Government Backdoors in Encryption

Samuel Weiss

Abstract

The year was 1993, and for the first time, the National Security Agency of the United States of America released their very own computer chip called the Clipper Chip. This chip was intended to be adopted by telecommunication companies as a secure way to transmit voice data. However, by 1996 it was entirely defunct. Yet the Clipper Chip has a legacy far beyond its use, for it was the US Government's first attempt at adding a backdoor in an encryption algorithm. Since those early days, various governments around the world have dreamt of freely reading their citizens secure communications, even if the information is encrypted. Because electronic communications, both secure and insecure, play such a large part in our lives, the issue of government backdoors has become a huge point of controversy both in the US and abroad. It has become a hot issue not only because backdoors present the technological issue of how to secure a backdoor, but also a moral and ethical issue of citizen's rights to privacy. This debate, though long running, is also coming to a turning point; recent leaks and disclosure have shown that governments and government agencies around the world are trying desperately to intercept as much information as they can, to the point that any non-encrypted communications should simply be considered public. This paper will show that government backdoors in encryption algorithms in any capacity are harmful to end users and should not be allowed.

http://www.techweekeurope.co.uk/wp-content/uploads/2013/04/Backdoor.jpg

People in Support of Backdoors

- CIA Director John O. Brennan
- FBI Director James Comey
- NSA Director Mike Rogers
- President Barack Obama
- United Kingdom Prime Minister David Cameron
- North Carolina Senator Richard Burr
- Arkansas Senator Tom Cotton
- Head of the New York City Police Department, Bill Bratton
- Belgian Politician Jan Jambon
- And many more

Introduction

Cryptography is an ancient art, dating back to antiquity when the Romans used a simple cryptographic technique to obscure their messages should their runner be intercepted. But it was not until the digital age that cryptography truly came into its own. The widespread availability and increasing speed of microprocessors led to an immense proliferation of encryption techniques, although they were still overused to securely transmit messages. Although encryption has become much more widespread, the principles behind them have remained mostly unchanged.

Encryption is a way to hide information such that it can only be accessed with a specific key. There are many techniques, but they all hide information by changing the contents of the message in some predictable way. The Romans accomplished this with a technique called a Caesar Cipher, which operates by shifting the characters in the text to be encrypted down the alphabet. For example, the character ‘a’ shifted once is ‘b’, and since ‘z’ is at the end of the alphabet, it becomes ‘a’ when shifted once. In order to decrypt the message once it has been encrypted, one needs only to know the “key” of how much each character has been shifted. This is a very simple encryption method, and the desire to more securely hide information led to the development of the more complex algorithms and techniques which are very commonly used today.

But why do we still encrypt information today? The simple answer is that the internet is very trust-based, and that we have come to rely very heavily on it. Public wifi hotspots, like those found in coffee houses around the world, have proliferated widely, and are often used for sensitive applications like online banking. The problem is that any message you send to your bank on these public networks can be intercepted by anyone else on the network, using a technique called packet sniffing. In order to protect private information from prying eyes, enciphering information has become a highly effective and popular method of establishing privacy.

In fact, encryption has become so effective that governments around the world have taken notice. Many organizations monitor internet traffic to attempt to find evil-doers, from pirates stealing intellectual property to terrorist cells recruiting on internet forums. However, their efforts have been stymied by encrypted communications. This led to the proposal of the Clipper chip, a computer chip to conceal voice transmission from others but leave them open to listening by the NSA. At first glance, the idea of a government backdoor in encryption does not seem like a terrible idea. It would allow government agencies to better detect illegal or dangerous activity on the internet. But that simply isn’t the case, government backdoors in encryption is dangerous and needs to be stopped.

Maksim Kabako/SshutterStock

http://cdn.cfo.com/content/uploads/2014/04/securitylock.jpg

Discussion

What role does government surveillance play in this day and age? Government backdoors in the United States may not appear to have bearing on the other side of the planet. However, they are leading the push towards the worldwide adoptions of cryptographic algorithms with a backdoor. Since the United States is a technological leader, this would mean that people around the world would use this fundamentally weak encryption algorithm. This is problematic for a number of reasons. First and foremost, encryption algorithms designed to be accessible to law enforcement must contain some weakness that allows government agencies to break the encryption, be they American or other. Secondly, the United States has a history marked by aiding oppressive regimes in the past, and a backdoor key to encryption provided by the United States could be used to quash dissent around the world. For these, and other reason, government mandated backdoors in encryption cannot be allowed to exist.

Conclusions

I hope that in this poster I have introduced you to the what encryption is, why it is important, and why it should be defended from government tampering. I hope that you have come to understand the dire consequences of government mandated backdoors in encryption algorithms and why they cannot be allowed to exist. I hope that you will appreciate the security afforded to you by these encryption algorithms, secure from tampering. I hope that you support strong encryption for all, because it is right and because it is necessary. Thank you.

Contact

Sam Weiss
Tufts University
Email: samweiss250@gmail.com
Website: Samuelweiss.github.io
Phone: (952) 270-7215

References

1. Thielman, Sam. "US and European Officials Reignite 'back Door' Encryption Debate after Paris." *The Guardian*. The Guardian, 18 Nov. 2015. Web. 14 Dec. 2015.
2. Temperton, James. "No U-turn: David Cameron Still Wants to Break Encryption (Wired UK)." Wired UK. Wired, 15 July 2015. Web. 15 Dec. 2015.
3. Lyon, James. "Crypto." Caesar Cypher. Practical Cryptography, n.d. Web. 15 Dec. 2015.
4. "Publicly Affirm Your Support for Strong Encryption." Publicly Affirm Your Support for Strong Encryption. White House Petitions, n.d. Web. 15 Dec. 2015.
5. Reitman, Rainey. "Save Crypto: Tell the White House We Can't Sacrifice Security." Electronic Frontier Foundation. Electronic Frontier Foundation, 08 Dec. 2015. Web. 15 Dec. 2015.
6. Wu, Tony, Justin Chung, James Yamat, and Jessica Richman. "Encryption Backdoors." The Ethics (or Not) of Massive Government Surveillance. N.p., n.d. Web. 14 Dec. 2015.
7. Rivest, Ronald L. "The Case against Regulating Encryption Technology." Sci Am Scientific American 279.4 (1998): 116-17. Web.
8. Barker, E. B., E. B. Barker, and J. M. Kelsey. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. N.p.: n.p., n.d. Print.
9. Soghoian, Christopher. "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era." (n.d.): n. pag. Web.
10. Encryption Technology and Possible U.S. Policy Responses, U.S. House of Representatives Subcommittee on Information Technology of the Committee on Oversight and Government Reform Cong., 1 (2015) (testimony of Kevin S. Bankston). Print.
11. Founding, Fathers. "The Bill of Rights." N.d. MS. The Charters of Freedom. Web. 15 Dec. 2015.