, and for the future, will be to create new products that are far simpler and easier to use, cost less to manage, and provide a higher level of assurance that the enterprise is in compliance with government regulations and industry standards. Secure messaging and data-storage solutions should become more transparent to the end user. Nearly all the technologies needed to transparently encrypt, decrypt, sign, and verify any data object—such as an email, a video clip, or a voice transmission—are already in place today. At the same time, however, future products based on these newer application technologies will also offer a degree of user interaction—or at least enterprise-level modification—to accommodate the varied and specific security needs of particular groups of users.

So, the underlying implementations will be more sophisticated than they are today, but the user interface will be virtually transparent to most users. That is the future of encryption—enabling us to accomplish more complicated tasks with far less effort, and more securely. Products that utilize encryption technologies must be made more transparent and more effective for the end user. In doing so, these products not only become easier for end users, they also enable consistent, automatic, and enterprise-wide policy enforcement. This is where most enterprises are heading, particularly for email and data-storage protection.[64]

Within five years the math for cracking encryption algorithms could become so efficient that it may render today's commonly used RSA public key cryptography algorithm obsolete. While it might take longer, the end of RSA as an effective tool is inevitable, says Alex Stamos, CTO of the Artemis division of NCC Group. The most likely choice right now is elliptic curve cryptography which is more complex mathematically to unravel than RSA, and businesses should take immediate steps to advance an orderly shift to the stronger scheme.[53] Thus the field of encryption is continuously evolving, and many changes and improvements in security and encryption technology are expected in the next 5-10 years.

6.2. Conclusion

The encryption landscape is changing continuously. Organizations should anticipate to the advances in breaking encryption algorithms by phasing out algorithms that are no longer secure and by adopting new and secure encryption standards. The biggest disruption in cryptography is expected from quantum computing. It will take many years for an attack based on quantum computing can be successful but if it succeeds the consequences will be enormous.

[63] Computerworld (2013), 'Cloud computing 2014: Moving to a zero-trust security model', http://www.computerworld.com/s/article/9244959/Cloud_computing_2014_Moving_to_a_zero_trust_security_model, accessed on August 4, 2014

[64] Dunkelberger, Philipp (2004) 'The Future of Encryption', 'http://www.ttivanguard.com/austinreconn/encrypt.pdf, accessed on August 20, 2014

Theme 2: Feasibility of a secure “European Internet Subnet” part of the “Global Internet”

This theme focuses on the concept of Internet segmentation, creating a European Internet Subnet or otherwise. Partially this builds on the idea of secure Internet communications as in a corporate network, but also covers other options, advantages and disadvantages, cryptography at lower network levels and security baselines.

7. Advantages and Disadvantages of a Secure European Internet Subnet

This chapter provides an integrated answer on the questions 7, 8 and 11.

Question 7

What would be possible technological, security, privacy and economic advantages and disadvantages of a secure "European Internet Subnet" strategy, which would effectively amount to a secure European Internet Subnet relying on the exclusive use of "EU network infrastructures" for the transfer of "EU data" between "EU data centres" housing "EU cloud computing and social network services" operated by "security-accredited EU nationals" working for "EU Companies" that are subject to "EU Data Protection Legislation" on "EU territory"?

Question 8

What are technology orientations and high-level options that would make it possible to create a secure "European Internet Subnet" where it would be impossible for any observer to collect meta-data by tapping traffic via telecom operators, and/or using web-browser cookies and web-site trackers? How to interconnect the "European Internet Subnet" to the rest of the Internet world in a secure and interoperable way? Do we need a new Internet for that purpose? Are there potential inter-operability issues with the concept of a secure European Internet Subnet?

Question 11

Is it feasible to build and security-manage the "European Internet Subnet" in the same way a very large international company would typically manage its own large international private IP network?

What would be the advantages and disadvantages of proceeding that way?

Would it be feasible to make European Internet traffic anonymous when routed outside of the secure "European Internet Subnet" over the global Internet?

Would we need "gateways" to filter traffic between this "European Internet Subnet" and the rest of the Internet, and to detect security breaches and possible abuses originating from external "nontrusted" data networks?

In this chapter the elements of the questions 7, 8 and 11 are combined. The basic question underlying these three questions is:

How could we protect our EU internet ...on such a way..that.. it would be impossible for any observer to collect meta-data ....by tapping traffic via telecom operators, and/or using web-browser cookies and web-site trackers [or any other way]?

For descriptions of surveillance technologies we refer to Part 1 of this study.

7.1. What are technology orientations and high-level options that would make it possible to create a secure "European Internet Subnet" . Include the consequences for the access to the global internet and the interoperability.

7.1.1. What is a subnet ?

As commonly known the internet is a network of networks, hierarchically binding together presently more than 40.000 relatively independent networks . These more or less independent networks are technically called autonomous systems (AS). An AS is a heterogeneous network typically governed by a large enterprise for easy management. An AS has many different subnetworks with combined routing logic and common routing policies. Each subnetwork is assigned a globally unique identification number by the Internet Assigned Numbers Authority (IANA).

A Subnet is thus a logical grouping of connected network devices keeping a substantial part of the data traffic within a the local network . The subnets obtain full connectivity through transit agreements in which a network obtains the capability to receive and forward from another operator against monetary payment, who in turn has obtained the capability to reach all other destinations either through paid transit or peering agreements.

Network designers employ subnets as a way to partition networks into logical segments for greater ease of administration. When subnets are properly implemented, both the performance and security of networks can be improved.

A new network operator who wants to get access to the other 40,000 networks should comply to the international internet rules and protocols and buy or negotiate a peering agreement with an IXP or other AS network.

The independent networks are connected with peering agreements on a sort of international virtual marketplace. The actual transfer of data packages through these connected networks follow the rules of the Border Gateway Protocol (BGP). BGP is the protocol that addresses the routing of packets among different autonomous systems.

Originally the internet was developed as a means to connect users to the few distributed computing facilities in the US with strong restricted military access. Similar networks were subsequently developed by other government agencies and organizations that recognized the value and benefit provided by a networked environment. Initially these networks lived separate lives, but quickly these domains were connected and had to be able to interface and provide the means to exchange data with the other major networks at the time, which remained autonomous units but could directly interact using a common protocol.

This was the starting point of peering between autonomous systems and the principles of these early interconnection agreements live on until today. Finally a huge ocean with many islands, significantly differing in size, but each with explicit need to be connected to the other islands.

With the rapid growth of users and the geographical coverage area of the initial individual sub-networks, the expansion also brought in architectural changes. Instead of continuing to build a network by linking individual sites as equals, NSFNET introduced hierarchies into network design: institutions connected by this new infrastructure would be part of smaller local and regional networks, which were linked at network access points (NAP) to a long-distance backbone providing access to other parts of the country. This hierarchical organization into tiers, with Tier1 being highest up the hierarchy, is a core feature of today's interconnection landscape.

During the early years of the separate networks it gradually became clear that no single operator, not even the global backbone operators , were large enough to monopolize the network and customers were expecting connectivity to any service and part of the Internet.

7.1.2. BGP and its security

The approximately 40,000 subnets are connected with the Border Gateway Protocol (BGP) . The technical security of the interconnection ecosystem is largely driven by the security of BGP.

BGP as a protocol stems from the early days on the internet where espionage and cybercrime were beyond imagination. BGP is still considered by most providers and experts "the Achilles' heel of the Internet". Indeed, most of the recent interconnection-related incidents and Internet outages have revolved around BGP failures and vulnerabilities, and as BGP disorders tend to spread fast within this protocol monoculture, many incidents can have regional, national or even international impact. (Butler et al.[35]).

Recently within IETF's working group on Secure Inter-Domain Routing[39] (SIDR) and its solutions are gradually being adopted. The recent RFC 6480[40] describes a Resource Public Key Infrastructure (RPKI) to list, digitally sign, and verify prefixes. With RPKI it becomes possible to track whose prefixes are owned by whom.

7.1.3. Negative side effects of the anarchical internet

The idealistic and slightly anarchistic drive behind the current success of the internet show unfortunately also the dark side of freedom. Just like any other system or construction, the internet with all its complexity, contains many weaknesses, which notwithstanding the valuable efforts of many, will never be repaired completely. This offers consequently attractive opportunities for many to make use or misuse these imperfections. Leaving cybercrime aside, the opportunities on state level are roughly two-sided. For some nations the security of the state is under pressure internally, creating a demand and supply for technology to either track, reduce or even eliminate the activities of their own citizens on the internet and keep control on the data to the rest of the world. (North Africa, Syria, Myanmar, North Korea and China). For other nations the threat is primarily external and these nations track the foreign operators forming a possible threat to their nation. (keep everybody ignorant and inside, versus keep everybody out). However all nations share separately the same basic requirement: keep foreign intelligence out and let them not interfere in your internal affairs. We focus on the latter, because that is the central issue of this report.

7.2. What is the most effective way to keep foreign intelligence services out of national networks ?

7.2.1. Political agreements and sanctions

The most preferred option to solve international disputes, especially with allies, should be to find a political agreement. Such a process is actually taking place. Since 29 March 2011, the European Union has been negotiating with the United States government an international framework agreement (so-called 'Data Protection Umbrella Agreement') in order to protect personal data transferred between the EU and the US for law enforcement purposes.[65] Although valuable and relevant, this agreement does not imply any promise on collecting information for intelligence purposes for the security of the state. There are no formal references that these agreements are in place and neither are these

[65] Factsheet EU-US negotiations on data protection, June 2014, available at http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf, accessed November 2, 2014

imaginable. Not with allies, and certainly not with other countries.[66] This leaves nations to do whatever possible to prevent this collection and participate in the cat and mouse game, which in the end is won by the richest or the smartest.

7.2.2. Blocking physical access

If political agreements on spying are not possible, nations should rely on alternative ways to keep national secrets and the privacy of citizens inside. Generally speaking two ways are available. Physical and/or logical protection. Physical access to digital national information could be implemented by separating the national network, guarding the gateways, strict identify and access management (IAM) for all users on the network and securing the fiber cables throughout the nation. Theoretically possible but with the notion that no digital system will ever be perfect and the sheer vastness of the fiber networks and the impossibility to protect these, gives few confidence in the physical options for protection. Even when some imperfection would be accepted, the question remains whether the advantages for national security shall in the end outweigh the negative consequences for legitimate users.

7.2.3. Blocking logical access

Although some physical thresholds will always be required to reduce the possibilities for foreign data-collection, specialists[67] conclude that encryption is still the most effective and sustainable way to protect digital traffic. With encryption the complexity of physical protection could be reduced significantly, assuming the quality of cryptographic technology satisfies the needs and the architecture of the network leaves no unprotected spots. With the present internet architecture, still fundamentally unsecure, this leads to serious challenges. End-to-end encryption as the holy grail is for many in industry and research institutes a fast developing domain, with significant progress already achieved. Basically the knowledge on the possible ways forward is available, but a firm and clear policy is required to actually build fundaments for further success. Still the development of a countervailing data collection agency in the EU is realistically also a prerequisite to improve our knowledge and insight in the actual foreign mass surveillance, simultaneously enhancing the negotiation position to foreign data collectors.[68]

7.3. Conclusion

What would be possible technological, security, privacy and economic advantages and disadvantages of a secure "European Internet Subnet" strategy, which would effectively amount to a secure European Internet Subnet relying on the exclusive use of "EU network infrastructures" for the transfer of "EU data" between "EU data centres" housing "EU cloud computing and social network services" operated by "security-accredited EU nationals" working for "EU Companies" that are subject to "EU Data Protection Legislation" on "EU territory"?

Summarized answer:
Effectively securing the EU internet against threats from the rest of the world requires a radical isolation of the EU internet resulting in severe limitations for the development, freedom and prosperity of the EU citizens and

[66] 'Why America spies on its allies (and probably should)', Max Fisher, Washington Post, 29 October 2013, http://www.washingtonpost.com/blogs/worldviews/wp/2013/10/29/why-america-spies-on-its-allies-and-probably-should/, accessed on 15 november 2014.

[67] Christian Doerr, researcher University of Technology Delft

[68] Brussels demands 'EU intelligence service' to spy on US, Bruno Waterfield, Telegraph,, November 4, 2013 , http://www.telegraph.co.uk/news/worldnews/europe/eu/10425418/Brussels-demands-EU-intelligence-service-to-spy-on-US.html, accessed November 15, 2014

Industry. Even with these severe limitations there still will be many ways for very smart datacollectors to bypass the isolation and get access to the required data.

Question 8

What are technology orientations and high-level options that would make it possible to create a secure "European Internet Subnet" where it would be impossible for any observer to collect meta-data by tapping traffic via telecom operators, and/or using web-browser cookies and web-site trackers? How to interconnect the "European Internet Subnet" to the rest of the Internet world in a secure and interoperable way? Do we need a new Internet for that purpose? Are there potential inter-operability issues with the concept of a secure European Internet Subnet?

Summarized answer:
Effectively securing the EU internet against threats from the rest of the world requires a radical isolation of the EU internet. For this isolation huge investments will be necessary in the development of reliable equipment, protocols and encryption. The largest investment however will be necessary in an agency with many, highly skilled operators and security specialists responsible for the thorough and continuous analysis of in- and outbound data traffic. (ref paragraph 7.5)

Question 11

Is it feasible to build and security-manage the "European Internet Subnet" in the same way a very large international company would typically manage its own large international private IP network?

What would be the advantages and disadvantages of proceeding that way?

Would it be feasible to make European Internet traffic anonymous when routed outside of the secure "European Internet Subnet" over the global Internet?

Would we need "gateways" to filter traffic between this "European Internet Subnet" and the rest of the Internet, and to detect security breaches and possible abuses originating from external "nontrusted" data networks?

Summarized answer:

An EU subnet could theoretically be managed like a mega-Intranet. Actually there are many very large organisations (Wallmart, US MoD) in the world that run intranets successfully, the available functionality in any intranet is however always small and uncomparable with the real internet. Creating an intranet with the usability-level of the real internet would require a very large engineering, operations and security organisation with far-reaching mandate and equivalent responsibilities. (ref paragraph 7.5)

Overall conclusions on the European Internet Subnet

The consequences of several options for perimeterization of the EU at the level of the Internet (both higher and lower OSI levels) are severe. The open economy of Europe and the open nature of the European part of the Internet would most probably suffer substantial damage when isolated. At some level connections with the other parts of the Internet should be maintained, to keep access to social media, Cloud services, business partners and so on. But the technological challenges to have Gateways and prevent intrusions (for surveillance or other) are numerous. It would also be an expensive solution, in any option, and much less efficient than other technology foresight options.

8. Feasibility of a secure "European Internet Subnet"

"What are technology orientations and high-level options that would make it possible to create a secure "European Internet Subnet" where it would be impossible for any observer to collect meta-data by tapping traffic via telecom operators, and/or using web-browser cookies and web-site trackers? How to interconnect the "European Internet Subnet" to the rest of the Internet world in a secure and interoperable way? Do we need a new Internet for that purpose? Are there potential inter-operability issues with the concept of a secure European Internet Subnet?"

Sub questions 7, 8 and 11 are answered together under question 7).

9. Technological feasibility of cryptographic solutions

This annex pursues to provide answers to the following questions:

"What is the technological feasibility of using sophisticate cryptographic solutions at a lower network level to encrypt and sign network "routing information" and thus ensure it can only be "routed" over specific "trusted European data networks"? The objective being to prevent that network routing information (destination and origin IP addresses, port numbers, and other technical information) be intercepted for meta-data analysis purposes by a third party? How technically feasible would it be to give end-users some choice and control over the way their traffic is routed over "privacy compliant" vs "not privacy compliant" data network architectures"? Is this desirable?"

In the digital world there are many ways for third parties to intercept traffic that is not addressed to them, legally or illegally. However analyzing in detail these huge volumes of digital data flowing permanently through IP networks worldwide is challenging and requires substantial resources, but has been done. Interceptors need indications to filter potential valuable data packages from the large volumes of irrelevant data. This is more specifically relevant when data is encrypted, as decryption is even for highly specialized interceptors, time and processing power consuming. But also for legal reasons metadata is relevant, because most lawful interceptors need metadata to justify to formal responsible authorities the need to access the data content itself.[69]

Metadata

For effective filtering of data, interceptors use the available metadata adhering to the content of the data. This metadata may contain a wide variety of data elements. Potential valuable metadata elements are routing information, indicating who is sending data to whom, the type of the data (text, images, voice, formats) and data size. Sometimes even the subject of the message may be part of the metadata. All these elements together form valuable indicators for an automatic detection system to specifically mark this transmission for further and deeper analysis[70].

To deny or at least complicate the effective use of interception by unlawful parties, the masking of metadata is consequently assumed as an effective method. This masking however should not hamper the regular and sometimes necessary efforts of intelligence gathering, but should provide for these only to be used when necessary.

Weaknesses in internet routing

As stated above there are many vulnerabilities in the architecture of the internet in general and the design of the TCP/IP protocol more specifically. For this report the relevant weaknesses are the uncovered content of the data packets flowing openly through the network and the design of the routing principle, requiring that each router needs to read the destination address, and check it with the routing table to find the next link for the packet. Each router is more or less independent. There is no global supervisor governing the network of routers.

