William “Chris” Fenton

CSF - Ethics

03/04/2016

Cryptographic Backdoors

Introduction

The use of encryption and cryptography to secure communications has a history that dates back to at least 1900 BC.[1] The ancient Greeks, Indians, and Romans have documented histories of using cryptography, the art and science of creating secret correspondence usually by means of enciphering and deciphering a message in a secret code or cipher. In the digital age, cryptography entails the encoding and decoding of digital information. In cryptography, encryption is the process of encoding information and decryption is the process of decoding said information. As more and more of our information is stored and accessed via the Internet, safeguarding that information has become a key concern in the digital age. Encryption has increasingly become the norm when accessing and transmitting sensitive information; furthermore, the majority of all website traffic is estimated to become encrypted within the year.[2]

---

1 Sidhpurwala, “A Brief History of Cryptography.”

2 Hackett, “Most Internet Traffic Will Be Encrypted by Year End. Here’s Why.”

As the use of cryptography rises as a means to keep our information private, the security of the technology that we rely upon to safeguard our information becomes ever more important. We are trusting cryptography and encryption to safeguard our most sensitive information: our medical and financial records, passwords, private communications with colleagues, friends, and family. By placing our trust in the security of the protocols that encrypt private information, we become more susceptible to breaches of that trust that expose our private information against our will. It is in this light, in the mindset of trust, that we must discuss the ethical ramifications of government induced cryptographic backdoors--the process of building a means of bypassing the cryptographic security into the system itself.

The US Government and Cryptographic Backdoors

The US government and the NSA in particular have long history of involvement in cryptography and cryptographic backdoors. For example, the NSA's 1994 Clipper chip was designed to allow warrantless access of voice communications. The design was quickly demonstrated to be insecure, undermining the veracity of the project. And the promotion of deliberately weakened cryptographic ciphers in website encryption by the U.S. government left websites vulnerable to the recent Logjam and Freak TLS downgrade attacks.[3] Additionally, the Dual_EC_DRBG algorithm that was strongly supported by the NSA and pushed into the National Institute of Standards and

[3] Green, “A Few Thoughts on Cryptographic Engineering.”

Technology 1997 report for recommendations on the creation of random number generators used in cryptographic systems is widely suspected of containing a NSA backdoor.[4] These are only a handful of example of suspected cryptographic backdoors created and implemented by the US government. More recently, the FBI has asked Apple to bypass the built-in encryption of multiple iPhones used in suspected crimes, potentially creating a backdoor in millions of phones.[5] US law enforcement and some members of congress have been calling on companies to provide backdoors into their encrypted products, and the issue of cryptography and privacy has resulted in an increase in the public discourse surrounding these issues.

The Ethics of Privacy

In this paper, we will examine the ethics of privacy and the implications of cryptographic backdoors through the framework of virtue ethics. Virtue ethics places an emphasis on individual moral character and the virtues that support a moral life.[6] Although privacy can have varying levels of importance among different societies, privacy is increasingly becoming a social value critical to a functioning democratic society.[7] In the traditional ethical discourse, privacy is framed through the notions of negative freedom and autonomy--creating personal space separate from public and political life. In this regard,

---

4 Zetter, “How a Crypto ‘Backdoor’ Pitted the Tech World Against the NSA.”

5 Thielman, “Apple’s Encryption Battle with the FBI Has Implications Well Past the iPhone.”

6 Hursthouse, “Virtue Ethics.”

7 *The Universal Declaration of Human Rights*.

your right to privacy is a negative freedom that declares that others do not have the right to violate your privacy except under extreme circumstances. This view of privacy has been classically aimed at invasions of privacy by governments (vertical) but has more increasingly been adapted to include protection of privacy against corporations and your fellow citizens (horizontal). In this discourse, the emphasis in digital privacy has centered around what information about you is accessible or public; however, in virtue ethics, according to Plotinus' theory of self-determination, it is not enough to simply allow a person or group to determine what private information is shared, but why information should be shared.[8]

