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 makes com-

putation reasonably fast but can 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. EES 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 the Clipper Chip, a component that could be added to landline phones to enable encrypted communication.[7]

Privacy

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.

[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 in a span of nine days, and will find the correct key in half that, on average.

[6]See Abelson (1997) and Froomkin (1995) §I.C

[7]See Froomkin (1995) §I.C.2.

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.