Encryption Paper

Garrett Greenwood

Dr Dow, ECS 3361

The University of Texas at Dallas

Fall 2015

Without the ability to keep secrets, individuals lose the capacity to distinguish themselves from others, to maintain independent lives, to be complete and autonomous persons.... This does not mean that a person actually has to keep secrets to be autonomous, just that she must possess the ability to do so. The ability to keep secrets implies the ability to disclose secrets selectively, and so the capacity for selective disclosure at one's own discretion is important to individual autonomy as well.

– *Kim L. Scheppele*[1]

In order to protect the freedom of speech and privacy of information, strong encryption can be used to hide information from those without the proper credentials. However, well-encrypted data is also impossible to use in legal cases, public defense, or surveillance and allows criminals to hide their digital actions. To combat these activities, government agencies like NSA have been attempting to either limit the effectiveness of encryption methods or require methods for exceptional access to data. This debate sparked in the '90s, when it was decided that encryption should be allowed with certain caveats, but it has resurfaced lately considering the amount of personal encrypted information that private companies hold.

Publicly available encryption entered the spotlight in the early 1970s, with the U.S. Data Encryption Standard(DES).[2] Built as a collaboration between the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), and IBM, it was designed to replace the conflicting standards of the time. The NSA was closely involved in its development, leading to concerns about its security and the possibility of a back door despite being certified as "free of any statistical or mathematical weaknesses".

DES was wildly successful and even became internationally used despite extensive export restrictions which treated it as a weapon, restricting U.S. based companies from selling DES-equipped products to foreigners. Still, books containing the DES specifications could be printed and distributed freely and the standard quickly went global.[3] Soon, it was the most used encryption standard.

DES is a symmetric encryption scheme, meaning that both parties can encrypt and decrypt plaintext with a shared key. The key is 56 bits long, a sweet spot that made computa-

tion fast but could be brute-forced with reasonable investment. For example, an investment of $10 million in 1993 could produce a machine capable of cracking a DES key every twenty-one minutes[4] and the Electronic Frontier Foundation spent $250,000 on a custom machine in 1998 that cracked a key in twenty-two hours.[5] Therefore, it would not be unreasonable for any country or wealthy individual to break DES reliably with enough investment.

In the 1990s, NSA began to push a new standard for encryption that would give them access to encrypted information. Called the Escrowed Encryption Standard (EES), it is designed so that users can communicate securely against decryption from everyone but the U.S. government.[6] EES uses 80 bit keys and a stronger encryption method, making it at least 2^{14} times harder to brute force than DES.[7] It is also built on the SKIPJACK algorithm, which was classified on release. Therefore, users of EES would need to rely on government-supplied implementations and escrow keys.

The main use of EES is in the Clipper Chip, a component that could be added to landline phones to enable encrypted communication.[8] Each chip has a unique serial number and encryption key duplicatedand held by the government. In order to safeguard these keys, each is split into half and given to different "escrow agents" who only release them if a lawful need is demonstrated. These agents must protect these keys from theft, unlawful or fraudulent requests, and transmit them safely.[9]

To participate in a Clipper-encrypted phone call, users must press a red button to enable the security feature. At this point, two more keys come into play. The two phones coordinate a session key unique to that phone call, encrypt it using their preprogrammed

chip keys, append their device IDs, encrypt it again using a government master key, and finally broadcast the result over the line. Law enforcement agencies who have a record of this call can then use the master key to uncover the IDs of each phone in the conversation. Once they obtain the corresponding key from the escrow agents, they can decrypt again to get the underlying session key which opens up the entire message.[10]

All of this complexity creates a secure environment only if several assumptions hold true. The governmental master key may not fall into the wrong hands. Although the key will only exist in hardware circulated among law enforcement agencies, it may still be stolen or used nefariously.[11] The escrow agents must only hand over keys in the case of lawful requests, and keep them safe otherwise.[12] The phones communicating must implement a secure method for choosing a session key. This step isn't handled by the Clipper Chip and must be implemented by each manufacturer.[13] Finally, each implementation of these encryption methods must not have mistakes. Like the recent Heartbleed vulnerability, a small error may lead to the exploitation of the entire system. If any of these goes wrong, the integrity of the entire system and the promised security is lost.

