Xander Eisert & Maxwell Jones

Dr. Im

CIS 483

16 April 2020

Encryption: A Defense of Personal Privacy

**Encryption: What Is It?**

The locks on our front doors serve an immensely important purpose: they keep us safe from intruders and maintain and protect our privacy. Duplicate keys can be made to allow others access to our homes and, by extension, access to our personal lives and secrets, and we have the right as citizens to maintain and protect our privacy from the government so long as there is no legal precedent to intrude on us (for example, search warrants due to an investigation). Encryption is the lock on our personal computers, our data, and anything we hold in privacy. It is virtually unbreakable by any tool other than virtually nonexistent quantum computers. The United States government wants to take away the right to encrypt data in order to prevent criminals from using it to permanently hide digital evidence, but the importance of encryption to the public cannot be overstated, and it must be protected.

We can liken the right to put locks on our doors to the right to encrypt our personal data. Encryption serves as a tool to protect individuals and their privacy in a world where digital theft is getting easier with each passing day. Even if an individual has nothing to hide, would he or she forego a lock on their door? A lock on your door, or in this case your data, serves to keep your own privacy regardless of whether you’ve got anything to hide. Despite the negative connotation of hiding things from prying eyes, there is ample reason to have encryption for completely legal purposes.

Perhaps one of the biggest reasons for encryption’s existence is the unsecure Internet. When it was built, the early pioneers of the Internet had no intention of implementing privacy features, as they had no idea the scope to which the Internet would grow. As it did grow, the need for privacy on the Internet became more and more pertinent with the advent of online shopping & secure checkout, personal information submission, and anonymity in conversation.

The use of encryption also facilitates protection of personal information within companies such as hospitals and banks. In a database, personal data is encrypted and therefore protected from prying eyes within and outside any individual company. A passport, a driver’s license, a social security number, these are all extremely volatile components of our personal information, and without encryption, the data could be easily compromised, and the entire infrastructure of the government and personal identity would become meaningless. 256-bit AES encryption has the power to protect personal data from most any potential breaches for a theoretical maximum of thousands of years of brute-force password cracking methods (Porter).

Web traffic alone is also incredibly important and necessary to protect via encryption. Usernames and passwords are easily intercepted by several exploits and man-in-the-middle attacks, and keylogger programs and cross-site scripting make online privacy a problem even when performing the most mundane tasks. Bigger websites use HTTPS, which is encrypted by default, but to encrypt traffic to unsecured websites, many people use VPNs to make a “tunnel” using the same AES-256 encryption that protects most other confidential data. VPN services are extremely popular with the privacy-minded in order to guard their Internet traffic from prying eyes such as an ISP. We will discuss this more in the “Action Plan” section.

**Legal Circumvention of Encryption**

Following the event that took place December 2015 in San Bernardino California, the FBI located and found one of the attackers’ work phones. This phone was an Apple iPhone 5C. Once the FBI had possession of the device, they began to investigate the device and had learned the phone was protected by a four-digit code. The caveat to this though being if you do not get the four-digit code in 10 or less tries then all the data will be destroyed off the device. Seeing that with a four-digit code there are 10,000 different number combinations 10 tries would not be enough.

In response to this the FBI called upon Apple to create an iOS firmware update that would forgo this erasing of encrypted data if the 10 four-digit passcode tries failed. The FBI made this call based on the All Writs Act. The All Writs Act gives the federal courts the power to “issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.” (Richards, et. al.) The FBI called upon the All Writs Act for this case because of the event that happened claiming the work phone could hold evidence pertaining to the case they are trying to solve.

Apple has disagreed with this calling of the All Writs Act and does not give in. CEO Tim Cook stated in an online statement that while Apple respects the FBI, they feel there would be subsequent issues regarding data security in the future if Apple were to give into this. This would set major precedence on this topic if Apple were to give in as Apple being a large company and is known for their encryption on their devices. Apple and CEO Tim Cook fear that if they give into this that the All Writs Act could be called in the future to do the same thing under different pretense that the FBI and other government bodies may deem probable cause to use this act.

The FBI had called upon Apple to write an updated iOS firmware that would create a backdoor into their own devices that could be pushed remotely and turn off the erasing of data after 10 failed attempts of the passcode. This was asking Apple to break their own encryption that their customers rely them to have. The worry here is that if Apple gave into this it could be used in court to be done to another company. It is also unclear how far this could be pushed in terms of what is considered probable cause. For this case it was based on the event that happened in California, but who is to say the next time they try to use the All Writs Act it could be for something smaller? This is a big turning point for encryption and the users who trust the companies they buy their products from to keep their data safe and private.

