Seminar 2 – Encryption

Sam Florin
Information Security, Jönköping University
Sflorin@kth.se

1. Introduction

Encryption is the process of encoding information and has many use cases in the security industry. It adds an extra layer of security, so even if data (plain text) is accessed by the wrong party, it will not be readable in its encrypted form. Encryption is mostly used in applications where data is either in rest or transission such as secure network communication, machines and stored data. For sensitive data and communication, this is particularly important since no software system, over its lifecycle, is 100 % secure.

There are 2 types of encryption schemes, asymmetric (public key) and symmetric (private key) [1, p.776-795]. There are also emerging techniques such as the homomorphic encryption (an extension of asymmetric or symmetric scheme) and secure multi-party computation. Widely used techniques, still today, are the algorithms DES (symmetric), AES (symmetric) and RSA (asymmetric) [1, p.776]. Given all necessary properties of a correctly constructed RSA mechanism, it would still take years to find the private key with today's computational power [1, p.793][2].

Although today's encryption algorithms will be vulnerable to future quantum computers and algorithms, these advancements may also utilize and drive better encryption techniques [3, p.1]. This results in that some of both today's and future's encrypted data may never be decrypted, unless the secret key is given or a backdoor is built in.

In general, encryption retains and preserves privacy and confidentiality for individuals and companies, but some cases of encryption may also complicate the work of law enforcement and sercret intelligence. This complication has driven law enforcement to request court orders on making manufactoring companies responsible, forcing them to create backdoors for encrypted applications. For example, the Apple vs. FBI case where Apple declined the request due to the potential damage for users of creating a backdoor, opening up for misuse, abuse, leakage and theft [4][5].

2. Problem Statement

Shall we limit the use of encryption for companies and individuals? Is it possible to make usage of encryption conditional before the law?

3. Analysis

To get insights and different perspective on how to deal with encryption cases, an analysis has been done with focus on [5].

Encryption is good because it retains and preserves privacy and confidentiality, thus security, for individuals and companies. Encryption is an important part of cyber security so limitations or creation of backdoors will open up for more security vulnerabilities according to Application Developers Alliance and Apple [6, p.18-26].

If an application is not allowed to be secure enough to avoid hackers, it would affect the whole market of that business [6, p.19]. It would also be problematic for smaller to middle-large businesses meeting requests of such a caliber as the Apple vs. FBI case without taking any damage (beeing compelled to create intellectual property) [6, p.18-26]. What if the encryption was outsourced, what if the an open-source encryption service was used?

There are resonable to say that more and stronger encryption would result in less crime. If a service changes their encryption policies, it is likely that criminals would change platforms, but also cyber criminals could exploit the non-encrypted data. A key principle in maintaining an open internet with all the possibities it comes with (transactions, messaging, sharing etc.) is to use encryption. I agree with [7, p.87], that the methods for getting investigative information in Apple vs. FBI case would undermine a public and governmental goal of equal or greater importance including personal safety, security and freedom online and that: "gevernment's efforts should not come at expense of the rights and overall security of the public and digital ecosystem". I am certain that these values can be applied to other encryption cases.

In the Apple vs. FBI dispute, American Civil Liberties Union brings up similar points to Application Developers Alliance and Computer & Communications Industry Associations, but they also emphazises the ensuring of free speech and an open internet as a result of enhanced encryption technologies [8, p.91] and that forced backdoors could have a bad impact on this.

Bruce Sewell (Apple) are pushing on that they shall be able to develop the most secure products as possible which they won't with a backdoor. He also pushes on that they don't have a backdoor software bacause its not safe and to develop one would put thousands of users to risk. He is pushing on the consequences and the potential damage that a precedent for government intrusion could result in [9, p.101-103].

Susan Landau (PhD of cybersecurity poicy, former Google and Sun Microsystems engineer) gives a nuanced summary of the big picture, inline with the earlier given arguments and pinpoints today's mobile phone usage, cybersecurity threat, the long-term damage of proceeding with FBI's request [10, p.106-130]. She also critizises FBI's current approach and reveals that there most likely are other feasable sources such as private forensics analysis firms or hacker communities possessing the knowledge of hacking the phone [10, p.109-111, 118].

