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 duplicated and 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] 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.

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.

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.

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.