Any router in a upstream network therefore has access to the metadata within it, and in principle, anyone can insert a router in a network and manipulate the routing tables to attract relevant data traffic.[71]

[69] See for instance: https://www.aivd.nl/publicaties/@3033/interception/

[70] New York Times (2013) 'No Morsel Too Minuscule for All-Consuming N.S.A.,' http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?_r=1&&pagewanted=all (accessed November 24th 2014)

[71] Michael Mimoso, Threatpost.com , Internet-traffic-following-malicious-detours-via-route-injection-attacks, November 20, 2013 http://threatpost.com/ (accessed on 24 november 2014)

To solve this weakness, there are basically two approaches imaginable: (physically) separating the EU trusted network as a subnet of the Internet or protecting the EU data packets within the internet.

9.1. Approach 1: The European Internet Subnet, physically separate the EU network

To effectively separate the EU network physically first means that connections to and from the EU environment should be well guarded, by deeply analyzing the content of all passing traffic (DPI, deep packet investigation) and taking appropriate actions. This could mean formal control of a state-governed or other, independent body. Furthermore, there needs to be an effective surveillance method to monitor the presence of illegal separate external connections. Also an effective EU Identity Management process (distributed or centralized) is required to prevent illegal access inside the EU network by non-EU citizens. This has its drawbacks, like the sheer size of this effort and the varying approaches between Member States in digital identities. Also there is the real possibility of identity mules (people who offer their digital identity in exchange for something else, usually money).

One of the strongest measures against personal data extraction is prohibiting the export of personal data to non-EU data processors. In a thought experiment, this would mean seriously investing in gateway technology and monitoring, similar to the Great Firewall of China. It would limit market access to especially US Cloud providers, even if they would have their own data centres on EU soil. This would no doubt be very unpopular with the general public. The main economic difference with the Chinese situation is of course that this is a much larger and less fragmented market where years ago Chinese substitutes were initiated for popular American services like Google, eBay, Twitter et al. Despite being censored, these platforms attract many millions of users[72].

It is good to notice too that besides the impact on EU citizens, a physical segmentation in combination with strong data protection rules could also result in severe economical disputes, like claims for the lost investments in facilities in the EU.

Finally, the consequence of a physically separated internet implies that also the physical network, the fibre cables stretching all over the EU, should be protected (at the lowest OSI level). Eavesdropping on fibre cables is relatively easy and, using present technology, practically undetectable. Eavesdropping on submerged cables has been done for decades, with improved data collection technology providing ever more advanced and easily obtainable results. In the current situation, tapping on physical networks, not necessarily underwater, seems to be very effective, as the revelations on the Tempora project from the Snowden files indicate.[73] Analysts conclude that for these reasons the old-fashioned technology on submarine data collection seems to disappear[74].

9.2. Approach 2: Protecting the EU data packets on the internet

The second way of protecting EU metadata is to mask the information in such a way that unauthorized persons or systems cannot understand the content; i.e. cryptography. The options for protection and encryption of data packets are twofold. First the content should be protected and second the routing data should be protected to prevent it gets deviated outside the EU. The first option, End-to-end Encryption of data is extensively discussed in other annexes.

[72] http://readwrite.com/2010/03/03/china_top_3_social_network_sites, see also Annex 5.

[73] Guardian, the, GCHQ taps fibre-optic cables for secret access to world's communications, 21 June 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[74] Reuters, The Navy's underwater eavesdropper, July 19, 2013, http://blogs.reuters.com/great-debate/2013/07/18/the-navys-underwater-eavesdropper/ (accessed on November 24th, 2014)

For many years encrypted route control products have been available on the market.[75] With this technology ISPs can manage the routing paths for their outgoing traffic.[76] This technology is relevant for ISPs to provide optimized Internet connectivity and, at the same time, decreases the cost of bandwidth. Theoretically one can imagine a situation in which all EU ISPs are able to route traffic only on predefined safe routes in order to keep all EU data inside the EU (by managing routing tables accordingly).

Effectively however, you still have the same challenges as described in the last paragraph on physical separation the network. First there will be many users legitimately requiring unauthorized external routes. This traffic has to be investigated deeply by a reliable agent equipped with suitable mandate, rules and equipment. Secondly, this method assumes that all inside users are trusted and that there are no other illegal and non-surveilled connections with non EU domains elsewhere are in place.

If (semi-)centralized encryption of meta and content data is not possible for practical reasons, alternatively the encryption of metadata could be delegated to the user community itself. The EU governments then provide the knowledge and facilities to the user community. An example of this concept is Onion routing.

Hiding routing information

A number of other options are available to hide routing information. Some of these options are based on the concept of **mix networks**[77]. Mix networks are routing protocols that create hard-to-trace communications by using a chain of proxy servers known as mixes which take in messages from multiple senders, shuffles them and sends them back out in random order to the next destination. Applications that are based on this concept include **onion routing** and **anonymous remailers**.

An alternative that does not add an extra layer of complexity is to replace the network routing layer (layer 3) with another one that does not reveal a global identity. **Dovetail**[78] is an example of such a proposal. Dovetail combines ideas from **Source-controlled routing** and low-latency anonymity systems.

Onion routing

A widely used method to prevent that network routing information be intercepted for meta-data analysis purposes by a third party is Onion Routing, well-known for legal and illegal use as Tor. Onion Routing prevents the transport medium from knowing who is communicating with whom. The network knows only that communication is taking place. In addition, the content of the communication is hidden from eavesdroppers up to the point where the traffic leaves the OR network. There is a Tor network of several hundred nodes, processing traffic from hundreds of thousands of unknown users. The protection afforded by the system makes it difficult to determine the number of users or application connections. The code and documentation is available under a free license.[79] Many public organizations support materially or politically the Tor concept in public.[80]

The protection Onion Routing offers is not 100% however. It is dependent of whether the identity of the initiator of a connection (the sender) is hidden from the responder of the connection, or vice versa. Recent publications on the Onymous operation[81] indicate that the Tor network is infiltrated by law

[75] http://www.techopedia.com/definition/2532/route-control

[76] Ballani, H., Off by Default!, http://www.eecs.berkeley.edu/~sylvia/papers/ballani-defoff-camera.pdf

[77] http://en.wikipedia.org/wiki/Mix_network

[78] Sankey, J. and M. Wright, Dovetail: Stronger Anonymity in Next-Generation Internet Routing, PET symposium 2014 papers, 2014

[79] Source: www.torproject.org

[80] The TOR project sponsors, webpage https://www.torproject.org/about/sponsors.html.en (24 November 2014)

[81] Andy Greenberg, 11.07.14, Wired, ‘ Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains’; www.wired.com (24 November 2014)

enforcement agencies, but the modus operandi is not yet clear. It could still be that end-users of Tor have been compromised and not the network principles.

Many scientists and volunteers are actively involved in the further development of the onion protocol. One of the fundamental challenges they face is the protocol scalability. When in the near future the user base and the data volume is going to grow significantly, the overhead traffic to manage the network will become too heavy[82]. As the infrastructure of Tor now relies mainly on individual volunteers, a new explosion in Tor success could well lead to a call upon governments or industry to support the professionalization.

Still the concept of massive adoption of Onion routing could be one of the long term policy options for the EU to prevent that network routing information be intercepted for meta-data analysis purposes by a third party. This would mean amongst others distribution of Onion software or collectively installing plug-ins in browsers. Also, it would encompass investments in much more exit nodes.

If the value of the requirement is broadly and seriously supported by many member states and politicians, the development of a EU-wide Tor network could be an realistic option in the long term. Anticipating this development a comprehensive strategy is required involving academia, Industry and the user community creating the conditions and the circumstances to create a high quality EU internet with a high privacy level and with very strict surveillance policy managed by a reliable and professional EU intelligence service .

Beyond Onion

Garlic routing is a variant of onion routing that encrypts multiple messages together to make it more difficult for attackers to perform traffic analysis.[83]

Invisible Internet Project (I2P)[84] is an implementation of garlic routing. I2P is an anonymous network layer. It is designed in such a way that other software can use it for anonymous communication. It is controlled through a router console, accessible with a web browser. On top of I2P there implementations for e.g. web browsing, email, blogging and forums, website hosting, real-time chat, file sharing, decentralized file storage.

I2P has some similarities with Tor but there are also some differences. I2P has a distributed network database and peer selection while Tor has a centralized point to manage the overall view of the network, as well as gather and report statistics[85]. Tor has a larger user base, has significant funding – including developers – and is build and optimized for exit traffic.

9.3. Conclusion

To prevent that network routing information from being intercepted for meta-data analysis purposes by a third party , the EU could **physically or logically separate the network** from the rest of the world. The impact of both of these options on the community are however enormous: the material and technical prerequisites to develop these concepts are costly and finally the effectiveness of the concept is limited. The concept of onion routing is attractive but today not scalable enough to be used for the EU as a whole. With further developments and significant investments this would however be an attractive policy option on the longer term.

[82] J. McLachlan, A. Tran, N. Hopper, and Y. Kim, "Scalable onion routing with torsk," in Proceedings of the 16th ACM conference on Computer and communications security, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 590–599.

[83] http://en.wikipedia.org/wiki/Garlic_routing

[84] http://en.wikipedia.org/wiki/I2P

[85] https://geti2p.net/en/comparison/tor

10. Technological and organizational feasibility of European security baseline

This annex pursues to provide answers to the following questions:

"What is the technological and organisational feasibility of developing a European security base line & standard, and then of enforcing its adoption and implementation within Europe with all key Internet stakeholders? What would be the advantages and disadvantages of proceeding that way? What are the on-going initiatives and how do they compare with each other?"

10.1. What are security baselines?

A security baseline defines a set of basic security objectives, which are pragmatic and complete, but do not impose any technical (or other) means. The details on fulfilment of these objectives are determined by the owner of a specific (IT) environment and depend on the characteristics of that environment. Derogations usually are possible and expected (but preferably explicitly).[86] Baselines do not cover strategy or public regulations, but offer guidance for tactical and operational measures in terms of people, process and technology.

Security baselines are well known instruments for designing security in single organizations and industries (including the public sector). The objectives of baselines consist of topics (indicators, the 'what'), norms (standards, the level) and metrics (the how much and how do we know/measure). Usually such baselines build on market standards such as ISO2700x, which is considered best practice. ENISA has drafted a shortlist of such information security standards in 2012.[87] In the last two years this list has grown significantly across the EU, with many translations of ISO2700x to national or industry standards.[88]

10.2. Security baselines are considered a policy option for security in the EU

Given the fact that networks and systems are interconnected and influence each other, fragmented approaches in security hinder the creation of trust among peers, which is a prerequisite for cooperation and information sharing. According to the draft NIS Directive, there "*currently is no effective mechanism at EU level for effective cooperation and collaboration. (...) this may result in uncoordinated regulatory interventions, incoherent strategies and divergent standards. Internal Market barriers may also rise, by increased compliance costs for cross-border operating businesses*". [89]

Earlier EU studies covered the subject of security baselines before, as an option to improve e-government and e-health services for instance: "*The development of such a baseline starts by outlining a security strategy on a political level that presents a roadmap of security measures for Europe. Implementing a security check list could be the short-term measure to start improving the level of security of eGovernment services. In the mid-term perspective it would be relevant to start looking at policy options that can achieve*

[86] Based on: CERN Computer Security (2010), 'Mandatory Security Baselines' https://security.web.cern.ch/security/rules/en/baselines.shtml , accessed on August 10, 2014.

[87] ENISA (2012) 'Shortlisting network and information security standards and good practices', Version 1.0, January 2012. https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards , accessed on August 10 2014.

[88] In the Netherlands, for example, ISO2700x has been translated into separate security baselines for the central government (BIR), municipalities (BIG) and water boards (BIWA).

[89] European Commission (2013) 'Proposal for a Directive of the European Parliament and of The Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across The Union', http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=202368 , accessed on July 31st 2014

Security by Design of crucial components. In the long-term, policy measures that push for highly secure entire IT-systems become relevant"[90]

This idea takes the idea of security baselines much further: from a true baseline with objectives to secure components to secure IT systems. The focus shifts from standardization to certification, much more detailed, much more compulsory.

This paragraph here is restricted to the initial step, the checklist/standards as comfort building measure within organizations, between organizations in an industry or supply chain (or in an e-government context) or between Member States.

A good example of such a baseline as comfort building measure in a supply chain is the PCI-DSS standard[91], which defines security objectives for different actors in the chain of card payments (Point of Sale (device), merchant, services provider, acquirer). This helps establish secure transactions even if multiple different businesses are involved.

The draft NIS Directive is less far reaching in its ambitions. Article 14(1) prescribes a risk based approach for selecting appropriate measures, but the draft Directive does not refer to a specific set of measures or a specific standard. Using standards is encouraged, but the choice is left open:

"Article 16

Standardisation

1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security.

2. The Commission shall draw up, by means of implementing acts a list of the standards referred to in paragraph 1. The list shall be published in the Official Journal of the European Union."[92]

The question here is, if a big step forward, namely harmonization of security baselines across the EU, would provide more safeguards for privacy and security against unlawful mass surveillance.

10.3. EU security baselines do not necessarily offer protection against mass surveillance

As mentioned, a common EU security baseline aims to raise the general level of security in the EU, several slightly more specific aims have been attached to the concept. Not all necessarily and specifically including mitigating mass surveillance risks though. If this is the case depends on the scope and objectives in the baseline.

The main benefits of security baselines would be at least improved co-operation across borders through a common understanding and language, better protection of (then formerly) 'weakest links' and easier (more uniform) audit or other form of supervision. [93] By raising the overall level of protection, EU Member States and their citizens should become less attractive for attackers than lesser

[90] STOA (2013) 'Security of eGovernment Systems - Conference Report', http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/513510/IPOL-JOIN_ET(2013)513510(ANN02)_EN.pdf accessed on July 31st 2014

[91] Payment Card Industry (2013) 'Data Security Standard. Requirements and Security Assessment Procedures, Version 3.0', https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0, , accessed on July 31st 2014

[92] European Commission (2013) 'Proposal for a Directive of the European Parliament and of The Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across The Union', http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=202368 , accessed on July 31st 2014

[93] Based on ENISA (2012)

protected countries. This is because the costs will rise of surveillance, cybercrime or other attacks. However, to really offer more security & privacy against mass surveillance targeting the EU, specific objectives will have to be set and the accompanying controls rigorously implemented. Incorporating those specific objectives probably meet political discussion.

10.4. Market standards offer a good starting point for a generic EU security baseline

An earlier ENISA study pointed out that EU-wide security good practice (or baseline) should be based on ISO 27001/27002 standards. And if business continuity requirements are included, those could be based on BS 25999. The idea of different sets of requirements for different kinds of businesses can be adopted from PCI-DSS[94], although some of the implementation enforcing mechanisms in the card payment industry are not available or not as strong in other sectors. Regulation is probably needed where the market system will not lead to spontaneous adoption of baselines.

For generic baselines the content will not be the main hurdle for implementation, also because according to the mentioned study, ISO2700x is used extensively across the EU. Out of scope for this study however was a detailed comparison of all national and industry standards/baselines. This report cannot conclude on the barriers deriving from differences between nations and/or industries.

10.5. The scope and desired standard are mainly political challenges

Scoping is one of the first issues to tackle with baselines: what/who do the EU security baselines cover? Critical Information Infrastructure, including the Internet and other telecom backbone? E-government systems? Financial Services? All services providers for EU citizens? The broader the scope, the more stakeholders will be involved, the more complex decision making will be. This scope would ideally match that of the NIS Directive, which was when writing this report still under debate. The draft version holds a fairly broad scope in Annex II however. The current EU regulatory framework only covers telecommunication companies.

Another matter is what is considered *up to standard* per subject in the baseline? This also requires detailed discussion, taking differences between industries and countries into account.

In the end both are not technical discussions, but a political one. For certain some industries (or range of facilities) should be included in the scope, to help mitigate the risks of mass surveillance. For instance (mobile) telecommunications and Internet backbone facilities, but also ICT hardware and software, social media and (other) Cloud services. These are the services used extensively for producing, sharing, processing and storing massive amounts of personal data.

In the nearby future also devices in the Internet of Things ought to be considered, as they too can be part of a mass surveillance program, interfering with privacy. These ‘things’ can range from ‘wearables’ (like smart watches) and TV’s to cars, clothes and vending machines, all able to (remotely) provide digital information about their owner or user.

10.6. The digital world is dynamic, so should implementations of baselines

With the fast pacing developments in both technology and attack mechanisms, security can only be successful as an on-going process, with continuous iterations to adapt to new circumstances. Any framework, standard or baseline should be able to be high-level enough to leave room for swift operational adjustments. This is the current practice with the standards mentioned earlier, describing objectives. Organizations implementing the standard as their baseline put in the details and can adjust

[94] ENISA (2012)

these according to a scheme that fits their needs (or possibilities). That scheme can range from years to months. The standards themselves are also periodically evaluated and adjusted to new times. ISO2700x for instance was revised between 2005 and 2013.

