Comment from Chaos Computer Club e.V. (CCC) for the Joint Public Hearing on Human rights and technologies: the impact of digital surveillance and intrusion systems on human rights in third countries in the European Parliament, Wednesday 21 January 2015

Dear Chair of the Subcommittee on Human Rights Mrs Elena Valenciano;
Dear Chair of the Committee on International Trade, Mr Bernd Lange;
Dear Rapporteur for the report on Human rights and technologies, Mrs Marietje Schaake;
Dear Members of the European Parliament;
Dear Ladies and Gentlemen;

We would like to thank you for the invitation to this public hearing. Since 1981 the Chaos Computer Club deals with civil liberties in the digital world and we appreciate the efforts of the European Parliament to address surveillance as an important human rights issue. We will take the opportunity to raise our concerns about the scope of the current export regulations on ICT security technology.

"Intrusion software" and human rights

Regulation EC 1382/2014 amending the Community regime for the control of exports, transfer, brokering and transit of dual-use items follows the "intrusion software" clauses in the Wassenaar Arrangement. These clauses are intended to protect activists, dissidents and journalists whose lives are endangered by government surveillance. We welcome the initiative to protect citizens from unjust surveillance activities. However, our intervention will show that the intentions are contradicted by their real-world effects on technical security of ICT systems. In order express our view the intervention is split in three main parts: The problem with the scope, the problem with the definition and lessons learned from past export controls on strong cryptography.

The definitions used for "intrusion software" are overly broad, applying almost universally to elementary building blocks of security research. Among the unintended effects of the definitions are chilling effects on the development of anti-surveillance measures and on the discovery and repair of existing vulnerabilities and vulnerable systems. The definitions impose a prior restraint on the publication of security research, analogous to the export controls on strong encryption software that were in effect in the 1990s. The anti-surveillance intent of Wassenaar will, however, be fully fulfilled if surveillance-enabling software and hardware is addressed directly by naming the respective products respectively services individually. Another approach would be to prosecute the actual transfer and use of technology in well defined cases of surveillance deemed unjust by EU standards.

Moreover, software is speech. And free speech that can only be abridged for overriding reasons of public interest, by law and in a proportional fashion - in line with Article 52 of the European Charter of Fundamental Rights. The Wassenaar Arrangement's definition of "intrusion software" covers too many other types and uses of software that it cannot be implemented in a proportionate manner. Especially in light of the fact that the goal, namely denying authoritarian governments the means for surveillance, can also be achieved by restrictions on consulting and implementation services related to intrusion software.

Export controls only work with the right scope

Export controls work with well defined physical goods such as weapons and equipment that require not only expertise but also possibilities for manufacturing and maintenance. Due to a necessity of shipments there is an identifiable supply chain and controls can be enforced. For many of the "classical" controlled goods it is not enough to know how a certain technology works, there are needs to be equipped with the right tools and machines in order to build or assemble parts. However, this also often involves civilian technology used to build all types of tools and spare parts, so that they cannot be restricted without seriously harming the functioning of a technical society. Some of those classical examples are engine lathes or combustion engines and its research for safety and effectiveness.

The problem of scope

The Review of export control policy: ensuring security and competitiveness in a changing world COM(2014) 244 states: "*Exports are increasingly transmitted, not transported. In the age of cloud computing, information flows containing sensitive technology can be used to produce unlimited quantities of sensitive goods and present a major challenge for export control, especially due to the inapplicability of border controls, and the difficulty for companies to ensure compliance (e.g. with respect to IT architecture, engineering collaboration, travel of experts etc). Export controls thus need to operate 'online' in the context of a globally connected world, in which intangible technology transfers (ITT) have become increasingly significant vis à-vis the physical movement of goods.*". A footnote explains what "ITT" means: The "*Intangible technology transfer includes both the transfer of technical information via electronic means and the transfer of knowledge and skills by persons*".

The lack of necessity of physical shipments and travel renders classical export restriction controls ineffective. Surveillance of network connections in order to detect violations is neither feasible nor desirable. Enforcement is therefore dependent on detection of malicious use of specific technologies in the field rather than just presence of the underlying technology itself.

ICT security can't be improved if research, publications, talks and trainings are under an export control regime. How could a researcher or auditor easily distinguish what specific technology is under control if the technology is described in a overly broad way, as it is right now? How will the proposed legislation deal with talks at conferences dealing with serious vulnerabilities and issues? Is an EU researcher allowed to talk in the US about vulnerabilities or exploitation techniques (where this list of controlled technologies is currently not in effect)? How do we deal with exploits and exploit development kits in order to make people understand what impact which vulnerability has and to develop defenses against known ones? How must exploits be published? Are training programmes export controlled if publicly accessible (i.e. via streaming or recording)? It is also unclear what it means in more unspecific ICT environments, like test and staging environments or for the education of security officers in companies, governments and research facilities.