Under bulk surveillance and the real or potential existence of large scale cryptographic backdoors, it is increasingly more difficult to know in what ways your private information has been collected and used. Under a traditional ethical and legal framework, the lack of documentation for how surveillance data has been used has made it difficult for those that would bring legal action against the government over the breach of their privacy to demonstrate real harm the government has caused them.[9] However, under virtue ethics, if an agent acts negligent, that agent may still be culpable even without any concrete evidence of damage or harm that has occurred as a result of their actions. In this regard, virtue ethics provides a framework that can help guide the political and legal discourse in the digital age. It’s not enough for the government to believe that it is acting

---

8 Stamatellos, “Self-Determination and Information Privacy: A Plotinian Virtue Ethics Approach.”

9 van der Sloot, “Privacy as Human Flourishing.”

under the strict confines (real or imagined) of the law, the state has an obligation to act in a virtuous manner: this may include the obligation to avoid abuses of power and to act openly and transparently.

Conclusion

The digital age has greatly transformed the nature of the way that we interact with each other, the nature of commerce, and the nature of our private lives. As we become more aware of this transformation, the use of digital security methods such as encryption becomes more prevalent as a means to safeguard our privacy. And as we become more reliant upon strong cryptography as a means to safeguard our private information, we become more susceptible to cryptographic backdoors. By operating under secrecy and with almost no public oversight, the US government has made us more vulnerable to breaches of our private information by either purposeful spying on their own citizens or more indirect means such as introducing security holes that others, such as criminals and foreign governments, can eventually find and exploit as in the case of the Logjam and FREAK attacks.[10]

By holding our government to a virtue ethics standard of not abusing its power and acting in an open and transparent manner, we can reshape the legal and political

[10] "Issue Brief."

discourse around privacy and potentially open the door to reforming our current surveillance practices and creating a new framework for privacy in the digital age.

Works Cited

"A 'Backdoor' to Encryption for Government Surveillance." *A "Backdoor" to Encryption for Government Surveillance*. Accessed March 4, 2016. https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/.

Green, Matthew. "A Few Thoughts on Cryptographic Engineering: A History of Backdoors." Accessed March 4, 2016. http://blog.cryptographyengineering.com/2015/07/a-history-of-backdoors.html.

Hackett, Robert. "Most Internet Traffic Will Be Encrypted by Year End. Here's Why." *Most Internet Traffic Will Be Encrypted by Year End. Here's Why.*, March 30, 215AD. http://fortune.com/2015/04/30/netflix-internet-traffic-encrypted/.

Hursthouse, Rosalind. "Virtue Ethics." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Fall 2013., 2013. http://plato.stanford.edu/archives/fall2013/entries/ethics-virtue/.

Sidhpurwala, Huzaifa. "A Brief History of Cryptography." *Red Hat Security*, August 14, 2013. https://securityblog.redhat.com/2013/08/14/a-brief-history-of-cryptography/.

Stamatellos, Giannis. "Self-Determination and Information Privacy: A Plotinian Virtue Ethics Approach." In *4th International Conference on Information Law*, edited by Maria Bottis. Nomiki Bibliothilei Group, 2012.

The Universal Declaration of Human Rights. Allen & Unwin, 2008.

Thielman, Sam. "Apple's Encryption Battle with the FBI Has Implications Well Past the iPhone." *The Guardian*, February 20, 2016, sec. Technology. http://www.theguardian.com/technology/2016/feb/19/apple-fbi-privacy-encryption-fight-san-bernardino-shooting-syed-farook-iphone.

van der Sloot, Bart. "Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data?" *JIPITEC* 5, no. 3 (December 23, 2014). http://www.jipitec.eu/issues/jipitec-5-3-2014/4097.

Zetter, Kim. "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA." *WIRED*, September 24, 2013. http://www.wired.com/2013/09/nsa-backdoor/all/.