On the free use of cryptographic tools for (self) protection of EU citizens

January 20, 2016

Contact person: Demosthenes Ikonomou

E-Mail: isdp@enisa.europa.eu

Context

There is a legitimate need to protect communication of individuals and individuals to public and private organizations. In our brick and mortar world, this need is reflected by the use of letter envelopes and seals. Furthermore the right to secrecy of correspondence is inscribed explicitly in most EU member states' constitutions and in art 12 of the declaration of human rights. Especially in individual to individual communication, however, equivalent protection measures for electronic communication are only occasionally used. Moreover, the desire to exercise this fundamental right has often been depicted as threat to business models or even public security. Advocates of better data protection have often been discredited by the motion that if you do nothing wrong then you have nothing to hide. This has damaged the users' trust in services which are based on electronic networks and information technology, numerous examples in the press for a more evidence see e.g. symantec's state of privacy report 2015[1].

Now, with a society that increasingly depends on trustworthy electronic services, unprotected communication becomes a threat. Criminals and terrorists might seize data from unprotected communications and abuse the gained knowledge. The potential for abuse ranges from simple criminal activities such as burglary during leave to targeted attacks on public personas to destabilize social peace.

But vulnerable digital services are not only a risk for the civil society. In the European Digital Agenda it has been pointed out that trust in information technology is of uttermost importance. The new NIS Directive shall "allow[..] the public and private sector to trust digital networks' services at national and EU level. By setting incentives to foster investments, transparency and user awareness, the strategy will boost competitiveness, growth and jobs in the EU." Hence, the regulatory framework on digital products needs to encourage industry to provide trustworthy services by the use of technological protection measures.

The role of Cryptography

In electronic communication, cryptography is the essential tool that allows implementation of secrecy and integrity of correspondence. It provides the electronic equivalents of the letter cover, the seal or rubber stamp and the signature. Policy that regulates, i.e., limits the use of cryptography has been proposed and put in place in the past. This policy attempts either limiting the use of cryptography to certain algorithms that have backdoors and interception mechanisms for law enforcement and intelligent services, or limit the allowed key size in such a way that a powerful attacker can break the scheme. The latter has been introduced under the (at that time certainly correct) assumption that these capabilities are used only for legitimate cause, and that criminal or terrorist organizations do not have access to the technology which would be necessary for abuse.

[1] http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf

Nowadays computing power as a service is a fact, thus this assumption does not hold anymore. Below we discuss several aspects of crypto regulation and their difficulties from a technical point of view.

Lawful interception

Take home message: The use of cryptography might make lawful interception harder and by this less efficient or even ineffective.

For the investigation of major crimes, it might be of advantage to intercept the communication of individuals. It goes without saying that for legitimate interception high legal standards need to be followed. The following discussion assumes that these legal issues are solved and focuses on the technical perspective. The use of cryptographic tools make communications unintelligible, hence the intercepted data might be useless for investigations. It is possible to implement cryptographic measures that allow key recovery and key escrow; however, their implementation might be expensive and might introduce new vulnerabilities to the systems. Furthermore, a ban of cryptographic tools might not even be enforceable.

Cryptographic tools are widely used to protect our information infrastructure from malicious users. Today cryptography is mainly used to protect the access to services such as bank accounts and personal email boxes, e-commerce applications, and communication of individuals and groups (e.g. virtual private networks and message encryption, i.e., end to end encryption).

If cryptography is used to protect access to a service, then the service provider is an endpoint of communication; it has some of information to perform the service. So technically speaking, it has the means to disclose that information on request[2]. However, since usually session keys (which are meant to be one time use) are generated in a way that it is impossible to reconstruct them, disclosing this information might only be feasible for future communications. This property, known as forward secrecy, is intended to protect past communication even in case of successful attacks.

Aside from the difficulty of recovering session keys, another challenge is that users might also hold private keys, unknown to the service provider. If messages are sent to the users encrypted with their public key, access to their private keys is needed for decryption. However, it is common practice to generate and store these keys only on the users' devices. Similar to forward secrecy, this strengthens the security of the system, since a potential attack against the service provider has less impact on the users' security.

Key recovery and escrow

Take home message: Key recovery and escrow might enable lawful interception, but it introduces new technological risks to IT infrastructure and it might even damage the gathered evidence.

To overcome the issue with forward secrecy and private keys, key recovery and escrow schemes might be used. Key recovery means being able to reconstruct the key from the encrypted message itself, while key escrow means keeping a securely stored copy of that key. To the best of our knowledge, ready to use implementations of these schemes do not exist and the deployment of such systems would imply fundamental changes of the telecommunication infrastructure.