Following this train of thought, a EU baseline needs to be concrete and high level enough to leave room to move for organizations and adjust to new threats. And also the EU baseline needs to be periodically evaluated.

10.7. Compliance to baselines requires an accepted level of monitoring

A measure installed to achieve trust, can only be trusted if it can be seen and checked. Earlier studies (ENISA 2012, STOA 2013) therefore recommend that there should be some form of supervision and oversight of implementation at EU and Member State level. Performance metrics (for a common KPI dashboard) should be mandatory in the EU to benchmark. Different institutional set-ups of such supervision are possible and need to be evaluated. These set-ups are out-of-scope for this study, but we embrace the idea of oversight and supervision. It is advisable to combine this role with participating in evaluation of the baseline itself, as the supervising authority or authorities will have a good overview of the workings of the baseline.

10.8. Beyond baselines: Certification for ICT hardware

In general security baselines do not prescribe detailed security requirements for hardware and software. This would require a different instrument, which will be much more costly to implement and maintain. Certification of hardware and software is such an instrument.[95] In theory, the use of certified product evaluations or certified development processes could be made mandatory, but it will be very hard to enforce if components are produced outside the EU.

This latter statement is especially true for software. It can be ordered on the web, downloaded and installed with ease. Modern coding, programming and assembling tools can make millions software producers, large and very small, publishing millions of lines of code on a daily basis. It is difficult to envision a situation where every (major) software in use within the EU is certified.

For ICT hardware this is substantially different. It is much harder to design, produce and distribute hardware on a large scale. Import and export of hardware is also a physical process, with more opportunities for supervision and enforcement of regulations. We see a parallel with the automotive industry, where all new car models are examined and approved before entering EU roads. In this process of homologation approval of a (certified?) authority or institute in one EU country leads to approval for all EU countries. This experience can be reused and adopted to the context of cyber security. Lastly, in order to ensure a level playing field and maximum security certification should be implemented for both EU and non-EU produced ICT-hardware.

10.9. Conclusion

Security baselines do not necessarily make the world a more secure place, but they do improve transparency between Member States and with regards to specific vulnerable industries. Thus security baselines are more about confidence building between nations. But depending on the measures prescribed and the standards per measure, baselines can raise the overall level of security, also against cybercrime threats.

Implementing baselines requires detailed discussions however, on scope (what industries etc.), security measures to be covered and standards per measure, but this is not completely new nor

[95] STOA (2013)

innovative. The challenge is mainly a political one: an EU security baseline needs to be both concrete and high level enough to serve all relevant industries and to adjust to technology dynamics. For instance the Internet of Things will change the scope of objects to be secured dramatically.

11. The “European Internet Subnet” as large international private IP network

Is it feasible to build and security-manage the “European Internet Subnet” in the same way a very large international company would typically manage its own large international private IP network?

What would be the advantages and disadvantages of proceeding that way?“

Would it be feasible to make European Internet traffic anonymous when routed outside of the secure “European Internet Subnet” over the global Internet?

Would we need “gateways” to filter traffic between this “European Internet Subnet” and the rest of the Internet, and to detect security breaches and possible abuses originating from external “nontrusted” data networks?

Sub questions 7, 8 and 11 are answered together under question 7).

Theme 3: Advantages and disadvantages of open source for security

This theme is about the open source options for all kinds of software, (European) Cloud and social media, open encryption standards and open hardware.

12. Advantages and disadvantages of using open source software

This annex pursues to provide answers to the following questions:

"How would the use of open source operating systems and open-source applications, by public administrations, by Internet Service providers, and by end-users strengthen or weaken the security of the Internet, IT products & services, and finally the privacy of end-users? Would the use of open-source products such as Linux, FreeBSD, openBSD, LibreOffice, Open Office, Mozilla, Android etc…be reducing or increasing the risks of implementation of backdoors compared to the use of proprietary software such as Windows, OSX, MS office, IE, IOs etc…What about the case of open-source Android versus closed-source IOs for instance? Are there significant security and vulnerability differences between the two mobile OS? Is one more compromised than the other by organisations doing mass surveillance?"

12.1. Using Open Source Software

Development and adoption of Open Source Software (OSS) is a recurring recommendation in security and privacy discussions.[96] The rapid growth in Internet has created the prerequisite for in numerous OSS development communities and widespread use. The collaborative effort of those communities has enable alternatives for almost all proprietary (also known as closed source) software.

From a security & privacy perspective the attractiveness of OSS lies mainly in the openness of the source code: anyone can review it and propose a fix for any problems encountered.[97] The drive to publish found vulnerabilities is not hampered by fear of reputation of the vendor and in fact publishing is encouraged. But please note, major open source applications might also have 'owners' with reputations to protect![98]

According to Anderson[99], vulnerabilities found by a vendor might be withheld from the public, because they are provided to their government for exploitation. Only until outsiders (e.g. other governments, cyber criminals) start exploiting it too, the vendor starts shipping patches. In this sense, OSS and the way it is supported by communities (code checking / review) can help finding and removing and even preventing backdoors enabling mass surveillance in widely used software.

Besides this, OSS also has the potential to decrease Europe's technological dependence on especially US vendors, with all accompanying advantages in terms of security & privacy. Investing in European OSS instead of in licenses of US vendors can stimulate the European software industry for billions of euro's.

Bias, bias and statistics

But how secure is OSS when looking at the facts? Discussions around OSS tend to be determined by the bias of the participants however, even if empirical data does not justify claims.[100] In most studies

[96] This includes the European Parliament report '*on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*'(2013/2188(INI)), published in 2014.

[97] See Part 1 of this study, chapter 6, where a concern is expressed with regards to the 'black box' character of commercial software.

[98] Wheeler, Dick (2004), Secure Programming for Linux and Unix HOWTO, Chapter 2, Is Open Source Good for Security?, http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html , accessed on August 12, 2014.

[99] Anderson, Ross (2002) 'Security in Open versus Closed Systems. The Dance of Boltzmann, Coase and Moore', in: Open Source Software : Economics, Law and Policy, http://www.net-security.org/dl/articles/toulouse.pdf, accessed on May 12, 2014

[100] Schryen, Guido (2009) 'Security of Open Source and Closed Source Software: An Empirical Comparison of Published Vulnerabilities', http://www.bibsonomy.org/bibtex/b72580b5932700da4873fe1ba70134aa, accessed

on this subject, empirically no significant differences in security between open and closed source software appear. Although in some cases the researcher finds empirical results that argue that "compared with closed source software, vulnerabilities in open source software: (a) have increased risk of exploitation, (b) diffuse sooner and with higher total penetration, and (c) increase the volume of exploitation attempts."[101] The level of (absence) of vulnerabilities therefore seems not to be the primary reason to pitch for OSS as security measure. The interesting thing is, that empirical evidence is already ten years or more old, still the discussion continues.

It is the process, stupid!

It is not the difference between open and closed, that determines the level of security, but much more the quality of the lifecycle management process.[102] Factors that influence this quality include:

- How rigorous is code reviewing and testing executed?
- How many versions are currently in the market and supported?
- Are security and privacy key interests of the supporting community?
- And of course the size and level of expertise of the community.

The OSS lifecycle management process with its openness and communities has its advantages, but also its challenges, for which some level of support might be in order.

Example Android vs. iOS: open does not necessarily mean more secure[103]

Symantec's Mobile threat report revealed that there are 387 documented vulnerabilities on Apple's iOS software, compared to a mere 13 on Android. However, despite Apple's higher iOS vulnerability score, Android remained the leading mobile operating system in the amount of malware written for it in 2012 because it is more open and less restrictive than Apple's iOS and has a much larger market share.

In fact, while Apple's iOS had the most documented vulnerabilities in 2012, there was only one threat created for it, whereas in the case of android although only 13 vulnerabilities were reported, it led all the mobile operating systems in the amount of malware written for the platform. It is claimed that 32% of those attacks were hackers attempting to steal information like e-mail addresses and phone numbers, showing that a growing number of malware authors are looking to commit some form of identity theft.

The different lifecycle management processes play an important role. Apparently it is far easier to offer infected apps for download via the Google Play apps store than through Apple's AppStore.[104] Attackers also benefit from the fragmented Android ecosystem (lots of versions current) that keeps the vast majority of devices from receiving new security measures provided, leaving users exposed to known and documented threats.

on August 12, 2014. Likewise Anderson (2002) and Iyengar, Kishen (2007) A Security Comparison Of Open-Source And Closed Source Operating Systems, http://www.swdsi.org/swdsi07/2007_proceedings/papers/236.pdf, accessed on August 12, 2014

[101] Ransbotham, S. (2010) An Empirical Analysis of Exploitation Attempts based on Vulnerabilities in Open Source Software, Workshop On The Economics Of Information Security, http://weis2010.econinfosec.org/papers/session6/weis2010_ransbotham.pdf , accessed on May 20, 2014

[102] See amongst others Anderson (2002).

[103] Based on Symantec (2013) Internet Security THREAT REPORT 2013, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf, accessed on August 12, 2014.

[104] Juniper (2013) Third Annual Mobile Threats Report 2013, http://www.juniper.net/us/en/forms/mobile-threats-report/, accessed on August 12, 2014

12.2. Challenges and key players

The development and maintenance (the lifecycle management process) of OSS meets a number of challenges that need to be addressed:

- The quality of review process depends heavily on quality (to read and write secure code) and availability of volunteers in most cases. These volunteers might work for companies, paid to support the OSS. But often they are truly (unpaid) volunteers, attached to the OSS, because they use it themselves. Heartbleed and other incidents can be detected earlier with auditing and checking code. TrueCrypt is a typical example of a problem of the commons: worldwide use dependent on 2 or 3 developers.
- OSS in more exotic programming languages, or niche or rarely used applications, might not attract a community large and/or expert enough to maintain the application and its security. Even widely used OSS like (once) TrueCrypt or OpenSSL have (had) fairly small support communities, that require support in terms of extra volunteers or funding to maintain their work.
- Reviewing and testing code can be boring. For many developers it is much more attractive to (just) fix what annoys them in the software. This might work out slightly different for commercially distributed OSS, where above average rigorous maintenance processes are deployed because the vendor has a (usually limited) liability for its products and a reputation to protect
- As mentioned above, an attacker doesn't necessarily need the code to find vulnerabilities. Like closed source, OSS also benefits from penetration testing.
- Distribution of fixes and feedback of found vulnerabilities to the developers are crucial. Likewise the installation of fixes on end-user devices of course, but this is quite similar to closed source (assumed that the OSS in question has a user-friendly, automatic update mechanism).

12.3. Conclusion

Despite the fact that it is not a universal remedy, OSS still is an important ingredient in a strategy for more security and technological independence. The quality of the support processes of OSS is crucial for its security though and those support processes face challenges that mostly cannot be solved without outside (financial) support:

- Support and fund maintenance and/or audit of important OSS platforms: open source initiatives, some of them widely implemented in very important systems, like OpenSSL[105], TrueCrypt/Ciphershed[106], GPG[107], Tor[108], OwnCloud[109] and others[110] need funding to keep going and be audited (both on code and processes).
- Promote Secure Software Development guidelines for all sorts of open and closed software. This should include distribution (to and from developers and to end-users).

[105] https://www.openssl.org/, accessed on August 25, 2014

[106] www.ciphershed.org, accessed on August 8th, 2014. At moment of writing, the first version of CipherShed was in development, "rebranding" the TrueCrypt 7.1a code. TrueCrypt itself was discontinued as of May 28th 2014.

[107] https://www.gnupg.org/ , accessed on August 8th, 2014

[108] https://www.torproject.org/ , accessed on August 8th, 2014

[109] https://owncloud.org/, accessed on August 8th, 2014

[110] This list does not mean the research team endorses this or any other OSS specifically; nor does the European Parliament.

- Certification schemes for specific critical types of OSS, potentially supported by technical tests (e.g. penetration tests) could be considered.[111] A recommendation supporting this would be to set up an agenda of critical OSS for the EU.

[111] Likewise Richardson, Robert (2014), "Open source needs some sort of body that promotes secure architectural design and coding", in: Open source needs more than the Open Crypto Audit Project, http://searchsecurity.techtarget.com/opinion/Open-source-needs-more-than-the-Open-Crypto-Audit-Project (accessed on November 4th 2014)

13. European next generation of secure open source Cloud Computing and Social Network websites

This annex pursues to provide answers to the following questions:

"Would it make technical sense for Europe to develop its own independent next generation of secure open source Cloud Computing and Social Network websites to compete with US ones (such as Facebook, Google, YouTube, LinkedIn, Instagram, etc..)? Is it technologically feasible for the European industry to catch up technology-wise with that of the US and to offer EU-based services similar to and as attractive and easy to use as the US ones? What would be advantages and disadvantages of following such an industrial policy in Europe from different technological, economic, security and organisational perspectives?"

As more and more countries are developing services that can operate (if need be) apart from the internet[112], it is no more than logical that there is an EU-wide focus on the question if it is desirable to develop specific, EU internet-related services. China leads the race in developing social networking sites that are alternate to that of U.S ones. YouTube, Facebook, and Twitter are blocked in China, but their Chinese equivalents are expanding. China is able to produce alternatives for each of the globally used US social networks like Youku for YouTube, Sina Weibo for Twitter and QZone for Facebook. The user base in China has increased in such an enormous manner that for instance even if Facebook is allowed in China it very probably will not reach the same dominance as it currently has in the US and Europe.

13.1. What is being proposed?

One of the main Snowden revelations about the NSA is the fact that major American companies are, willingly or unwillingly, the subject of major tapping operations[113]. Moreover, the grounds for this are legal, since the FISA court has approved the actions of the NSA in this regard, especially when it concerns non-USA residents[114]. The idea of developing own versions of services has quietly been promoted by countries in the form of separate social networks, search engines and the like.

[112] The Guardian (2014), 'Putin considers plan to unplug Russia from the internet 'in an emergency'' http://www.theguardian.com/world/2014/sep/19/vladimir-putin-plan-unplug-russia-internet-emergency-kremlin-moscow , accessed on Oct 5, 2014

[113] The Guardian, (2014) 'NSA Prism program taps in to user data of Apple, Google and others', http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, accessed on Oct 5, 2014

[114] European Parliament (2014), 'The US Surveillance programmes and their impact on EU citizens' universal rights', pp. 16-19 http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf , accessed on Oct 5, 2014

Rank	Name	Registered users	Active user accounts	Date launched	Country of origin	Date of user stat.
1	Facebook	1.6+ billion	1.32 billion	February 2004	United States	June 2014
2	Tencent QQ	1+ billion	829 million	February 1999	China	August 2014
3	Tencent Qzone	712+ million	645 million	2005	China	August 2014
4	WhatsApp	700+ million	600 million	June 2011	United States	August 2014
5	Google+	1+ billion	540 million	June 2011	United States	October 2013
6	WeChat	600+ million	438 million	January 2011	China	August 2014
7	Skype	663+ million	300 million	August 2003	Estonia	March 2014
8	Twitter	500+ million	271 million	March 2006	United States	July 2014
9	Instagram	300+ million	200 million	October 2010	United States	March 2014
10	LINE	490 million	200 million	June 2011	Korea	July 2014
11	Baidu Tieba	1 billion	200 million	December 2003	China	December 2013
12	Sina Weibo	503+ million	156 million	August 2009	China	August 2014
13	Viber	300 million	105 million	December 2010	Israel	February 2014
14	YY	300 million	100 million	December 2010	China	August 2014
15	VK	270 million	100 million	September 2006	Russia	September 2014

Table: list of virtual communities with more than 100 million active users[115]

From the above data, it can be inferred that U.S and Chinese Social networking websites lead the race in the user database when compared around the world and the same goes with cloud computing services. There are many reasons for this and definitely security is one of them. Other reasons include user satisfaction, ease of customization and the continuous changes their algorithm undergoes being open source networks. It can be seen that the user data base of these networks stand very far from that of other countries.

The idea of EU Cloud (and other) services is subject to some differentiation though: it is not always clear (even from the EU's own Cloud Strategy) if this means specific European services or just a differentiation by which data is only used in the EU. For instance, several commercial service providers who operate worldwide offer European Cloud services, in the sense of localized data. In the context of this paper, European services are described as services operated under European law, and where all the data is stored and used within the EU.

The idea of independent or anonymous services has always been popular in tech circles, where the NSA revelations led to the search for alternative services, such as *DuckDuckGo* as a search engine, and more recently, *Ello* as a social network. The use of these alternatives has so far however been limited. However, the rise of social media like Yammer, which offer corporate accounts for a *Twitter*-like

[115] Multiple sources, assembled on: http://en.wikipedia.org/wiki/List_of_virtual_communities_with_more_than_100_million_active_users, accessed on October 9th 2014.

medium, suggests that secure applications can be adopted in a corporate (or government) environment first.

There are some movements towards open source cloud solutions, such as in services like *OpenStack*, an open source IaaS solution. However, as the recent acquisition of open source cloud provider *Eucalyptus* by US firm HP proves[116], open source is no guarantee for non-US involvement. In the context of this policy option, using open source is treated as one of the ways in which independence from globally operating and integrated services could be achieved. However, the main focus is on developing separate European services.