All of these issues and more were brought up by a group of scholars and cryptoanalysts in 1997[14]. Their article on the technical hurdles of a key escrow system was instrumental in the public debate and the Clipper Chip was eventually abandoned[15].

In the meantime, innovation on the Internet has flourished in an environment supported by open encryption standards. Systems like Twitter and Facebook would likely not exist if there was a requirement for built in key escrow. Even still, law enforcement's fears

about "going dark" and being unable to collect important evidence came untrue and in fact, they have "much better and more effective surveillance capabilities now than [they] did then"[16].

Today, encryption is at the heart of the Internet. Society has become more dependent on these systems which are under constant attack, increasing the importance of encryption since it entered the public sphere forty years ago. We have also learned more about how to build strong cryptosystems, although their difficulty is still mainly in the implementation. Encryption standards are also no longer under export restrictions and the Advanced Encryption Standard (AES) is now used around the world, much like DES was.[17] Otherwise, the encryption environment today is very similar to when the escrow debate came up in the 1990s.

Modern cryptography systems are asymmetric and rely on seperate keys for encryption (public key) and decryption(private key).

The context of the debate has also switched from law enforcement requesting "key escrow services" to "exceptional access methods". The key difference is that exceptional access is much more broad and encompasses key escrow. Exceptional access is the ability for law enforcement agencies to obtain the plain text for any encrypted message that they can obtain through legal means. This would require all implementors of encryption to be able to decrypt user data transparently and at will, which poses two issues with modern communication security practices.[18]

The first issue lies in the practice of *forward secrecy*. Similar to the Clipper Chip discussed earlier, each session has its own symmetric session key shared between both parties. It is quickly becoming standard standard practive to delete these session keys after each transaction. In this model, the system is more safe against attacks because an attacker will only be able to compromise ongoing sessions. Otherwise, a single infiltration could lead to the compromise of the entire history of encrypted information.[19]

As a result, the system has no way of reading messages sent in the past, which is directly incompatible with the needs of an exceptional access system.

The second issue is that the current best practice involves using *authenticated encryption* to verify both the identity of the other party and that the message hasn't be tampered with. Therefore, this method can provide both authentication and confidentiality. A private key is used to generate signatures while the public key can verify the integrity of the message and sender. Implementing key escrow in order to read messages would therefore compromise the private key, giving the ability to forge messages and ruining the integrity of the system.[20]

Both of these modern practices are reduced in effectiveness by the need to provide exceptional access. Additionally, the nature of today's large app economy would make it nearly impossible to perfectly implement exceptional access. If one app implemented key escrow, its users who are concerned about the security implications of a more complicated system could simple move to another system.

However, that just covers the technical aspects to the current debate on exceptional access methods. There are still many legal and ethical facets to explore. Arguments have been made against

In response to the Congressional hearing that revitalized the debate, a new proposal suggested a method of wiretapping without needing to weaken the secure infrastructure.[21] This approach involves leaving the underlying software as it is and instead exploits hidden bugs. These so-called *0-day vulnerabilities* (named so because bugs are discovered on day 0 and worked on later) are often subtle but can have great effects on the security of the system. For example, the Heartbleed bug allowed for private keys used in certificates to be cracked with minimal effort. From these keys, an attacker can access all of the data in the website's databases, including user communications.[22]

A recent study found that these 0-day vulnerabilities last an average of 312 days between first use and their public disclosure.[23] During this time, the closed knowledge of the bug is extremely valuable since it can be used for surveillance and evidence gathering. As a result, these bugs have become commodoties that are being sold both in commercial and underground markets.