Key Disclosure laws state that if a device you have has encrypted data on it that is under the suspicion of having unlawful data on it then in certain cases with the required documents, law enforcement could require the key to decrypt the data and use against you in the court of law. For us in the United States we are protected from this by the Fifth Amendment of The Constitution which protects witnesses from being forced to incriminate themselves. However, for some other countries such as Australia this is not the case. Law enforcement there are allowed to retrieve password/decryption keys from suspect material. If the subject does not provide the decryption key, then they could be jailed for up to 6 months. In other countries such as Canada, their rules against Key Disclosure are along the lines of if law enforcement must ask for the decryption key is inadmissible and the seizure of data unreasonable.

This does however have somewhat to do with the US government wanting to have access to encryption information from large tech companies. The issue here is that this would no longer make the data as “encrypted” as before because the government would have access to the keys. It would then be speculated that if they felt a need to use the encryption information to decrypt a device they could do so since they have access already. This would not be the smartest idea, not only because at any point could the government say their reason for the use of the encryption information is lawful, they would also be holding encryption information for the largest tech companies. This would most likely put a target on the holding server of that encryption information and make the tech companies encryption more prone to decryption if hackers obtain that information. At that point the encryption the tech companies have promised their customers will be gone.

The EARN IT act was created with the mindset of helping the fight against child sexual exploitation online. This act would make hold tech companies responsible for happens on their websites. Instead of not being liable for what is being done on their website, companies must “earn” to not be held liable. This would be done by showing that there are content management filters and monitors put in place to scan for elicit photos and conversations. This however could become a problem for companies who promise their customers end-to-end encryption. There are some speculations that this act is steering towards opening the ability for government bodies to monitor once encrypted data. This is the opposite direction that you want to go as this is the entire reason encryption is used: to protect your information from being monitored.

**Action Plan**

The biggest problem with encryption legislation is that not enough voters understand why encryption is in their best interests. The only way to improve that is to shed light on the biggest privacy issues and flaws in the system that we discussed in the beginning section. People need to be informed of the many ways encryption helps to protect them in their daily lives and how it does orders of magnitude more good than bad. Perhaps another way the masses can be swayed is by having them take a close look at how spam callers always seem to be bothering them. If your phone number, a personalized ten-digit code unique to only you, can be found easily enough for dozens of call centers to call you up to try and steal your money, could the same not be done with a 9-digit Social Security number? Information theft runs rampant, and encryption helps to slow it down. The largely unencrypted Internet and the lack of care and concern make information exchange much easier than one might think.

Have you ever gone to Amazon.com and looked for something, then gone to another page and see an ad along the side for the item you just looked up? It seems most if not all people have seen this. This is because of the collection of data. Companies are willing to spend large sums of money for different data to help analyze and increase their large datasets. The more data they have on people the more they will be able to tailor things to you. Big data has become a large part of company’s abilities to tailor ads to customers, along with tracking information on smart phones.

Anymore it is becoming more and more apparent that companies are aiming to sell their data that they have from their customers. For many this is the largest form of profit for them as other companies are chasing data to help figure out trends and analyze the big data. In order to analyze big data, you need a large dataset, which most of these companies have with how many customers they have and the information they gather from profiles, Google analytics from monitoring their websites on popular parts etc. This should not be the sole reason for a company to exist, but based on the book The Goal, “The goal of a company is to make money now and in the future.” (Goldratt) Some people do not realize the vast amount of information companies are able to pull from your searches online to visiting their page once. All that is tracked and kept being used. Encryption is necessary and important to help fight against this as well as some potential legislation regarding what information can be used and sold. It seems legislation has not caught up to this trend, but perhaps soon it will, and this will change.

In order to maintain encryption on the level it needs to be, there are some things that must not be done by the government. The government does not need access to decryption keys that large tech companies have as it could possibly be abused in the future. Not only that, but the storage device that would hold that decryption data could become a target and be hacked itself. If that is the case the encryption promised by tech companies will be obsolete. Companies should keep their encryption keys within their organization, the more it gets put out there, the higher a chance for a leak.

Works Cited

Goldratt, Eliyahu M, and J. Cox. The Goal: A Process of Ongoing Improvement. Goldratt Group,

1984.

Porter, Kim. “What Is Encryption and How Does It Protect Your Data?” Norton

Richards, Neil, and Woodrow Hartzog. “Apple v the FBI: Why the 1789 All Writs Act Is the

Wrong Tool.” The Guardian, Guardian News and Media, 25 Feb. 2016,