13.2. The technological feasibility of promoting European (open source) Cloud Services and social media

Technologically, there are no great impediments to developing European services. In fact, in earlier decades, many examples of European, or more specifically, nationally-oriented social media abounded. However, these have never been developed with the security of European users in mind, and has no specific legislation attached to protect users.

On a limited scale, European companies are competing in the global market. However, this global market precludes an exclusive European focus for these companies.

13.3. Why should be EU cloud, social media and search engines be promoted?

From a security standpoint, there is much to be said for operating separate European services.

Rule of Law. EU citizens are considered third parties under US law. In other countries where the rule of law is even less defined, the position of EU citizens who use services is even less certain. If services are specifically targeted at EU citizens and visitors and data is only collected and stored within the EU, compliance with EU law is more easily enforceable.

Independence. Since the tech world is a highly volatile market with lots of acquisition, the service a user signs up for today may be acquired by a different company tomorrow. Setting up standards for services aimed specifically at the EU market would provide a certain measure of independence from these market movements (although agreement will still ensure access of acquired services to EU markets)

Accountability. Basing users and user data in the EU ensures accountability, in the sense that there is no risk of takeovers affecting legal ownership of user data. Offering European cloud services or a search engine will mean that operations must be based in a European country and thus be compliant with its laws and the framework of laws and guidelines in the EU.

13.4. What are the limitations and drawbacks of offering EU services?

Market inefficiency. The most obvious drawback of the scenario of developing European social media is that it will create market inefficiencies. Foreign players being unable to operate in Europe or differentiating their service for European users will mean unnecessary hurdles to business and innovation. Moreover, EUservices being unable to expand beyond their home turf will hamper growth and innovation within the EU market.

[116] Wired, (2014), 'HP Acquires Open Source Cloud Pioneer Eucalyptus', http://www.wired.com/2014/09/hp-eucalyptus/, accessed on October 9th 2014.

Lack of demand. The appeal of the currently popular cloud services, social media and search engines lies in the fact that they are a) the best (or interchangeably the best) service available and, usually more importantly, widely used.

Problems with using outside of the EU. Interoperability problems lie ahead in heaps in this scenario, both between devices, but more importantly, between countries, once users start moving abroad.

Interdependence hard- and software. If the idea of developing EU services is to be free of foreign meddling, it is highly likely that this goal will be missed, because foreign hard- and software, as well as personnel is integrated in every operation of major IT business and development. The chance that these are, or will be equipped with backdoors or simply required to cooperate with local intelligence and law enforcement, is large indeed.

Balkanization. The idea of 'cutting up' the internet and its services goes against the very ideas that propelled the internet and have fueled EU policy towards a 'free, open and secure' internet.

Installed base. Many companies and consumers have adopted US based Cloud services for their business, communication or leisure. It would take a substantial effort to transfer their data, social network et al. to a different platform.

Limited effect against mass surveillance. In the case of Google and Yahoo, public reports point out that the NSA tapped directly into communication links to get access to user information, including those traveling to and from overseas data centers.[117] Just protecting European datasets in Europe or implementing strictly EU Cloud services does not provide any guarantee against such practices, especially when European Intelligence agencies cooperate with foreign agencies.[118]

13.5. Key Players

In the context of the EU Cloud Strategy, the European Commission spoke to many key players. (CloudSigma, Microsoft, ATOS, IBM, Alcatel-Lucent, SAP). Although some of these players are US-based, there is an established European IT market, as well as a booming startup culture in parts of Europe. A report released by the European Commission in 2014 maps Europe's top ICT hubs[119] and suggests healthy prospects for both business and R&D. In this sense, finding parties to develop these services shouldn't be too hard. In fact, being able to develop services within the European market might help counter the monopolizing nature of current market trends by encouraging development of competing services without them being bought or squashed by their competitor.

Another group of key players consists of the incumbent Cloud services providers, like Microsoft, Google, Facebook, LinkedIn, Amazon, eBay, AliBaba and others. They have a stake in maintaining the status quo. The US based services providers feel the market pressure in the sense of loss of trust due to the Snowden revelations. Their fear is to lose market share caused by government actions and some urge their legislators for more transparency[120] and more protection for (US) citizens.[121]

[117] The Guardian, (2014) 'NSA Prism program taps in to user data of Apple, Google and others', http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, accessed on Oct 5, 2014

[118] See for instance: Süddeutsche Zeiting (2014) BND leitete Telefondaten an NSA weiter, 24 June 2014, http://www.sueddeutsche.de/digital/geheimdienste-bnd-leitete-telefondaten-an-nsa-weiter-1.2016504, accessed on October 9th 2014.

[119] European Union (2014), EU Atlas of ICT Hot Spots, http://is.jrc.ec.europa.eu/pages/ISG/eipe/atlas.html , press release at http://europa.eu/rapid/press-release_IP-14-435_en.htm, accessed on October 9th 2014.

[120] AOL et al. (2013) 'USA Freedom Act Letter' http://sensenbrenner.house.gov/uploadedfiles/usa_freedom_act_letter_10-31-13.pdf , accessed on October 9th 2014.

[121] Fedscoop (2014) 'Microsoft champions Internet privacy, calls on Congress to act', 24 June 2014, http://fedscoop.com/microsoft-calls-congress-act-privacy/, accessed on August 10 2014.

13.6. Conclusion

Although it is technologically feasible to encourage a ‘EU-only’ infrastructure, and in some senses a desirable development, a development like this is precluded by the EU’s own market demands, as well as practical impediments of market size, regulations and a lack of practical effect. In order for these services to work, there would need to be either a strict policy on the part of EU and member states prescribing EU-only measures to governmental agencies and suppliers, or a market-driven movement would have to be facilitated (in which consumers would choose products based on the criteria of security and independence as USP’s – a questionable presumption, when set against price and efficiency criteria).

14. Strengths and weaknesses of open source implementations compared to that of proprietary solutions

This annex pursues to provide answers to the following questions:

"Does it make technological sense to use open encryption standards, and open-source hardware and software encryption solutions to reduce the risks of implementation of backdoors and design flaws in encryption systems (cfr recent case with RSA)? For instance, what are the strengths and weaknesses of open-source implementation by Certification Authorities and encryption solutions such as DogTag, EJBCA, gnoMint, OpenCA, OpenSSL, TinyCA, XCA over proprietary solutions commercialised by RSA, Verisign, ENTRUST or UTIMACO for instance ? What if national security agencies contribute or take the lead of the development of some open-source projects, as it seems to have already been the case in the past with SE-Linux for instance? What is the risk to ending up with un-detected backdoors in this scenario?"

14.1. Open encryption standards, open source hardware and software encryption solution

The only proper way to use encryption is to use open encryption standards. Only standards that can be scrutinized by the cryptography community can be expected to be secure. The algorithm should only depend on the secrecy of the key(s), not of the algorithm. Independent evaluation is considered the norm and has for example been applied to the selection of the successor of DES: AES and the current selection of the successor of SHA-2. Besides that Europe currently does not have an independent evaluator similar to NIST in the USA. Therefore we often rely on the evaluations from the USA, even though Europe has top cryptography researchers.[122]

When making the assessment about whether to use hardware or software encryption, be it open source or not, always take into account that with hardware a higher level of security can be reached. Software has the disadvantage that it can be changed by an attacker and/or the keys can be extracted more easily.

When using open source software encryption algorithms it provides the opportunity to verify not only the design but also the implementation. This is considered an advantage above closed source implementations that cannot be verified. Open source not only enables verification, it also enables attackers to find vulnerabilities in the implementation. This small disadvantage is not as important as the possibility of verification of the source code. This is also the case for Open Source Software for Certificate Authorities and encryption solutions.

Although in the case of certificate authority it is currently more important to come with a better certificate model than to worry about backdoors in software because an evil organization could use any other certificate software to generate an evil certificate.

If national security agencies take the lead in developing such software, it is important that the changes to the software are independently verified so not just one organization can make changes to the software which otherwise make it possible to add backdoors or other additions with bad intentions. If no independent verification can be done, the open source adds much less value.

For open hardware it is very hard to prove that hardware only has the designed functions and no malintended functions have been added. To ensure that, the manufacturing process and logistics are required to be secure. In general and certainly for mass production this is almost impossible to do.

[122] E.g. in the United Kingdom: Ross Anderson; Belgium: Bart Preneel, Vincent Rijmen; in the Netherlands: Marc Stevens, Benne de Weger, Arjen Lenstra, Niels Ferguson.

14.2. Conclusion

Open source software has an important security advantage over closed source. The possibility to evaluate the product makes it easier to evaluate it and determine if it has vulnerabilities. For open source software it is important how the verification of changes in the software is arranged. Because the manufacturing and logistics of open hardware are difficult to secured, the value of open hardware for security is smaller.

15. Risk of backdoors in the case of open source hardware

This annex pursues to provide answers to the following questions:

"Would the use of open hardware design for CPU, chipsets, etc…contribute to reducing the risks of backdoors implemented at the hardware level? What are the risks that some chip manufacturers implement hidden capabilities that can be exploited for mass surveillance purposes? Is it better or worse than for proprietary hardware designs? What could be done in practice to promote open hardware design practices?"

15.1. Introduction

For surveillance the advantage of interfering at hardware level, is that all sorts of software level security measures can be circumvented. It ensures direct access to the hardware used by both users and ISPs. The NSA revelations suggest wide-scale adoption of this point of entry[123], but the use of certain brands has long been banned by western security services.[124]

One of the security measures circumvented is of course encryption, otherwise the strongest line of defense. With Differential Power Analysis (DPA) attackers can monitor fluctuating electrical power consumption of a chip to statistically derive cryptographic keys. This would render encryption useless, especially against targeted attacks. If such an attack is performed on hardware providing E2EE on a communications channel, then the all of the communications shared is unveiled.

Commercial providers like Cryptography Research already provide solutions to better protect devices against DPA. Such solutions are in use for mobile devices, pay television systems, bank cards, security identity products, HSM's and other components.

But measures will not be taken unless vulnerabilities are known and users/owners can modify their hardware. They are dependent on (mainly US and Chinese) vendors.

15.2. Open source hardware

Open source hardware is "*hardware whose design is made publicly available so that anyone can study, modify, distribute, make, and sell the design or hardware based on that design. The hardware's source, the design from which it is made, is available in the preferred format for making modifications to it. Ideally, open source hardware uses readily-available components and materials, standard processes, open infrastructure, unrestricted content, and open-source design tools to maximize the ability of individuals to make and use hardware.*"[125] Open source hardware (or OSH) provides the freedom to control technology while sharing knowledge and encouraging commerce through the open exchange of designs.

OSH can includes schematic, Hardware Description Language (HDL) code, and layout files. Software and firmware interfaces such as drivers, compilers, instruction set, and registers interfaces should be available and open source. All information and documentation, like application notes and interfacing information, should be also openly available.[126]

[123] Greenwald, Glen (2014) *No Place to Hide,* New York: Metropolitan Books

[124] Tech Republic (2013) 'Corporate espionage or fearmongering? The facts about hardware-level backdoors', http://www.techrepublic.com/blog/it-security/corporate-espionage-or-fearmongering-the-facts-about-hardware-level-backdoors/, (accessed on August 20, 2014)

[125] OSHWA, 'Open Source Hardware (OSHW) Statement of Principles 1.0', http://www.oshwa.org/definition/, accessed on August 4, 2014

[126] Ferreira, Edy and Stoyan Tanev (2009), 'How Companies Make Money Through Involvement in Open Source Hardware Projects', http://timreview.ca/article/228, accessed on August 20, 2014

15.2.1. Use of OSH (open source hardware) to reduce risk of backdoors

While there is no foolproof defense against government spying, snooping by entities like the National Security Agency could be made far more difficult through the use of Internet infrastructure built on open-source hardware, an academic researcher says.[127]

Eli Dourado, a research fellow at George Mason University, argued that companies using open hardware would be in a better position to detect backdoors or vulnerabilities planted by the NSA or any other government agency. "To make the Internet less susceptible to mass surveillance, we need to recreate the physical layer of its infrastructure on the basis of open-source principles". According to Dourado, success would come from the fact that anyone could fully audit the hardware, make changes and then distribute the modifications to others. This model has driven the success of open source software used across the Internet today. Such technology includes the Linux operating system and the Apache Web server.[128]

15.2.2. Complexities involved in implementing open source hardware

While the ability to fully audit hardware sounds good, the reality is many organizations do not have the people with the expertise to continuously examine updates of low-level code in hardware, Murray Jennex, a professor of information system security at San Diego State University, said.[129]

Part of the charm of open source software is the "*do-it-yourself*" (DIY) aspect of it. If one find a bug, or just want to improve a feature, there's the possibility it can be done one one's own. But microprocessors are arcane devices and the complexity involved within their circuits does not lend itself to DIY improvements. That's not to say big software projects aren't just as complex as microprocessors, only that hardware gates, signals, and pipelines interrelate in a way that lines of commented source code do not.

In Open source software (OSS) "free" may be confused with "gratis" ('free beer') because it often costs nothing to make your own copy. In OSH the situation is different. People can download free hardware designs, but they either have to pay someone to manufacture the hardware or buy the components and tools or manufacture to hardware themselves. In most cases, it is very costly to manufacture the hardware. The costs are related to the replication of the physical hardware, not with the replication of the design itself. Perhaps some hardware manufacturing pioneers make open hardware design and can sell the required equipment themselves.[130]

In some pieces of hardware, the cost of the IP, which includes the cost of the design, is much lower than the cost associated with manufacturing and integration. For example, in the case of microprocessors, designs built on OSH IP cores alone are not likely to be commercially successful. This means the cost of some commercial IP cores must be added to the final cost of the hardware product. Another challenge arises as hardware is not as modular and compartmentalized as software. Modularity is a critically favorable characteristic for OSS production. For example, modularity was important in the case of the Apache software allowing developers to work in particular areas without affecting other modules.[131]

[127]Gonsalves, Antone (2013) 'Researcher argues for open hardware to defend against NSA spying', http://www.csoonline.com/article/2134047/network-security/researcher-argues-for-open-hardware-to-defend-against- nsa-spying.html, accessed on September 21, 2014

[128] Dourado, Eli (2013) 'Let's Build a More Secure Internet,' http://www.nytimes.com/2013/10/09/opinion/lets-build-a-more-secure-internet.html?ref=international&_r=1&, accessed on October 10, 2014

[129] Gonsalves (2013)

[130] Ferreira and Tanev (2009)

[131] Ferreira and Tanev (2009)

15.2.3. Promotion of open source hardware

The costs related to designing, verifying and understanding OSH are high as explained before. This process requires appropriate Electronic Design Automation (EDA) tools[132] which are very expensive. In addition, hardware testing and verification requires expensive external hardware equipment such as oscilloscopes, analyzers and wafer probes. Currently, there are open communities developing open source EDA tools that will eventually improve to the point where they will be competitive with commercial EDA tools.

A major obstacle is the fact that some commercial EDA tools are designed to work with commercial FPGAs[133] that are protected by commercial secrecy. Open source EDA tools can not be adapted to interface with those FPGAs without facing legal issues. One of the suggested solutions is the development of open source FPGAs whose interfaces would be open enough to allow the use of any open source EDA tool.[134]

15.2.4. Conclusion

A backdoor on a silicon chip jeopardises any efforts of adding software level protection. This is because an attacker can use the underlying hardware to circumvent the software countermeasures.[135] A debug port (JTAG[136] or other) or factory test interface can potentially be used as points to scan the silicon chip for backdoors or Trojans. Most chips manufactured these days have such a port or interface.

Until the development of more efficient 'silicon' scanning techniques, it has been unfeasible to test real silicon chips for Trojans or backdoors. Researchers have been able to use a (low-cost) system to independently test silicon for backdoors and Trojans 'in a matter of weeks'. [137]

Open source hardware has as distinguished advantage that anyone can perform that test and make proposals for solving vulnerabilities AND implement them.

Advanced intelligence services could still try to exploit open hardware, given the fact that there is no 100% certainty of security. And of course, open hardware would do little to prevent the government from reading e-mail if it still had the cooperation of Cloud providers or other technology companies. Open source hardware is therefore not a panacea by itself. But, open hardware would at a minimum make the mass surveillance efforts more difficult, more costly and probably less effective.[138]

[132] EDA are software tools for designing electronic systems such as printed circuit boards and integrated circuits.

[133] A Field-programmable gate array (FPGA) is an integrated circuit designed to be configured by a customer or a designer after manufacturing

[134] Ferreira and Tanev (2009)

[135] Skorobogatov, S. and C. Woods (2012) Breakthrough silicon scanning discovers backdoor in military chip, 2012

[136] Joint Test Action Group (JTAG), common name for the IEEE 1149.1 Standard Test Access Port and Boundary-Scan Architecture

[137] Skorobogatov, S. and C. Woods (2012)

[138] Likewise: Dourado (2013)

Theme 4: Advantages and disadvantages of pushing towards “end-to-end” user encryption

This last theme focuses on end-to-end encryption, including a wide array of topics like end-to-end encryption in Cloud computing and social networks, advantages and disadvantages, electronics banking, e-mail, GSM and IPSEC vs SSL VPN. Please note that in some paragraphs, “end-to-end” encryption has been referred as E2EE.