The FBI can spend resources either discovering 0-days on their own or purchasing them on the market. Once obtained, they can develop an exploit tool that compromises a vulnerable target using the bug. These tools would be extensively tested to ensure that they don't deal any collateral damage, then will be distributed to law enforcement and used where legally appropriate.

This practice would open up its own class of questions if it were to be publicly adopted. Should the government exploit these bugs silently, or report them and improve the software base? Should the government discover these bugs with their own research teams, or purchase them commercially? If they are purchased commercially, where does the government draw the line when buying from questionable sources?

The last question at least has an analog in current public policy. The use of paid informers to uncover a criminal organization similarly serves to support one who's activities are against good public policy. Also, the law enforcement officers performing the exploit will still be held to wiretapping laws, such as minimization.[24]

Notes

[1]Kim L. Scheppele, Legal Secrets 302 (1988) (reference omitted).

[2]See Froomkin (1995) §I.B.1.

[3]See Froomkin (1995) §I.C.1.c.i.

[4]See Froomkin (1995) §I.B.2. and Appendix A.

[5]See Gilmore (1998) p.1-14. EFF custom designed and built a machine with 1,856 custom chips, each capable of testing 60 million keys a second. It can exhaust the entire keyspace(72,057,594,037,927,936 large) in a span of nine days, and will find the correct key in half that on average.

[6]See Froomkin (1995) §I.C. "Key escrow" refers to the recovery of the encryption key by the government.

[7]Each bit added doubles the number of possible keys to choose from and therefore, the amount of time needed to guess the correct key. At the time of writing, 2,048 bit AES keys are considered secure and used by companies like Google.

[8]See Froomkin (1995) §I.C.2.

[9]See Abelson (1997) §3.2.2.

[10]See Froomkin (1995) §I.C.2.a.

[11]See Froomkin (1995) note 194.

[12]See Abelson (1997) §3.2.1, §3.2.3. and Froomkin (1995) §I.C.2.b.

[13]See Froomkin (1995) §I.C.2.a and note 189.

[14]Abelson (1997) concluded that the system would "require significant sacrifices in security and convenience and substantially increased costs to all users of encryption. Furthermore, building the secure infrastructure of the breathtaking scale and complexity that would be required for such a scheme is beyond the experience and current competency of the field, and may well introduce ultimately unacceptable risks and costs."

[15]See Abelson (2015) p.1

[16]See textcitemit2015 p.2

[17]See Abelson (2015) §1.3.

[18]See Abelson (2015) §2.1.

[19]See Abelson (2015) §2.1.

[20]See Abelson (2015) §2.1.

[21]Bellovin et al. (2013)

[22]See Ltd. (2014)

[23]See Bellovin et al. (2013) p.69

[24]See Bellovin et al. (2013) p.70. Minimization ensures that the wiretapping only captures the subject and only during their criminal activities.

References

Abelson, Hal. 1997. *The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption.* Technical report. Columbia University. http://hdl.handle.net/10022/AC:P:9130.

———. 2015. *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications.* Technical report. Massachusetts Institute of Technology. http://hdl.handle.net/1721.1/97690.

Bellovin, S.M., M. Blaze, S. Clark, and S. Landau. 2013. "Going Bright: Wiretapping without Weakening Communications Infrastructure." *Security Privacy, IEEE* 11, no. 1 (January): 62–72. doi:10.1109/MSP.2012.138.

Froomkin, A. Michael. 1995. "Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution." *U. Penn Law Review 1995:* 709–897. http://scholarship.law.upenn.edu/penn_law_review/vol143/iss3/3.

Gilmore, John. 1998. *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design.* O'Reilly & Associates, Inc. http://cryptome.org/jya/cracking-des/cracking-des.htm.

Ltd., Codenomicon. 2014. *Heartbleed Bug.* http://heartbleed.com/.