Apple vs. FBI case could have been a precendent of disfavour for encryption and security but, luckily, it wasn't [6, p.18]. If there was a simple solution to the problem, I am certain that Apple would have acted differently. Instead, we must look beyond individual problems and enforce the long-term security. One would have to understand that cases like this can be complexy and ethically problematic. However, we must protect a less directed but far so great interest in sparing the privacy, confidentiality and security to people and business aswell as enforcing protection against other cyber threats. Even in Sweden where we culturally have a different view on freedom, I can't see how one would justify the means of compelling businesses to unlock devices, solutions or services in similar situations to every price.

4. Comment

The statements from the Apple vs. FBI hearing are obviously biased. However, they provide interesting perspectives in a complex subject. Despite the bias of the provided references, one must understand that these were given by professionals respectfully touching on the national tradegy as it is.

4. References

[1] C.P Pfleeger, S.L. Pfleeger, J. Margulies, *Security in Computing*, Prentice Hall, Pearson Education Inc, 2015.

[2] R.L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystem" Communications of the ACM, February, 1978 [Online]. Available: https://dl.acm.org/doi/10.1145/359340.359342. [Accessed Nov. 10, 2020].

[3] C. Gidney, M. Ekerå, "How a quantum computer could break 2048-bit RSA encryption in 8 hours", *Royal Institute of Technology*, May 23, 2019. [Online]. Available: https://arxiv.org/pdf/1905.09749.pdf. [Accessed Nov. 10, 2020].

[4] A. Kharpal, "Apple vs FBI: All you need to know", *CNBC*, March 29, 2016. [Online]. Available: https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html. [Accessed Nov. 11, 2020].

[5] B. Goodlatte, S. Husband, P. Apelbaum et al., "The Encryption Tightrope: Balancing Americans' Security And Privacy" U.S Government Publishing Office, Hearing before the committee on the judiciary house of representative, March 1, 2016 [Online]. Available: https://www.govinfo.gov/content/pkg/CHRG-114hhrg98899/pdf/CHRG-114hhrg98899.pdf. [Accessed Nov. 11, 2020].

[6] Application Developers Alliance, "Government Mandates to Weaken Encryption: A Threat to Democracy, Capitalism, and Securty", Application Developers Alliance, Statement for Hearing before the committee on the judiciary house of representative, March 1, 2016 [Online]. Available: https://www.govinfo.gov/content/pkg/CHRG-114hhrg98899/pdf/CHRG-114hhrg98899.pdf. [Accessed Nov. 11, 2020].

[7] E. Black, "The Encryption Tightrope: Balancing Americans' Security And Privacy", Computer & Communications Industry Association, Statement for Hearing before the committee on the judiciary house of representative, March 1, 2016 [Online]. Available: https://www.govinfo.gov/content/pkg/CHRG-114hhrg98899/pdf/CHRG-114hhrg98899.pdf. [Accessed Nov. 11, 2020].

[8] K. Johanson, N.S Guliana, "The Encryption Tightrope: Balancing Americans' Security And Privacy", American Civil Liberites Union, Mail-Statement for Hearing before the committee on the judiciary house of representative, March 1, 2016 [Online]. Available: https://www.govinfo.gov/content/pkg/CHRG-114hhrg98899/pdf/CHRG-114hhrg98899.pdf. [Accessed Nov. 11, 2020].

[9] B. Sewell, “The Encryption Tightrope: Balancing Americans’ Security And Privacy”, American Civil Liberites Union, Statement for Hearing before the committee on the judiciary house of representative, March 1, 2016 [Online]. Available: https://www.govinfo.gov/content/pkg/CHRG-114hhrg98899/pdf/CHRG-114hhrg98899.pdf. [Accessed Nov. 11, 2020].

[10] S. Landau, “The Encryption Tightrope: Balancing Americans’ Security And Privacy”, Statement for Hearing before the committee on the judiciary house of representative, March 1, 2016 [Online]. Available: https://www.govinfo.gov/content/pkg/CHRG-114hhrg98899/pdf/CHRG-114hhrg98899.pdf. [Accessed Nov. 12, 2020].