16. End-to-end encryption in cloud computing and social networks

This annex pursues to provide answers to the following questions:

"Would it be technically feasible for cloud computing and social network service providers to upgrade their services to allow their customers to encrypt partially or totally all of their data "end-to-end" (as opposed to the current practices where service providers have access to the decrypted personal data of all their customers)?

Could the same result be obtained by a new generation of third party applications, allowing for instance, a group of users sharing information on Facebook or LinkedIn to post encrypted information on their "walls", and in such a way that Facebook and LinkedIn service providers would be unable to decrypt it? What are the long-term technology orientations to implement "end-to-end encryption" amongst groups of users sharing personal data over a specific service? Is this feasible?"

16.1. Introduction

Social networking is ubiquitous and is only poised to grow further. The Snowden revelations show that the interest of parties performing Mass Surveillance is aimed specifically at social networks, since these contain unique information that cannot be traced in other ways. Cloud computing is another example of a source that contains a trove of information that is connected to the internet.

16.1.1. Cloud Computing

Cloud computing service providers do not implement strong security solutions as their products are cost-motivated. Users face increased risks from hackers. These vulnerabilities can easily be addressed through the adoption of industry standard encryption technologies, which are already in popular use by online banks and retailers. It is therefore technically feasible for cloud computing companies to provide better security and encryption, and in some instances, we are seeing these (paid) services emerge.[139] Mozilla is increasingly interested in building encrypted storage, for instance in enabling Firefox Sync. These do, however, entail some concessions to encrypting, since sharing can be cumbersome.

As was earlier alluded to, it is also financially not very attractive offer encryption by default for all of these products, since it requires considerable computational power and usability issues.

16.1.2. Social Network Service Providers

In the wake of the Snowden revelations, several startups that offer encryption have launched, or received more attention. Since March 2014, an app called MyApollo offers a Facebook-like interface with full encryption[140]. A similar initiative, Syme, has already gone belly-up.[141]
However, most major social networks still do not offer encryption – even if some (like Facebook and Google) now do offer HTTPS.

16.2. Third party applications

Third-party apps are available for Facebook users who want to use end-to-end encryption for their communication needs, while still being connected to 'regular' social media. Programs like Pidgin and

[139] See, for instance: https://www.wuala.com/ and https://spideroak.com/ , accessed Oct 1, 2014

[140] https://myapollo.ca/, accessed October 3, 2014

[141] PC World (2014), 'Syme, a social network that promised Ello-like privacy, has gone dark', http://www.pcworld.idg.com.au/article/556657/syme-social-network-promised-ello-like-privacy-has-gone-dark/, accessed Oct 14, 2014

Cryptocat, provide end-to-end ways to encrypt chats carried out over Facebook's Messenger app and other IM programs[142]. These do, however, pose issues with regards to the extra trouble it takes users to install and use these programs. In general only specifically 'aware' users now install these applications. Further development of these options certainly seems plausible, with increasing usability as a first priority.

16.3. Long-term technology orientations

As a long-term option, to allow end users to enjoy the functionalities of online social networks without compromising their privacy, an alternative is to structure the social network as a **peer-to-peer (P2P) network using encryption**[143]. A peer-to-peer approach respects privacy optimally, as it allows social interaction to have end-to-end or group encryption. Some technologies can even make it difficult to determine who is interacting with whom.

Another possibility could be to adopt a **decentralized approach** to online social networking.[144] Decentralized social networks have the potential to provide a better environment within which users can have more control over their privacy, and the ownership and distribution of their information. Therefore, online social networking will be more immune to censorship, monopoly, regulation, and other exercise of central authority. Decentralization promises higher performance, fault-tolerance and scalability in the case of an increasing user base.[145] Also, a decentralized approach to online social networking breaks the boundaries between social networking sites by providing users more freedom to interact with each other.

As was described in question 2 of this Annex, research in the US is directed to encryption in the cloud, which would make it possible to ensure encryption all the way also in these instances, to ensure secure Cloud Computing. These options however, are currently not available, so need more R&D and a stronger push.

[142] https://www.pidgin.im/ and https://crypto.cat/ , accessed October 3, 2014

[143] Oltheanu, Alexandra and Guillaume Pierre (2012) 'Towards Robust and Scalable Peer-to-Peer Social Networks', ACM, available at http://reconcile.pjwstk.edu.pl/AppData/Files/SNS12_Alexandra_Olteanu_authors_version.pdf, accessed Oct 3, 2014

[144] Yeung, Ching-man Au et al (2008) 'Decentralization: The Future of Online Social Networking' http://www.w3.org/2008/09/msnws/papers/decentralization.pdf , accessed Oct 3, 2014

[145] G. Pallis, D. Zeinalipour-Yazti, and M. Dikaiakos (2011) 'Online social networks: Status and trends.' In: New Directions in Web Data Management 1, volume 331, Studies in Computational Intelligence, pages 213–234. Springer Berlin Heidelberg.

17. Advantages and disadvantages of "end-to-end" encryption

This annex pursues to provide answers to the following questions:

"What would be the advantages and disadvantages of using end-to-end encryption from the following point of views:
(i) Privacy for the end-user;
(ii) Law enforcement and/or national security for the society as a whole;
(iii) Commercial issues for service providers;
(iv) intellectual/property and copyrights for authors;
(v) Technically given the need for more computing power and given caching issues"

(i) Privacy for the end-user

Advantages

With E2EE, messages are encrypted on the sender's computer and decrypted on the recipient's device. Telecom providers and service providers like Google, Facebook, Tencent or Microsoft only see the encrypted version of the message. Thus they cannot turn over (readable) copies to government agencies, even with a court order. In this way E2EE offers an improved level of confidentiality of information and thus privacy, protecting their users from both censorship and repression and law enforcement and intelligence.

Strong cryptographic software is available to those who want to use it as E2EE software and has existed since the 1980s. They include PGP (e-mail encryption software released in 1991), OTR ("off the record", for secure instant messaging) and the Internet telephony apps Silent Circle and Redphone, as well as newer ones, such as Proton Mail, DIME (aka Dark Mail) and specific plug-ins for Chrome, Firefox and other browsers.

A sufficient key-length and -size is necessarily to ensure protection: 128 bits or longer is advisable, but this depends on the algorithm employed too. Larger keys are possible (Blowfish can for instance handle 448 bits and AES demands 256 bits). Please see also Annex 6 - Latest technology prospects related to encryption.

Furthermore newer E2EE (like DIME and ProtonMail) also encrypt metadata, thus offering more security against mass surveillance on metadata.[146]

Disadvantages

E2EE offers no protection against software or hardware backdoors (on the device, after the 'End'). At some point the user has to access his or her information in order to read or modify it. Also targeted attacks with for instance screen scrapers or key loggers can still obtain the desired information from the users device. Protection is therefore not complete.

One of the best known problems of encryption software is (the lack of) user-friendliness.[147] Even if it has been acknowledged many times, it still proves to be hard to make E2EE easy to use and users

[146] Gallagher, Ryan (2013) 'Meet the "Dark Mail Alliance" Planning to Keep the NSA Out of Your Inbox', http://www.slate.com/blogs/future_tense/2013/10/30/dark_mail_alliance_lavabit_silent_circle_team_up_to_create_surveillance.html and Levison, Ladar, 'Lavabit is Dark Mail Initiative', https://www.kickstarter.com/projects/ladar/lavabits-dark-mail-initiative/posts , both accessed 17 October 2014.

[147] Whitten, Alma and J. D. Tygar (1999) 'Why Johnny Can't Encrypt' in Security and Usability: Designing Secure Systems that People Can Use, eds. L. Cranor and G. Simson. O'Reilly, pp. 679-702. See also: Lee, Timothy B. (2013) 'NSA-proof encryption exists. Why doesn't anyone use it?'http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-

value convenience more than security. Experts point to trade-offs between convenience and usability and security.

Users who do use encryption currently, stand out in the crowd, unless a lot more users are going to use it. This is especially a problem in countries with censorship/human rights issues, where using encryption might even be illegal.

A chicken-and-egg problem also arises: only if enough people are using it, and you know other people that are using it, does using encryption become useful. PGP, DIME/Darkmail or other encrypted e-mail applications only offer protection when communicating with other users with the capability to receive encrypted e-mail.

Encryption is only effective only if the person one thinks one is communicating with. This authentication relies on using the right keys. A 'man in the middle' attack can trick the sender into using the wrong encryption key. To thwart this kind of attack, sender and recipient need a way to securely exchange and verify each other's encryption keys. Confidentiality therefore heavily depends on authenticity.

Much mass surveillance effort depend on metadata to find the needle in the haystack. For privacy purposes, this metadata has to be encrypted too, not just the content of communications, but this is not the case with all E2EE solutions.

A more practical disadvantage of E2EE are the consequences of losing a password. Losing a user password means losing all data in the one's account, as the service provider has no access to the data and no private key either. This is, however, more a usability issue, not a privacy issue, though it might deter potential users.

E2EE has to be set up carefully too, in order to be effective. This is one of the reasons why it is found less user-friendly. It can happen that the user thinks they have encrypted their message or call, but in fact due to some mistake haven't.[148]

For the reasons above E2EE can also create a false sense of security for its users. It does not always offer complete protection, even when used correctly.

(ii) Law enforcement and/or national security

Advantages

The primary advantage of E2EE from a Law Enforcement and national security perspective is the protection of users (and society as a whole) against cybercrime and digital espionage. If content is encrypted, this sets up a serious barrier against malicious actors and prevents crimes and data leakage or at least lowers the potential impact.

As mentioned in Part 1, chapter 4.2, for surveillance cryptography still can be overcome with different approaches:

- Obtaining encryption keys
- Exploiting security vulnerabilities in the endpoints
- Exploiting weaknesses (or even backdoors) in the encryption programme
- Quantum cryptography (if/when available)

doesnt-anyone-use-it/, accessed on October 10, 2014. and CNET (2013) 'Dark Mail Alliance' looks to create user-friendly e-mail encryption, http://www.cnet.com/news/dark-mail-alliance-looks-to-create-user-friendly-e-mail-encryption/, accessed 17 October 2014. The Dark Mail Alliance, consisting of the founders of shuttered e-mail services Silent Mail and Lavabit, aims to create encrypted e-mail "easy enough for your grandma to use". See also their website https://www.darkmail.info/ and oddly more informative their contributions on crowdfunding website Kickstarter: https://www.kickstarter.com/projects/ladar/lavabits-dark-mail-initiative/posts

[148] Whitten et al (1999)

A completely different angle is the advantage of finding suspicious Internet traffic. With the current limited amount of E2EE usage the interesting encrypted mails, instant messages, voice traffic etcetera stand out in the crowd. They're probably the best place to dive deeper. See the study Part 1 for current capabilities on surveillance on both metadata and content.

If the E2EE technology is sufficiently available to users LE and intelligence also can profit from a false sense of security and look for mistakes/errors by users.

Disadvantages

First of all, E2EE offers possibilities for criminals and terrorists to hide the nature of their activities from LE and national security agencies.[149] Even with known suspects it might prove to be very difficult to obtain the content of their communications (and thus intentions, plans and actions).

Troels Oerting from Europol therefore recently stated that: *"The increasing trend towards greater encryption of online communications is not acceptable (...). Imagine in the physical world if you were not able to open the trunk of a car if you had a suspicion that there were weapons or drugs inside... we would never accept this. I think that should also count for the digital world. I hate to talk about backdoors but there has to be a possibility for law enforcement, if they are authorised, to look inside at what you are hiding in your online world.*" [150] His underlying statement is that "*privacy cannot equal anonymity*".[151]

In the same vein, FBI Director James Comey has urged the US Congress to force smartphone developers into building backdoors into all devices for law enforcement surveillance. He did so in response to new customer data encryption standards adopted by Apple and Google, that could hamper FBI surveillance efforts.[152] The proposal has been questioned, however, as there are doubts concerning privacy of US citizens and the competitive position of US vendors in Europe.[153]

For certain E2EE email tools, the service provider does not have the private keys to de-encrypt data and/or it is not located in a country which has the legal authority to obtain keys and/or user data. Paradoxically this then probably requires the monitoring agency to switch to targeted surveillance and as such a deeper breach of privacy.

However, content that lies with large email providers, even those with encryption facilities, are still within reach of government agencies if the provider also has the private key. A court order would probably be needed in most countries to get access to the required data.

Finally, secure email providers Silent Circle en Lavabit both closed down their e-mail services after the latter was ordered by a court of justice to hand over the key for user data. This has forced the business to come up with new concepts and a drive to keep their data *out of the hands* of Law Enforcement,

[149] See also Part 1 of this study, where it is stated that encryption is among the top 10 Internet challenges for law enforcement (according to the findings of the World Middle East 2014 conference Telestrategies).

[150] BBC.com 'Only 100 cybercrime brains worldwide, says Europol boss, http://www.bbc.com/news/technology-29567782, accessed 27 October 2014. In the

[151] See bbc.com (2014) and repeated during a key note speech on The Grand Conference 2014, November 6th in Rotterdam.

[152] Speech by James B. Comey, Director Federal Bureau of Investigation, Brookings Institution, Washington, D.C. October 16, 2014, http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (accessed on November 6th 2014). In the same sense Commissioner Bernard Hogan-Howe of the Metropolitan Police on November 6th 2014, see: http://content.met.police.uk/News/Commissioners-US-visit/1400027598397/1257246745756

[153] Macri, G. FBI Asks Congress For Backdoor Access To All Cellphones For Surveillance, 20 October 2014, http://dailycaller.com/2014/10/20/fbi-asks-congress-for-backdoor-access-to-all-cellphones-for-surveillance/ (accessed on 6 November 2014)

arguing that they otherwise lose the trust of those who fund their business.[154] In this way Law Enforcement successes also fuel (legitimate) innovations to better protect E2EE.

(iii) Commercial issues for service providers

Advantages

For commercial service providers E2EE offers no specific substantial advantages yet. There might be a business opportunity in offering encrypted email as a paid bonus option on (now still) free mail accounts.

User-friendliness and trustworthiness would be paramount though. For that reason some new initiatives, like Proton Mail and Ciphershed take residence and install servers in Switzerland to profit from the reputation and legal framework of that country.[155]

Disadvantages

With E2EE services providers lack access to content. This disrupts business models, certainly for currently free services ('mining free email' is a source of data for Google, Microsoft and others). 'If it is free, you're the product.'

Other business models are available, like paying for extra storage and/or per month, but many users are attracted to free.

Paid options still do not solve the issue that with encryption data enriching options like indexing, reformatting, filtering of user data are practically impossible. Providers like Facebook use this technique to present users with tailor-made timelines for instance.156 The overall service level and attractiveness decreases.

On the security side, E2EE might also hamper filtering spam, though there are other solutions to tackle spam (at telco's for instance).

In extreme cases pressure on service providers from Law Enforcement agencies to give access to encrypted user data can lead to shut-down of the company. The most notable example is Lavabit in 2013.

Lastly, If E2EE needs to be anonymity, then payment for services becomes an additional challenge for service providers. BitCoin and other cryptocurrencies offer a solution and so does cash

(iv) Intellectual property and copyrights for authors

Advantages

The primary advantage of E2EE for authors (in the broadest sense) lies in the protection of their content while stored or in transit. End-to-end encryption will secure Intellectual property (IP) as the IP will be sent in an encrypted form till it reaches the intended recipient, where it will be decrypted. So even if it is intercepted in the middle, it will not be possible to make sense of the encrypted data.

Disadvantages

[154] Levison, Ladar and Stephen Watt, Dark Mail, presentation on DefCon 22, 10 August 2014, http://www.youtube.com/watch?v=TWzvXaxR6us, accessed on 17 October 2014

[155] Forbes,' The Only Email System The NSA Can't Access', 9 May 2014, http://www.forbes.com/sites/hollieslade/2014/05/19/the-only-email-system-the-nsa-cant-access/, accessed on 17 October 2014, also https://protonmail.ch/, www.ciphershed.org

[156] Washington Post, NSA proof encryption exists. Why doesn't anyone use it?, 14 june 2013, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/

Enforcement of copyrights faces the same challenges as Law Enforcement. With encrypted content (and metadata) it is hard to check if measures (commonly known as digital rights management or DRM) that control access to copyrighted works are circumvented.

An example is the design of the new Mega website. Through HTML5, Mega utilizes in-browser, symmetric key encryption, making it impossible for the company to know or access what is being shared through Mega. This clearly shifts all piracy risks to users, Mega is just facilitating a Cloud storage service. By the way, user identifying data like usernames and IP are not encrypted, transferring all legal risks related to IP piracy to the users.

The example makes clear that with use of E2EE, service providers cannot share private keys, nor decrypt user data, if they do not have the private key. The copyright enforcer needs to have the private key to access the information, in order to prove copyrights are infringed.