Nonetheless, the view expressed in COM(2014) 244 is a clear threat to both research and general technical security of devices for general purpose computing. In the world where software like operating systems, browsers or office suites are manufactured worldwide in a distributed manner, protection of these systems is also organized in a global fashion. That means that advances in protective measures are also advances for users in countries subject to export controls – as long as they update their systems (unfortunately it was shown that many journalists and dissidents get attacked through vulnerabilities, that were known to the public and already patched by the vendors, i.e. Flash and Java exploits). However, chilling effects on ICT security discussions in the EU don't only have an impact on EU citizens but also on citizens of countries subject to export controls and thus their protection.

Basic attack and defense principles in information technology

The nature of ICT is that the attacker always has a disproportionate advantage: they can monitor a target, wait for things to happen like updates or for a specific misconfiguration and can also gather and exploit specific aspects of the targets environment. One major goal for software security research is to make it harder for attackers to carry out attacks. Security research is mandatory to increase resilience of any and all ICT systems, and to build protective measures in order to limit the harm done by successful attacks. So called "intrusion software" plays a major role in aiding security researchers executing these very tasks. Open discussion of vulnerabilities is required and consequently the use of tools to exploit them.

A problem of definition

EC 1382/2014 defines "intrusion software" as a class of software to be export controlled and covers many very common and essential techniques used throughout software engineering, not only those which are unique to malware and attack tools. For example software meant to test the effectiveness of intrusion detection and monitoring tools falls within the definition of "intrusion software". An effective and appropriate definition would focus on the capability to obtain sensitive user data from a targeted system (the term used is "exfiltration"). Surveillance is about receiving data, the condition of being surveilled does not exist without data being sent to be viewed or accumulated.

These techniques are used by computer security products, remote management software, antivirus, enterprise reliability and monitoring software and operating systems. They are also used for security related research and audits, ordered by SMEs as well as multinationals or governments. Vulnerability-finding software must generate “intrusion” to be effective and able to prove insecurities. EC 1382/2014 also defines *“Technology” for the “development” of “intrusion software”* which is even a *meta good* to be controlled. At some point there is no real difference anymore between goods that help developing "intrusion software" and goods to counter intrusions and to develop and improve security-related software.

Countering software-enabled surveillance (or any kind of surveillance) through "intrusion" (essentially, trespassing over a boundary, which in tech is necessarily an abstraction, and largely meaningless) is convoluted and counterproductive. Surveillance is about receiving data, the condition of being surveilled does not exist without data being sent to be viewed or accumulated. It's like defining theft as trespassing or unwanted proximity. Theft is about taking property without permission, not about proximity or entry. Even though it does sometimes involve trespassing, it is not defined by it, and including it would only muddle matters. Exfiltration is what clearly distinguishes security research and audits from surveillance.

So-called Fuzzers are a good example for a whole range of tools and code that would clearly fall under the export regime of EC 1382/2014. Fuzzers are software tools that provide invalid, unexpected, or random data to the inputs of computer programs. The programs are then monitored for exceptions such as crashes, failing built-in code assertions or for finding potential memory corruptions. These tools are not only widely available, it's also a quite successful approach for finding vulnerabilities. So automated operation and generation of code is an important way to make progress in this whole area of vulnerability finding.

Exploitation

Software is fragile and not all software is written with security in mind. But even if it were, vulnerabilities can't be completely avoided. Sometimes even a single misplaced character in thousands of lines of code can cause horrible problems that are present in widely used software for decades. In fact, we are still not able to perfectly predict the execution of programs on systems that are well known. Hence systems that are not well known – like heterogeneous environments on todays desktop, mobile and server systems – will behave even less predictable.

Security research follows the general pattern of software engineering. But controlling technologies of software development and automation is extremely broad and contrary to principles of software engineering itself (and this is what EC 1382/2014 tries to achieve). Exploits are not as exciting as people think they are, but exploits are both, result of (unintentional) computation and a foundation to improve meaningful security. Exploits are used to prove problems in code and system configurations that would otherwise not be treated as serious issues.

Lessons from the past

To understand the harm that export controls will have on the general security of technology can be seen with the export regulations of the 90's, the so-called “Crypto Wars”. To fully quote an expression from comments to public comment to the US discussion on this topic: "*Export restrictions on artefacts of cryptography have doubtlessly harmed [the] practical progress [of cryptography]. Not only Johnny Q. Public still can’t encrypt, but John the Special Agent can’t encrypt either!*". Without export controls the problems with intercepting and decrypting encrypted messages wouldn't probably exist to the current degree, because export controls on cryptography had an effect at the time when the current communication protocols got developed. We still suffer from decisions made in the light of "export cyphers" and how to implement exportable cryptography. These export controls had a tremendous chilling effect on innovation in the field of secure communications, and it is inevitable that export controls of the overly broad type of "intrusion software" will have an even more negative effect on the security of ICT systems now and in the future.

Thank you very much for your attention.

Christian Horchert
Chaos Computer Club e.V. (CCC)
Humboldtstraße 53
D-22083 Hamburg
Germany

Related Documents

EC 1382/2014: Commission Delegated Regulation (EU) No 1382/2014 (Export controls): http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2014_371_R_0001&from=EN

COM(2014) 244: The Review of export control policy: ensuring security and competitiveness in a changing world http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf

Public comment: Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How To Fix It http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf

Related Links

Fuzzing at Wikipedia http://en.wikipedia.org/wiki/Fuzz_testing