The design and development of such systems would require the involvement of several fields of expertise, namely cryptography, personal data protection and law enforcement. Furthermore, it would increase the

[2] The problem here is more whether the provider is under the same legal framework as the investigator.

complexity of protocols, thus introducing higher potential risks and increasing costs for all communication partners. Note this might even be an economic burden to software and service providers in our legislation, since providers outside of our legislative scope will be able to deliver more secure services at a lower cost.

Moreover, disclosing private keys carries an inherent danger: anyone who obtains a private key can perfectly impersonate the legitimate key owner. This might be a risk to the quality of evidence that is gathered by these means.

Bypassing

Take home message: It is easy to bypass systems that allow key escrow or recovery; evidence for bypassing will only be found during investigation.

When considering end to end encryption between individuals, the obligation to employ systems that allow key recovery or escrow might be difficult to enforce, since keys are generated and stored solely on the devices at the endpoint of communication. Furthermore, it is to assume that none of the key owners might cooperate[3].

A preliminary assessment may suggest that a general ban of such encryption tools can solve this problem; however, such a ban would be impossible to enforce. Indeed, the research community in the field has a long tradition of creating open access and open source for this purpose, a vast amount of tools is readily available for free. Furthermore, the algorithms are publically available and well documented, hence an average skilled programmer could implement them.

This leads to the following challenge: without context information, such as the deployed algorithm, it might be complicated to distinguish a cryptogram from a malformed message that contains only random noise. So a ban on end to end encryption would pose a difficulty for the potential investigator, namely how to prove that a suspect has used such forbidden technology and was not just transmitting random bit streams. Moreover, even if the use of cryptography could be easily detected, malicious users have access to a vast body of steganographic protocols (i.e., protocols that allow the user to put a hidden message in a cover media such as a picture). An investigator will usually not have enough information about the potential steganogram to discover its mere existence, let alone to decrypt the content.

The risks of legacy policy in cryptography

Take home message: vulnerabilities that where left from legacy policy have been abused to attack systems. Further, policy that limits the use of cryptography in commercial products can damage IT industry.

In the past several attempts have been made to limit the use of cryptographic tools by law. The most prominent example is the US export regulation for crypto during the cold war. The United States Government classified cryptographic algorithms as Auxiliary Military Equipment in the US Munitions List. Use of strong encryption by software developed in the US was only allowed on US soil. Outside of the US, only weak variants of the encryption routines were allowed – typically by using shorter key lengths. Although the policy was changed 15 years ago, it has still an impact on today's security, as we have observed with the recent FREAK and Logjam attacks.

Policy makers have the responsibility to pass laws that are just, equitable, and that have the least impact on people's and industry's freedom. Moreover, public policy tends to last for a long time. Computing costs are

[3] Key issue: privilege against self-incrimination

systematically decreasing, in ever shorter periods. Therefore, attacks that seem out of the reach of any one but a nation state will not remain so for the lifetime of the implementations. As such, policy makers

1. Should refrain from limiting in any way security features in computer software
2. Should refrain from limiting in any way the export of security features in computer software
3. Should consider lifting any and all existing limitations for security features in computer software.

Further, more subtle effects have been observed. In 1999 the U.S. Senate Committee on Commerce, Science, and Transportation collected information on the development of cryptographic products outside of the U.S. It was found that the foreign market was rapidly growing and that the quality of the offered products is at least at par with those from U.S. based companies. The testimony further suggests that U.S. export regulations did in fact damage IT industry.[4]

Conclusion

Cryptography provides the electronic equivalents of the letter cover, the seal or rubber stamp and the signature. These electronic tools are necessary to protect our assets in a highly computerized world.

Key escrow and recovery is theoretically possible, but it would need a fundamental change of our communication infrastructure and joint development efforts of many experts. The resulting infrastructure would be more complex, making it potentially more vulnerable to attacks and less resilient to failures. The economic impact might be undesirable. Furthermore, for individuals, it would be rather simple to bypass these systems (unnoticeable for law enforcement), which might make them ineffective. In addition future advances in cryptology and computing power might turn any mechanism that is specifically designed for law enforcement in a vulnerability that can be explored by criminal and terroristic organizations. Lastly, it is likely that restricting the use of cryptography in commercial products, will damage the EU based IT industries.

All the above mentioned issues are mere examples of currently widely used protection measures; emerging privacy enhancing technologies might introduce even more challenges. To overcome these issues, ENISA is eager to support the Member States and competent EU bodies to perform further analyses and to define a balanced approach to move forward.

[4] Statement of Lance J. Hoffman before the U.S. Senate Committee on Commerce, Science and Transportation, June 10, 1999