(v) Technically

Advantages

Performance of hardware still improves in terms of clock speed, available memory etcetera. In the long run, with current encryption performance losses in mind, performance does not have to be an inhibitor. However, if file size or key size increase substantially too, performance might stay an issue.

Disadvantages

Research in 2013 showed that only 30% of respondents (business and IT managers) state that their organizations "extensively used" encryption technologies.[157] It turns out that despite the advantages, encryption (incl E2EE) definitely has some serious technical disadvantages.

Performance loss is the most noticeable issue with encryption. It does matter which encryption algorithm and hash technique are used. Other factors are the type of use (read/ write, part of database or all of it etc.), size of file, bitsize of encryption key et cetera. The numerous estimates found on loss of performance of specific encryption solutions range from small to substantial (80% or more).

The **complexity of implementation** (for instance key management) is another disadvantage. Without proper implementation E2EE will create a false sense of security. For instance a study in 2013 by HP[158] on 2,100 mobile applications of 600 Forbes Global 2000 companies revealed that still 18% did not use secure HTTP for more sensitive operations, such as logging in, and also 18% incorrectly implemented HTTPS or SSL. And 75 percent of applications did not use proper encryption techniques when storing data on mobile devices, even if 97% of all applications accessed privacy sensitive data on the mobile device, such as contacts or photos.

Individual (home or professional) users will require even more easy to use implementations than corporate, with a full-time IT management staff at hands.

Bringing **more standardization** to the encryption products is furthermore necessary. Some vendors159 are trying to solve this interoperability problem between encryption systems with the OASIS Key

[157] Ponemon (2014) Global Encryption Trends Study, https://www.thales-esecurity.com/knowledge-base/analyst-reports/global-encryption-trends-study, accessed on October 15,2014

[158] HP Security Research (2013) 'HP Research Reveals Nine out of 10 Mobile Applications Vulnerable to Attack,' http://www8.hp.com/us/en/hp-news/press-release.html?id=1528865#.U9lyJfldVPp , accessed on October 15,2014

[159] For instance Dell, IBM, Oracle, SafeNet, Thales e-Security and Vormetric

Management Interoperability Protocol (KMIP).[160] This is intended for streamlining and standardizing communications between encryption products.

Also there are technical challenges in obscuring ***metadata***.[161] One way is to encrypt Internet Protocols too . Another way can be found in DIME/Darkmail, where standard mail protocols are replaced by proprietary ones.

17.1. Conclusions

With proper installations on both sides of an encrypted communication channel E2EE does provide protection against mass surveillance, but only so far as the encryption goes. At one moment or the other the data has to be unencrypted to be read or written by a (human) user.

All in all E2EE provides and will continue to be a serious challenge for Mass Surveillance, but technology there also evolves. This will probably remain an arms race the coming years.

[160] Lemos, R. (2014) 'Keypocalypse' another barrier to encryption systems, http://searchsecurity.techtarget.com/feature/Keypocalypse-another-barrier-to-encryption-systems, accessed 4 November 2014

[161] See on metadata also Part 1 of this study, chapter 3.

18. E2EE in critical European network infrastructures

This annex pursues to provide answers to the following questions:

"Should critical European network infrastructures, such as for instance global private banking and credit card networks implement the use of "end-to-end" encryption between their customers?

What would the technological and organisational options to maintain law enforcement and/or national security preventive and reactive investigation capabilities in this context? How can it be done?

Is the concept of "key escrowing" a good and trustable one in practice?

What about data retention policies?"

18.1. Implementation of E2EE in critical European network infrastructures

Critical infrastructures are defined slightly different varying by country, but critical network infrastructures are traditionally understood to be communication, transportation and utility networks. In recent years, the understanding of these can be expanded to encompass new areas that have grown essential, such as online banking. These infrastructures are all under a high risk of cyber attacks, and higher scrutiny from governments in critical infrastructure programs.

18.1.1. Use of E2EE in Banking

For systems like banking systems, the business model is now almost completely online, and security is of the utmost importance. Banks and other financial institutions are at the forefront of cyber attacks aimed at extracting data or disrupting services[162]. The Target breach of 2013 was notorious for its magnitude and relative ease.[163] ENISA has published a report[164] detailing the numerous threats to online authentication in banking, including threats against end users, threats against devices, threats against networks and threats against remote banking services. According to research and advisory firm AITE, E2EE is the most appropriate technological route to reduce credit card fraud in the US.[165] Many industry experts agree that end-to-end encryption is the future of credit card security.[166]

Banks are, however, also at the forefront of securing their communications. At least in the European context, using tokens and chip cards for making online payments have been common for years. SWIFT, the underlying infrastructure for most bank payments in Europe, applies encryption to all data transmitted over its network.

In this sense, E2EE has been common for years, and security levels for payments are only increasing. However, the number of attackers and their sophistication levels are also rising, as demonstrated in real-life scenario's such as High Roller and Eurograbber.[167] The plethora of internet- or at least WiFi-

[162] Financial Times (2014), 'Experts warn banks of more cyber attacks', http://www.ft.com/cms/s/0/9de4a842-2ef6-11e4-a054-00144feabdc0.html, accessed on August 23, 2014

[163] Wall Street Journal (2014) 'Target Now Says 70 Million People Hit in Data Breach' http://online.wsj.com/articles/SB10001424052702303754404579312232546392464, accessed on August 2, 2014.

[164] ENISA (2014) 'eID Authentication methods in e-Finance and e-Payment services' http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/eIDA-in-e-finance-and-e-payment-services/at_download/fullReport, accessed Oct 3, 2014

[165] Aite (2010) 'End-to-End Encryption in Card Payments: An Introduction' http://www.aitegroup.com/report/end-end-encryption-card-payments-introduction, accessed on October 10, 2014

[166] Trustwave (2010), 'Trustwave Unveils End-to-End Encryption Software Solution', https://www.trustwave.com/Company/Newsroom/News/Trustwave-Unveils-End-to-End-Encryption-Software-Solution/, accessed on October 10, 2014

[167] ENISA (2014), pp. 20-21

enabled devices is a point of worry though, with more attention in security development aimed at it.[168]

The European Central Bank and ENISA have pointed specifically at the risks associated with 'Card-Not-Present' fraud.[169] Remote transactions of this type represent only 10% of payments, but over 50% of card fraud cases. In these cases, encryption is hardly used, however.

18.1.2. Use of E2EE in other critical infrastructures

Critical infrastructures like energy companies are developing more and more services like smart metering, and other smart appliances, which involve more (personalized) data being transmitted to and from customers. Security in Internet of Things (IoT)-applications for these types of companies is still in an early phase, but is increasingly a point of worry.[170] The use of security measures in this field is, at this point, largely a black box.

End-to-end encryption (E2EE) provides various benefits to merchants as well as consumers in the banking and financial services sector:

Benefits for consumers

For consumers, using encryption for infrastructure services provides enhanced security of sensitive card information – a credit card number is not enough anymore to authorize payments, as well as during online transactions (no-one can impersonate the person and make unlawful transactions).

Benefits for merchants

For merchants, encryption offers monetary savings by minimizing the cost and complexity of adhering to industry regulations and standards such as the Payment Card Industry Data Security Standard (PCI DSS). It is probably the single most important measure merchants can take to protect cardholder information such as primary account data (PAN). The process of E2EE provides great risk reduction, as even if a thief is able to intercept data in transit, it will be unreadable and therefore unusable.[171]

18.2. Technological and organizational options to maintain law enforcement and/or national security

End-to-end encryption of user communications poses a challenge to police forces and other law enforcement agencies throughout the world, as its use is likely to nullify the capacity to intercept data before the entry point. They do, however, have ample possibilities for targeted surveillance of banking, telecommunications or other data. For example, the Australian Security Intelligence Organization (ASIO) is pushing for laws that would make telecommunications companies retain their

[168] The Inquirer (2014) 'Intel claims IoT encryption tool will make payment transactions more secure' http://www.theinquirer.net/inquirer/news/2376030/intel-claims-iot-encryption-tool-will-make-payment-transactions-more-secure, Accessed October 27, 2014

[169] European Central Bank (2013) 'Recommendations for the security of internet payments', available at http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf , accessed Oct 3, 2014 and ENISA (2014)

[170] Information Week (2014), 'HP Warns Of IoT Security Risks' http://www.informationweek.com/cloud/software-as-a-service/hp-warns-of-iot-security-risks/d/d-id/1297617, accessed on October 3, 2014.

[171] First Data (2009) 'Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance', https://www.firstdata.com/downloads/thought-leadership/fd_encrypt_token_pci_whitepaper.pdf , accessed on October 10, 2014

customers' web-browsing data, as well as force web users to decrypt encrypted messages.[172] Additionally, the agency is calling for enhanced powers to sift intelligence data from emails and social media sites, as well as forcing web users to decrypt encrypted material if requested to do so by the spy agency.

The options for mass surveillance of encrypted (payment) files are quite minimal, unless there is a way to systematically undermine these. One of those ways could be key escrow:

Key Escrow

The idea of key escrow is to place the keys needed to decrypt encrypted data in the hands of an authorized third party. The US government pushed for a key escrow system in the pre-dotcom era (1990s).[173] The idea was to allow law enforcement agencies to have the ability to decrypt encrypted information, provided they had the necessary court order. However, the tech community and companies weren't comfortable with the government having this ability. Also, there were technical problems with the proposed mechanism at the time. The use of key-recovery-based encryption infrastructures to meet law enforcement's stated specifications, in the view of many security professionals, undermines the security of encryption as a whole and increase costs to the end-user. Building the secure infrastructure according to requirements would be extremely complex. Even if such infrastructures could be built, the risks and costs of such an operating environment may eventually prove unacceptable. In addition, these infrastructures would generally require extraordinary levels of human trustworthiness.[174]

18.3. Data retention policies

A data retention policy is an organization's policy on the retrieval, use, and disclosure of message and traffic data. Companies have these in order to comply with legal and their own requirements regarding data recovery and archiving. Obviously, due to the confidential nature of the communications involved, a high threshold for accessing the stored information is needed.

The Court of Justice of the European Union in 2014 declared the European Data Retention Directive to be invalid, as it entailed a wide-ranging and serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary. [175]As part of improved risk management due to the increased risk of data loss, some organizations are trying to minimize the risk of losing data by simply only storing data that is necessary for service provision. This tailoring, or only verifying when it is necessary, also can be accomplished by using more 'attribute-based' identifying.

18.4. Conclusion

The use of end-to-end-encryption in some critical network infrastructures, such as banking, is at a very high level. Especially in Europe, standards for securing payment and transaction information are usually encrypted, and credit card payments based on only card numbers are rare. However, the number and level of sophistication of attacks is increasing, as is the damage caused. **Requiring the use**

[172] RT (2014) 'Spy agencies seek to store Aussies' web-browsing histories, end encryption' http://rt.com/news/australia-nsa-snowden-surveillance-510/, accessed on July 13, 2014

[173] Martin, Luther (2010), 'Key recovery vs. key escrow', http://www.voltage.com/blog/crypto/key-recovery-vs-key-escrow/ , accessed on July 13, 2014

[174] Schneier, Bruce (1998) 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' https://www.schneier.com/paper-key-escrow.html, accessed on July 13, 2014

[175] Court of Justice of the European Union (2014) 'The Court of Justice declares the Data Retention Directive to be invalid' http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf, accessed on July 13, 2014

of E2EE for all online banking and card transactions within Europe is the most certain way to allow payments to go forward unhindered. The laws of member states will still allow for the targeted access to transaction data, if required for law enforcement or intelligence purposes.

19. E2EE protocols for Email and instant messaging

This annex pursues to provide answers to the following questions:

"Why are "end-to-end" encryption protocols developed for Email (PGP) and instant messaging (OTR) not more extensively used in Europe today?

What could be envisaged to further increase their adoption? Is it feasible?"

In the past articles like 'Why Johnny Can't Encrypt'[176] have pointed us to some important reasons why E2EE is not used more for email and instant messaging. The conclusion was that mainly the lack of user-friendliness gets in the way. In this annex we'll discuss this and other valid reasons why E2EE is not more extensively used (in Europe or indeed at all). After that we explore options to increase their adoption, by circumventing some of the barriers identified.

19.1. Why are "end-to-end" encryption protocols for Email and instant messaging not more extensively used today?

There are several valid reasons[177] why E2EE is not used extensively for person to person communication by email or instant messaging. Based on our research we divide these reasons into different categories:

1. Technological
2. Psychological
3. Social
4. Political
5. Financial

19.1.1. Technological

User-friendliness of available tools

Consumers in most cases choose convenience and usability over security. Thus far many popular options for email or instant messaging put an emphasis on user-friendliness and not on security or privacy. The lack of user-friendliness is a classic theme to explain why E2EE is not used more extensively. "*PGP is not usable enough to provide effective security for most computer users*" [178], meaning that using PGP is so burdensome that even those with a strong desire for safe communication resist its use.

E2EE creates other problems for users as well. Conventional online services have processes for people to generate new passwords in case they forget the previous ones. This is possible because the service providers have access to unencrypted data. However, in the case of E2EE, if the password is lost it means losing all the data in the user's account.

Also, encryption is only effective if one is actually communicating with the party one intends to. It can happen that a malicious party imitates the intended recipient and convinces the user to share sensitive

[176] Whitten, Alma and J. D. Tygar (1999) 'Why Johnny Can't Encrypt' in Security and Usability: Designing Secure Systems that People Can Use, eds. L. Cranor and G. Simson. O'Reilly, pp. 679-702

[177] Most of them apply to Europe and the rest of the world. Only where necessarily we will make a distinction between Europe and other parts of the World.

[178] Soghoian, Christopher (2009) 'Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era', 8 Journal on Telecommuncations and High Technology Law 359; Berkman Center Research Publication No. 2009-07. http://www.jthtl.org/content/articles/V8I2/JTHTLv8i2_Soghoian.PDF, accessed on July 13, 2014

data. To prevent this imitation, the sender and recipient need to be able to verify each other's identities. However, this process of verification tends to be cumbersome. Even those who are willing to make the effort can make errors that lead to security lapses. Such security is useful only if other concerned people are employing it as well. Even people who have set up PGP usually send plaintext emails, as recipients often do not have the ability to receive encrypted email (interoperability issues[179]). Thus, people have a tendency to make use of what is already available on their computers.[180]

19.1.2. Psychological

It is, however, not just user-friendliness that prohibits users from adopting E2EE for their email or instant messaging. Research by the universities of Glasgow and Darmstadt reveals that several other more psychological explanations are valid.[181] This paragraph builds on their work as it is quite extensive, including both live assessments and desk research.

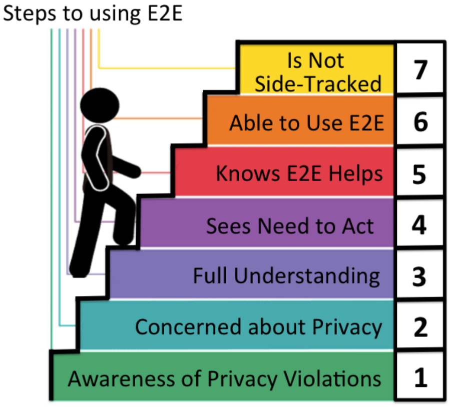


Figure Progression Towards E2E Encryption Deployment (source: Renaud et al. 2014)

The study found the following reasons for not using E2EE validated:

1. Users do not have any awareness of practical privacy issues. Other cyber related risks (like loss of a device) may be more top of mind, if such risks are part of a conscious consideration at all. A generic (theoretical) sense of privacy protection may be there, but it turns out that people offer a bit of their privacy for as little as a bit of chocolate.[182]
2. Users are aware of the possibility of privacy violation of their emails but do not take any action, perhaps because they are not concerned. Either they feel they have nothing to hide, it does no harm, they are not important enough to be noticed, or users consider their private email not as sensitive as their business email. Also, users may assume that security of email is someone else's responsibility (like the email provider) and hope that security is already taken care of. This also applies to the workplace, where employees may consider email security a job for the IT department.
3. Users may know that the privacy of their emails can be violated at client-side, but not that this can happen in transit or at the mail server side too. They may subsequently attempt to protect against client-based threats (like antivirus, locking desktops or strong passwords), but do not use E2EE. It is our estimate that most users lack a deep understanding of how the e-mail

[179] Renaud K. Et al., Why Doesn't Jane Protect Her Privacy?, paper for The 14th Privacy Enhancing Technologies Symposium, Amsterdam 2014

[180] Lee, Timothy B. (2013) 'NSA-proof encryption exists. Why doesn't anyone use it?'http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/, accessed on October 10, 2014

[181] Renaud K. Et al. (2014)

[182] Acquisti, A., Grossklags, J., Privacy and rationality in individual decision making. IEEE, Security & Privacy 2, 24–30 (2005)

infrastructure works. Especially for the youngest generation email or messaging or any other form of e-communication is something 'that's there'. Without a proper understanding of the workings of the underlying infrastructure (and the lack of tools that take over that understanding easily) it is much harder to take proper action.

