Encryption Paper

Garrett Greenwood

Dr Dow, ECS 3361

The University of Texas at Dallas

Fall 2015

Introduction

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.

History

Publicly available encryption entered the spotlight in the early 1970s, with the U.S. Data Encryption Standard(DES).[1] 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, certifying it as "free of any statistical or mathematical weaknesses", leading to concerns about its security and the possibility of a back door.

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. 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 computation 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[2] and the Electronic Frontier Foundation spent $250,000 on a custom machine in 1998 that could crack a key in twenty-two hours.[3]

test

Notes

[1]See Froomkin (1995) §I.B.1

[2]See Froomkin (1995) §I.B.2

[3]See Foundation (1998). EFF custom designed and built a machine with 1,856 custom chips, each capable of testing 2.5 million keys a second.

References

Foundation, Electronic Frontier. 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.

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.