4. Users may know that email privacy can be violated at different stages (client side, in transit, server side) but they fail to see the need to act. That might be because users either think they cannot counter the threat (hackers will get in or email providers will be collecting data), or because users accept the (in their eyes legitimate) reasons why emails are read by third parties. Targeted advertisements, access for national security reasons and network protection can for different groups of users be acceptable reasons for tapping into mail conversations.
5. Given the purpose of this study, that is somewhat startling and requires more quantitative research. How large is the group of users in Europe that actually accepts mass surveillance on their email or instant messaging when it is in the interest of national security?
6. Users may want to prevent violation or privacy but they do not know how to, i.e. that they should use E2EE. They lack the knowledge, or have only partial knowledge about E2EE advantages, good tools and ways to use them. If it is known and easy enough, a E2EE tool might be applied. At least they might consider it among other easier options (like not using email, or splitting content between media etc.).
7. Finally users understand that they can use E2EE to prevent privacy violation, but for some practical reason they are not able to. This links even stronger to user-friendliness and complexity of E2EE solutions. If it is too complex to use, motivation will be low. A better user interface design, help function or support desk and ease of use all will lower this barrier to some extent.

The mindset of individual users thus offers plenty of reasons not to use E2EE, ranging from lack of awareness to lack of skills. [183]

19.1.3. Social

Some individual users do not use E2EE, even if they understand that they can use E2EE to prevent privacy violation and technically able to. In some organizations employees did have the knowledge, skills and tools, but still did not encrypt all email.[184] One of the reasons identified was that employees considered it paranoid to encrypt all emails, which suggests a social element into their individual decision-making.

19.1.4. Political

In terms of practical blockades, prohibition to use encryption may hamper widespread use. Some countries (outside Europe) forbid the ownership and use of encryption tools, or may require a specific permit (some Asian countries).[185]

19.1.5. Financial

We have not found any evidence that says that the financial cost of E2EE tools prevents users to adopt them. In fact many of them are (near) free.[186] However it is difficult to calculate the cost of security and

[183] A practical experiment with appr. 20 consultants, witnessed by authors, produced more or less the same array of reasons.

[184] Gaw, S., Felten, E.W., Fernandez-Kelly, P.: Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In: Proceedings of the SIGCHI conference on Human Factors in computing systems. pp. 591–600. ACM (2006)

[185] A detailed research into the legal frameworks regarding encryption was not part of this study.

[186] Also see the options already available for E2EE email / instant messaging in Part 1, most of them are (nearly) free.

privacy breaches, let alone the business case of security measures. For larger implementations (e.g. for all employees of a company) this will play a role in decision-making.

19.2. Possible steps to increase adoption

The barriers mentioned also provide hints as to what should be addressed to spread the use of E2EE. In this paragraph we tackle the most favourable. Note: we found no solution that automatically will lead to mass use of E2EE. A combination of actions and a long term vision are required.

19.2.1. Increase user-friendliness

The design and user-interface of software such as PGP needs to be made more user-friendly, so that even people who do not have any knowledge of encryption or cryptography can use it. Since the design needs of such software are different from that of general software for end-users, it also requires separate usability evaluation methods to test whether the security priorities have been met. To design appropriate tests, one could look at other fields where there is an established liability for consumer safety; as these fields are likely to already have a body of research on how best to establish whether product designs successfully promote safe modes of use.[187]

A body of publicly available work on usability evaluation from a security context would be helpful, and it will most likely have to come from research sources.

The need for more user-friendly tools has fed development of new tools like DIME/Darkmail, Silent and Protonmail (see also Part 1 of this study). It also has spurred action of large service providers (see below).

19.2.2. Raise awareness and knowledge

There is apparently also a need to communicate an accurate conceptual (though simple) model of security to the user for better understanding of how email and instant messaging work and what the risks are. Easy to understand instructions on an easy to find and authoritative website help raise knowledge and thus lift one of the barriers identified.

From a technology point of view it is hard to see how convictions and mental calculations on the trade-off between privacy and other benefits can be influenced. This is more the field of psychology.

19.2.3. Collective implementation to overcome lack of awareness and deep knowledge

When users are not aware of a need to or not capable of implementing sufficient protection, service providers can offer a collective solution, unburdening the users (who will use what's on their computer anyway). Examples are already available. Google has introduced a Chrome extension earlier in 2014, called End-to-End, which uses OpenPGP and can be used by people requiring extra security or for sensitive emails. Using the extension, anyone can send and receive end-to-end encrypted e-mail through their existing web-based email provider.[188] Stats on E2EE usage[189] indicate that iCloud and me.com email-services also use E2EE.

[187] Whitten, Alma and J. D. Tygar (1999) 'Why Johnny Can't Encrypt' in Security and Usability: Designing Secure Systems that People Can Use, eds. L. Cranor and G. Simson. O'Reilly, pp. 679-702

[188] Rosenblatt, Seth (2014) 'New Chrome extension hopes to demystify encryption' http://www.cnet.com/news/new-chrome-extension-hopes-to-de-mystify-encryption/, accessed on July 13, 2014

[189] As found on http://www.google.com/transparencyreport/saferemail/ (accessed 7 November 2014)

This collective approach by service providers does increase protection against cybercrime. It does not eliminate the possibility of mass surveillance, unless the service provider does not have the keys to de-encrypt.

19.3. Conclusion

There is an overwhelming number of sometimes even convincing reasons why E2EE is not adopted more extensively. The lack of awareness and deep understanding of the technical email and messaging infrastructure inhibit users to take the right technical measures.

The measures to increase adoption try to tackle these barriers: raise awareness and level of knowledge, increase user-friendliness of options offered and promote collective solutions in which service providers take up the responsibility to make emailing and messaging more secure.

The latter option offers the most benefits in the short term and given the barriers identified also in the long run, but do not offer 100% protection against state sponsored mass surveillance. As is shown elsewhere, public pressure from Law Enforcement agencies across the world to keep backdoors and front doors open despite the increased use of encryption is already visible. This issue is therefore likely to remain the primary grounds for contention with regards to mass surveillance.

20. Privacy in GSM networks

This annex pursues to provide answers to the following questions:

"Do the GSM operators in Europe use "end-to-end" encryption over their voice radio networks (TETRA protocol) or are they in a position to decrypt all communications of their customers?
How can a user protect his/her privacy over a standard GSM network using specific commercial solutions to prevent GSM operators from decrypting its conversations? Is it feasible at a reasonable price?
Can these commercial solutions be implemented on a large scale for all customers of a given operator? Can they be developed independently of the operator?"

20.1. GSM operators in Europe

GSM security was designed in the 1990's. It only provided a limited level of confidentiality of the wireless link and authentication of the phones towards the mobile network. Because telecom equipment was very expensive at that time, not much research was done into the security of GSM. Many years later, reprogrammable phones came on the market and open-source GSM telephony software was developed[190] the interest in the (in)security of GSM increased.

Mobile networks usually do provide end-to-end security to its users. In the standard form it is defenseless against many attacks and fails to ensure strict safety of the user's telephone conversations and data transfer sessions. In GSM (2G) networks, only the radio link between the mobile phone and the base station is encrypted whereas the rest of the network transmits data in clear-text and can intercepted.[191] For UMTS the call is encrypted between the phone and the Radio Network Controller (RNC), which is still far from end-to-end encryption.

The encryption on GSM (2G) network that is used most for speech and SMS is 'A5/1'. A5/1 encryption is considered weak[192], and can be intercepted with a reprogrammable phone with open source software.[193] Encryption can be turned off (A5/0) by attackers, which is quite hard to detect for a user. Some operators have started to implement a newer encryption algorithm A5/3. This makes it much harder to intercept communication and to decrypt it. UMTS uses a better encryption algorithm than GSM for providing confidentiality. With GSM the network can only authenticate the phone (mainly for billing purposes). With UMTS the phone can also authenticate the network, preventing man-in-the-middle attacks. However this optional and not all mobile network operators (MNO) turn this option on. Because average customers are not aware of these options and how MNOs use them, they cannot make an informed decision about which mobile network to use. It also does not give MNOs an incentive to make their networks more secure for their customers. They only have an incentive to make it secure for billing purposes.

[190] osmocom.org, accessed November 1st, 2014. The Osmocom project is a family of projects regarding Open source mobile communications. It includes software and tools for a variety of mobile communication standards, including GSM, DECT, TETRA and others.

[191] Kulkarni, Mandar M. et al (2013) 'Encryption Algorithm Addressing GSM Security Issues- A Review', International Journal of Latest Trends in Engineering and Technology (IJLTET) Vol. 2

[192] Stackexchange (2013) 'Are phone calls on a GSM network encrypted?' http://security.stackexchange.com/questions/35376/are-phone-calls-on-a-gsm-network-encrypted, accessed on July 13, 2014

[193] GOVCERT.NL (2010) 'FACT SHEET FS 2009-05 Eavesdropping on GSM-communications' https://www.ncsc.nl/binaries/en/services/expertise-advice/knowledge-sharing/factsheets/factsheet-regarding-eavesdropping-on-gsm-communications/1/Factsheet%2BEavesdropping%2Bon%2BGSM%2Bcommunications.pdf, accessed on July 13, 2014

There are big differences between MNOs in Europe. See gsmmap.org for a worldwide overview of MNOs and how well they perform regarding interception, impersonation and tracking. GSM and UMTS protocols do not provide end-to-end encryption. It can be provided on top of these protocols, however MNOs in general do not offer end-to-end encryption. Because the communication on their internal networks in the clear, operators can store this communication and even provide access to law enforcement. This weakens the security of the whole because not only law enforcement can use this intercept interface. This (lawful intercept) interface is very interesting for national security agencies, criminals and hackers.

20.2. Protecting privacy over GSM networks

A German SIM card manufacturer has announced that it will be supplying Vodafone Germany with an end-to-end security system based on the phone SIM. The service will not be offered to individual subscribers but will be available through corporate and government sales and it enables secure voice calls. No price has been given for the secure SIM solution, but the firms hint at it being reassuringly expensive. Vodafone Germany has also announced a lower cost secure voice service aimed at individual consumers.[194]

GSM SecureVoice provides a VoIP (Voice over Internet Protocol) solution which makes End-to-End encryption possible. There are numerous subscription plans for different durations starting at 55$ for 3 months.[195] Although there are standards for encrypting communication over GSM, this is hardly used in the public domain, e.g. SCIP [196] SCIP specifications are not widely used and no public implementation is available. The TalkSECURE™ Wireless phone provides end-to-end high assurance secure voice and data communications for commercial GSM wireless networks operating in the 900/1800/1900 MHz bandwidths worldwide.[197]

GSMK Cryptophone G10, developed by GSMK (a German company in the field of mobile voice and message security) provides strong end-to-end voice encryption to individuals, corporations, and institutions.[198] Certain smartphones can run software for encrypting voice communication. The security of such communication not only depends on the encryption itself but also on the security of the smartphone itself. RedPhone (an Android app) is a free and open-source program that offers secure and encrypted calls. It uses WiFi or a data plan rather than the radio phone service. The end user has the advantage that MNOs do not get access to the metadata of the calls.[199]

20.3. Large-scale implementation of solutions

A few of the solutions to protect user privacy and provide end-to-end encryption, such as Android/iOS apps like RedPhone/SilentCircle can possibly be implemented on a large scale, given that the user's phone satisfy the minimum requirements.

[194] The Register (2014) 'Vodafone Germany looks to provide end-to-end encryption with SIM signatures', http://www.theregister.co.uk/2014/03/11/vodafone_germany_takes_g_and_d_secure_sim/, accessed on July 13, 2014

[195] http://www.securevoicegsm.com/encrypted-voip-calls/, accessed on July 13, 2014

[196] http://en.wikipedia.org/wiki/Secure_Communications_Interoperability_Protocol

[197] http://www.aosusa.com/wp-content/pdf/products/sectera/talksecure_wireless.pdf, accessed on July 13, 2014

[198] http://www.cryptophone.de/en/company/, accessed on July 13, 2014

[199] Neal, Ryan (2013 'PRISM-Proof Your Smartphone: 10 Apps To Keep The NSA Out Of Your Phone', http://www.ibtimes.com/prism-proof-your-smartphone-10-apps-keep-nsa-out-your-phone-1321085, accessed on July 13, 2014

20.4. Conclusion

Mobile phones are an important part of our society. In the past the fixed phone lines (or Public Switched Telephony Network, PSTN) was never encrypted. For GSM only the wireless part was encrypted and for UMTS some, but no more than that. Conversations can easily be intercepted on a large scale, because of a lack of end-to-end encryption. Some additions are available but are not being used on a large scale.

21. IPSec versus SSL-based VPN "end-to-end" encryption protocols

This annex pursues to provide answers to the following questions:

"What are the advantages and disadvantages of using IPsec versus SSL-based VPN "end-to-end" encryption protocols for establishing secure communications between two users over the Internet?

Is one protocol more compromised or secure than the other?

What is the expected long term evolution of these two protocols?"

21.1. IPSec versus SSL-based VPN

There are two types of VPNs. The first is a Site to Site VPN (home, office, mobile, Cloud etc.) and other is individual remote access VPN. For Site to Site VPN, IPSec is the best way today. For individual Remote access usually VPN based on TLS (SSL 1.0 and 2.0 are considered obsolete – we therefore call this type of VPN "TLS-VPN").

IPSec VPNs protect IP packets exchanged between remote networks or hosts. An IPSec gateway is always located at the edge (perimeter) of a private network. SSL[200] VPN products protect application streams from remote users to a TLS gateway. In other words, IPSec connects hosts to entire private networks, while TLS VPNs connect users to services and applications inside those networks.

IPSec VPNs can support all IP-based applications (to an IPSec VPN product, all IP packets are the same). TLS VPN application services vary, because each product has its own way of presenting client interfaces through browsers, relaying application streams through the gateway, and integrating with destination servers inside the private network.

Most TLS VPNs provide secure access to Microsoft Outlook Webmail, network file shares and other common business applications. However, they often require custom development to support non-browser-based apps

IPSec employs Internet Key Exchange (IKE), using digital certificates or pre shared secrets for two-way authentication. SSL(or TLS) Web servers always authenticate with digital certificates, no matter what method is used to authenticate the SSL client.

Both support certificate-based user authentication, though each offers less expensive options through individual vendor extensions. TLS VPN is the more secure solution for companies that decide to implement non-certificate user authentication.

IPSec vendors, for example, offer alternatives such as Extended Authentication (XAUTH) and L2TP over IPSec. However, XAUTH, which is frequently deployed using pre-shared group certificates and DHCP, is vulnerable to several known attacks.

SSL/TLS vendors support passwords and tokens as extensions. Further, SSL/TLS's encrypted tunnel protects the user's identity and credentials, making asymmetric authentication more secure than IPSec with XAUTH.

IPSec standards support "selectors"-packet filters that permit, encrypt or block traffic to individual destinations or applications. However, in practice they grant hosts access to entire subnets, rather than keep up with the headaches of creating/modifying selectors for each IP address change or new app.

[200] When we say SSL here, we refer to TLS based VPN as well. In most cases older SSL 1.0 and 2.0 versions have been substituted by TLS as security mechanism (TLS 1.0 corresponds to SSL 3.0).

TLS VPN products tend to provide more granular tools because they operate at the session layer, TLS VPNs can filter on and make decisions about user or group access to individual applications (ports), selected URLs, embedded objects, application.

SSL/TLS is better suited for scenarios where trust is limited or where installed certificates are infeasible--business partner desktops, public kiosk PCs and personal home computers.

Both TLS and IPSec support block encryption algorithms like TripleDES Cipher Block Chaining, which are commonly used in VPNs. TLS VPNs also support stream encryption algorithms like RC4 that are often used for Web browsing. Given comparable key lengths, block encryption is less vulnerable to traffic analysis than stream encryption.

21.2. Is one protocol more compromised or secure than the other?

21.2.1. Protection against frequent attack patters

Man-in-the-middle attacks

IPSec provides a certain level of protection against man-in-the-middle attacks as it prevents packet modification. However, this strong security feature also generates operational problems. Given an up to date implementation of TLS[201], the TLS VPN is almost as resilient against man-in-the-middle attacks, without IPSec's NAT conflict. SSL rides on TCP, so it is insulated from IP and port modifications, and thus passes easily through NAT. SSL carries sequence numbers inside encrypted packets to prevent packet injection, and TLS uses message authentication to detect payload changes.

Message replay

Both IPSec and TLS use sequencing to detect and resist message replay attacks. IPSec is more efficient, because it discards out-of-order packets lower in the stack in system code. In TLS VPNs, out-of-order packets are detected by the TCP session engine or the TLS proxy engine, wasting more resources before they are discarded. This is one reason why IPSec is broadly used for site-to-site VPNs, where processing power is critical to accommodate high-volume, low-latency needs.

Denial of service

IPSec has a slight advantage against (D)DoS attacks, such as packet floods, because it uses only datagrams, while TLS uses TCP sessions. This is because IP and UDP (IKE) datagram floods are conceptually easier to deflect than TCP SYN floods, which fill session tables and cripple many off-the-shelf protocol stacks.

21.2.2. Overall security comparison

SSL VPNs can provide the same user experience as IPSec VPN—but with less management complexity and greater control. In terms of security it is firstly a matter of practical implementation which solution is more secure. Theoretically and if done correctly IPSec is more secure because it is done at a lower level on the OSI Stack, at a Network Packet level.

It is really challenging however to configure IPSec at a granular level and much more easy to have granular control at the TLS VPN at the session layer. So from a practical purpose if done correctly TLS can be made secure more easily.

IPSec options are furthermore generally more vulnerable than the TLS alternatives in the case of user authentication (using the non-certificate option). IPSec vendors offer alternatives such as Extended Authentication (XAUTH) and L2TP over IPSec. However, XAUTH is vulnerable to several known attacks. And L2TP isn't broadly supported by VPN gateways or used by non-Microsoft shops. On the

[201] Currenty the minimum requirement is TLS 1.2 + patches for the Heartbleed attack

other hand, TLS's encrypted tunnel protects the user's identity and credentials, making it more secure than IPSec with XAUTH. Thus, TLS is almost as resilient against cyber attacks, without IPSec's operational problems.

21.3. Evolution: Software Defined Perimeters

Long term the current network architecture (network physical device based) will probably give way to more flexible and secure Software Defined Networks (SDN) or Software Defined Perimeters (SDP). SSL/TLS-based VPN and IPSec are both still in essence based on perimeter concepts: there is a world within and outside the (corporate) IT network. That perimeter model is becoming obsolete however:

1. Hackers can gain access to devices inside the network perimeter (for example via phishing attacks) and attack application infrastructure from within. This vulnerability continues to increase as the number of devices inside the perimeter grows due to BYOD, on-site contractors, and partners.
2. Traditional data center infrastructure models are being supplemented with external resources such as BYOD, Software as a Service and other Cloud services. Subsequently, networking equipment used for perimeter security is topologically ill-located to protect applications and the data used.

The approach of Software Defined Perimeter (SDP) addresses these issues by giving application owners the ability to deploy (dynamic) perimeters that are still invisible and inaccessible to outsiders, but can be deployed anywhere – on the Internet, in the Cloud, at a hosting center, on the private corporate network, or across these locations.

SDP evolved from work done at the Defense Information Systems Agency (DISA).[202] Connectivity in a Software Defined Perimeter is based on a need-to-know model, in which device status and identity are verified before access to application infrastructure is granted. The infrastructure cannot be detected, without visible DNS information or IP addresses. In 2013 the Cloud Security Alliance came up with a commercial concept for SDP.

SDP protects against a wide range of network attacks: DDoS, Man-in-the-Middle, XSS scripting, server scanning, SQL injection and many others.[203]

Basically SDP works with three different entities:

1. the *Initiating Host* (could be a user application on a mobile device, in the office or at home). The Initiating Host communicates with the SDP controller to request a list of A*ccepting Hosts* to which they can connect. The Controller may request information such as hardware or software inventory from the Initiating Host before providing any information.
2. the *SDP Controller*, that determines which SDP hosts can communicate with each other. The Controller may relay information to external authentication services such as attestation, geo-location, and/or identity servers.
3. *Accepting Hosts* hold the data or functionality the user is trying to reach. Accepting Hosts reject all communication from *all* hosts other than the SDP Controller. The Accepting Host connects only at the request of the Controller.

[202] Department of Defense, Global Information Grid Architectural Vision, 2007.

[203] https://en.wikipedia.org/wiki/Software_Defined_Perimeter

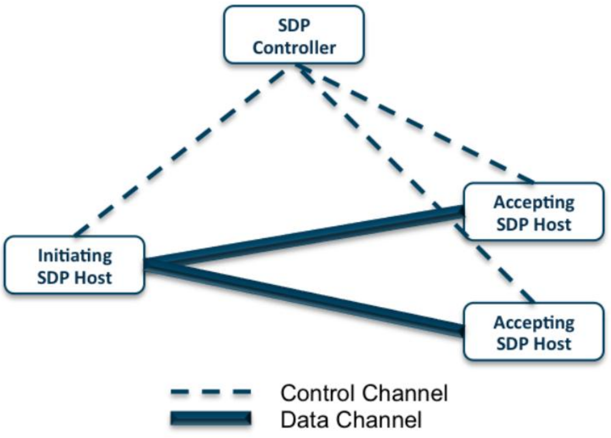
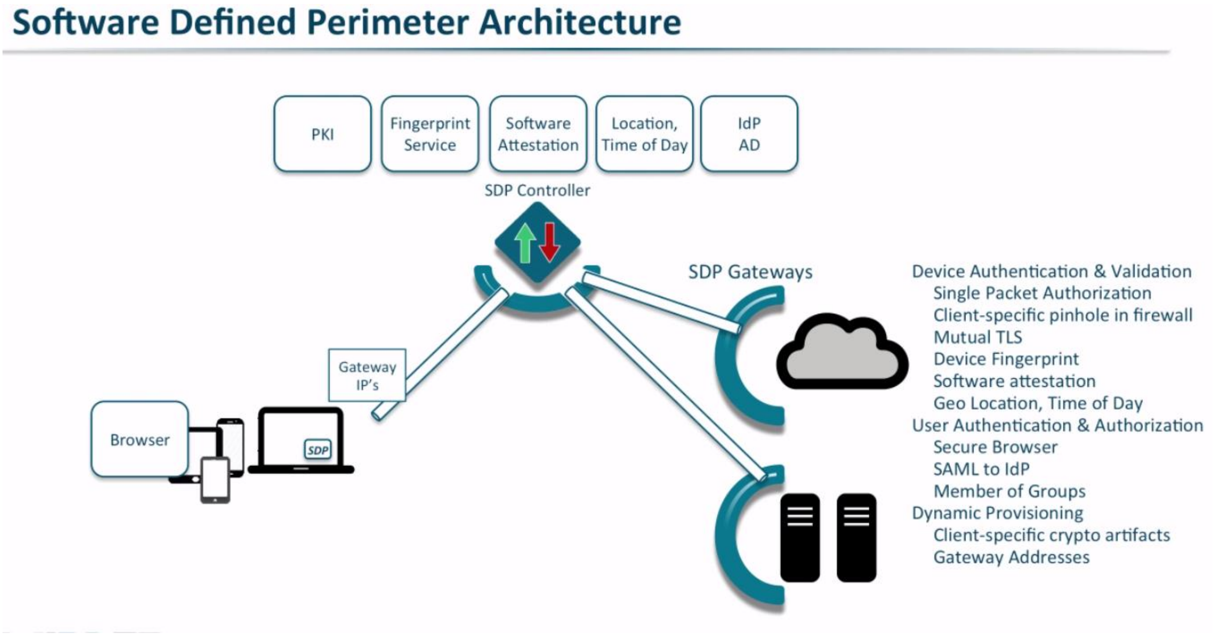


*Figure 1: The architecture of the Software Defined Perimeter consists of two components: SDP Hosts and SDP Controllers (source: Cloud Security Alliance Software Defined Perimeter Working Group, Software Defined Perimeter, December 2013)_*

The traditional networking model provides visibility and connectivity within the network and then adds a number of point controls to prevent access from non-trusted systems. SDP aims for no visibility and no connectivity, only establishing connectivity after end points prove they can be trusted.


Software Defined Perimeter Architecture

Device Authentication & Validation
- Single Packet Authorization
- Client-specific pinhole in firewall
- Mutual TLS
- Device Fingerprint
- Software attestation
- Geo Location, Time of Day

User Authentication & Authorization
- Secure Browser
- SAML to IdP
- Member of Groups

Dynamic Provisioning
- Client-specific crypto artifacts
- Gateway Addresses

Figure: overview Software Defined Perimeter architecture (source: video Software Defined Perimeter Protocol, on Vidder.com)

SDP utilizes five layers of security controls[204]

The software-defined perimeter architecture consists of five layers of security controls: single packet authorization (SPA), mutual transport layer security (mTLS), device validation, dynamic firewalls, and application binding.

[204] Based on Cloud Security Alliance – Software Defined Perimeter Working Group, SDP Hackathon Whitepaper, April 2014

Single Packet Authorization (SPA)

One of the primary objectives of the Software Defined Perimeter is to make the application infrastructure undetectable, showing no domain name system (DNS) information or IP addresses. Single packet authorization (SPA) enables the Software Defined Perimeter to reject all traffic to it from unauthorized devices. It requires that the first packet to the controller cryptographically verifies that it is an authorized device before being considered for access to the protected service. If visibility is granted, SPA is utilized again to enable the gateway to identify the traffic coming from authorized users and reject all other traffic.

Mutual Transport Layer Security (mTLS)

Transport layer security (TLS) was designed to provide device authentication prior to enabling confidential communication over the Internet. The standard was originally designed to provide mutual device authentication. However, in practice, TLS is typically used to authenticate servers to clients, and less from clients to servers. The Software Defined Perimeter uses the full TLS standard to provide mutual, two-way cryptographic authentications, also from client to server.

Device Validation (DV)

Mutual TLS proves that the device requesting access to the software defined perimeter possesses a private key that has not expired and that has not been revoked, but it does not prove that the key has not been stolen.

Device validation proves that the key is held by the proper device. In addition, device validation attests to the fact that the device is running trusted software and is being used by the appropriate user (for instance based on geo-location or time of day).

Note: all of this does require extensive identity and access management efforts.

Dynamic Firewalls

Usually firewalls use static configurations to limit incoming and outgoing traffic based on the address information in the IP packet (based on the quintuplet of protocol, source IP address and port, and destination IP address and port). This can lead to dozens to thousands of firewall rules.

D**ynamic firewalls** turn this concept around, having only one firewall rule: deny all. Communication with each device is *individually enabled* by dynamically inserting "Permit <IP quintuplet>" into the firewall policy. In the SDP architecture, gateways incorporate this dynamic firewall security control. SDP dynamically binds users to devices, and then dynamically enables those users to access protected resources by (dynamically) creating and removing firewall rules in the SDP gateways.

Note: this means the user has to be known to the application infrastructure manager, and cannot be anonymous.

Application Binding (AppB)

After authenticating and authorizing both the device and the user, the software defined perimeter creates encrypted TLS tunnels to the protected applications. Application binding constrains authorized applications so they can only communicate through those encrypted tunnels, and, simultaneously, blocks all other applications from using those tunnels.

This puts SDP in between the majority of security solutions presented in this study (being focused on OSI layers) and Jericho-like concepts focusing on data.

The workflow - how does SDP work?

The SDP framework has the following workflow:

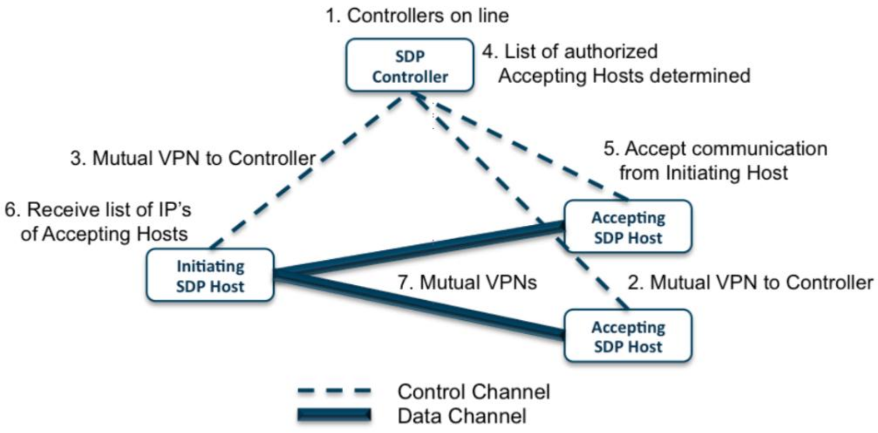

1. Controllers on line
SDP Controller
4. List of authorized Accepting Hosts determined
3. Mutual VPN to Controller
5. Accept communication from Initiating Host
6. Receive list of IP's of Accepting Hosts
Accepting SDP Host
Initiating SDP Host
7. Mutual VPNs
2. Mutual VPN to Controller
Accepting SDP Host
Control Channel
Data Channel

Figure 2: Workflow of the architecture of the Software Defined Perimeter (source: Cloud Security Alliance - Software Defined Perimeter Working Group, Software Defined Perimeter, December 2013)

1. One or more SDP Controllers are brought online and connected to the appropriate optional authentication and authorization services (e.g., PKI, device fingerprinting, geolocation, SAML, multifactor authentication, and others).
2. One or more Accepting SDP Hosts are brought online. These hosts connect to and authenticate to the SDP Controllers. However, they do not acknowledge communication from any other (potentially initiating and accepting) Host and will not respond to any non-provisioned request. That way they stay invisible for third parties.
3. Each Initiating SDP Host that is brought on line connects with, and authenticates to, the SDP Controllers.
4. After authenticating the Initiating SDP Host, the SDP Controllers determine a list of Accepting Hosts to which the Initiating Host is authorized to communicate.
5. The SDP Controller instructs the Accepting SDP Hosts to accept communication from the Initiating Host as well as any optional policies required for encrypted communications.
6. The SDP Controller gives the Initiating SDP Host the list of Accepting Hosts as well as any optional policies required for encrypted communications.
7. The Initiating SDP Host initiates a mutual VPN connection to all authorized Accepting Hosts.

The whole process is transparent for the end-user. He experiences only a very brief, barely detectable delay in the connection between his browser and the application and sees a SDP sign in his browser.

21.3.1. Promising results

So far SDP implementations have not been broken, as it was tested on two Hackathons.[205] These results are promising.

[205] RSA Conference February 2014 and the Cloud Security Alliance Congress in September 2014.

	Hackathon RSA Conference [206]	Hackathon CSA congress [207]
Period	February 2014	September 2014
Duration	5 days	14 days
Total dropped packets	>10 billion	2.9 billion
Number successful Single Packet Authorizations	0	0
Number successful mutual TLS authentications	0	0
Number successful user authentications	0	0

Besides the US DoD in their Global Information Grid, a small number of enterprises like Coca Cola[208] is developing SDP based secure access solutions for (international) business purposes.

In one case in the US a privacy group explored the option of setting up an alternative for TOR based on SDP. [209] Funding is an issue however, as the set-up and maintenance of SDP requires efforts that most probably exceeds that of volunteer organisations. A government funded effort would probably be more successful, although that raises questions on the independence and protection of privacy.

21.4. Conclusion

SSL and IPSec both have their advantages and disadvantages. In a nutshell, SSL VPNs tend to be deployed with more granular access controls than IPSec, but that also means network administrators may spend more time configuring and modifying individual and group access rules.

If you really need per-user, per-application access control, SSL is the better option. But If you need to give trusted user groups homogenous access to entire private servers and subnets, go IPSec (mainly for efficiency reasons).

Software Determined Perimeter (SDP) is a promising option against multiple network threats for both enterprises and individual users. It takes the disappearing network perimeters into account and grants access (and visibility) on a need-to-know basis.

From the perspective of this study SDP has its disadvantages too, as it requires detailed identity and access management efforts and thus provides no guarantees for anonymity to the managing party. Without proper identification and authorization, no access can be granted.

[206] "During the five-day event, there were more than 10 billion attacks at the Software Defined Perimeter. No one was able to circumvent even the first of the five SDP security controls layers.", Cloud Security Alliance, Hackathon On! Cloud Security Alliance Challenges Hackers To Break Its Software Defined Perimeter (SDP) At CSA Congress 2014, https://cloudsecurityalliance.org/media/news/hackathon-on-cloud-security-alliance-challenges-hackers-to-break-its-software-defined-perimeter-sdp-at-csa-congress-2014/ (accessed 17 November 2014)

[207] Cloud Security Alliance, Software Defined Perimeter Yet to be Hacked. Full Attack Analysis Coming Soon!, https://hacksdp.com/ (accessed on 17 November 2014)

[208] CTOVision.com, Software Defined Perimeter, Cloud Security Alliance: Coca-Cola Case Study, 28 October 2014, https://ctovision.com/2014/10/software-defined-perimeter-cloud-security-alliance-coca-cola-case-study/ (accessed 18 November 2014)

[209] Interview with Brent Bilger of Vidder.

Also SDP relies on existing encryption techniques, with issues as described in other parts of this Annex, including the common vulnerability: the ultimate dependence on one root CA (as single point of failure or rather: single point of compromise). On the other hand: SDP hosts only trust one certificate, that of the SDP Controller, and not hundreds, like the average browser.

If anonymity is not the goal, then SDP is one of the ways forward to protect complex network set-ups and working in the Cloud, mitigating the majority of widely spread attacks.

This document contains the Annex to the second part of the study on Mass surveillance, commissioned by STOA.

This Annex contains detailed information on the four subthemes defined in the initial invitation to tender for the study.

This is a publication of the
Directorate for Impact Assessment and European Added Value
Directorate-General for Parliamentary Research Services, European Parliament

PE 527.410
ISBN: 978-92-823-5538-1
DOI: 10.2861/984037
CAT: QA-06-14-229-EN-N