Encryption is Not Terrorism

Daniel Kohlbrenner, 2017
Computer Science and Entrepreneurship

"Do we want to allow a means of communication between people which we cannot read?" Prime Minister David Cameron asked the press, attempting to propose a ban on services which offer "end-to-end" encrypted messaging.[1]

Simply put, encryption is the technology used to protect data. When users wish to protect their data— passwords, bank account information, or important files—encryption allows them to store and share that data with the confidence that it will not fall into the wrong hands. When a person puts a lock on their front door, they only wish to share their keys with the people who are allowed into their home. Encryption works in a similar manner.

This technology is extremely important to our society. With the amount of personal information being created digitally, it is no wonder that people are starting to use encryption and other privacy tools as one would use a key and a lock on their front door. Encryption is essential because it protects this sort of information from being stolen. Services which offer "end-to-end" encryption protect a user's data the entire time that it travels over the internet. This type of service especially irks the Prime Minister because it makes it much harder for intelligence agencies such as GCHQ and the NSA to collect and store the public's private communications.

This anti-encryption rhetoric is not restricted to UK. Late last year, the director of the FBI proposed that the US government should force tech companies like Google and Apple to create mechanisms for law enforcement to access a user's data, regardless of his or her current privacy settings.[2] Commonly referred to as "back doors" these mechanism take the place of intentionally insecure programs that would allow law enforcement, as well as any knowledgeable hacker, to break into commonly known products. This is in response to the tech companies' recent release of cell phones that are encrypted by default, which would prevent someone from going into a phone and making a copy of all of its data.[3]

Claiming that cell-phone encryption would take law enforcement to a "very dark place," Director of the FBI James Comey called upon Apple and Google to reverse their policy of encrypting phones by default. Despite the fact that mobile encryption has made us safer as a whole, the FBI still went as far as lobbying the president to force tech companies to back door their products.[2] It's no secret why those who represent law enforcement would feel animosity towards encryption tools—encryption prevents any third party from accessing private data, even the police.

When Edward Snowden's leaks first appeared, it was revealed that the National Security Agency considered the use of encrypted web services to be probable cause to spy on a person's communications.[4] Statistically this was an easy way to narrow down potential targets, but ever since these activities were leaked, the amount of encrypted web traffic has increased dramatically.[5] Similarly, the NSA has increasingly worked to weaken encryption standards so that private messages would be easier to break into. In fact, the NSA paid computer security

giant RSA $10 million to use an encryption algorithm in their products that the NSA could easily break.[6] This demonstrates the increasingly destructive activities by intelligence and law enforcement against encrypted communications.

After the revelations, total encrypted Internet traffic in North America spiked from 2.29% to 3.8%. Other locations experienced even greater leaps in their use of encryption. Over 10% of Internet traffic in South America is encrypted during peak hours. [7] All of this is seen as a public reaction to online surveillance. Unfortunately, as long as it is at such a low amount, encrypted services will be used by intelligence agencies to statistically narrow down users and target them for surveillance. If encrypted web traffic is increased substantially, using encryption as probable cause will no longer be an effective way to single out users.

On the other hand, cyber attacks have been prevalent throughout the news and incredibly costly to both the public and private sectors as of late. The attacks on Target revealed thousands of customer's credit card information, showing the American public the cost of poor cyber security.[8] We are living in an age when it is increasingly clear that not securing one's data can be hugely costly. If the public used more encrypted services and other privacy measures, we would be much more protected against these hacker threats.

Intentionally weakening or outright banning encrypted services is a dangerous proposition because it weakens our technological infrastructure at a time where the protection of personal data has never been more important. As several security researchers in the UK have proven, weakening encryption standards, creating back doors in popular products, and generally poking holes in technological security for the sake of surveillance only makes it easier for hackers to exploit these artificial vulnerabilities.[9] When a technology is intentionally made weaker, spies are not the only ones capable of exploiting the weaknesses. While more information is put online and the theft of that information is becoming more and more costly, we need to focus on securing that data from any third party. It's through the implementation of *stronger* security measures and *less* destructive intelligence measures that we will have a more reliably connected society.

Over the past few months it has become clear that many world leaders don't like encryption, because it tends to get in the way of intelligence activities. These leaders claim that encryption is tool used by criminals and terrorists. The fact that some criminals have used these technologies, does not justify outlawing them. It is clear that the public demands a way to protect their data. Keep in mind that for our networked society to ensure the privacy of individual users, individuals need to be safe from all unwanted third parties. Selective security is weak security and weakening encryption only puts innocent users at risk. So when Cameron asked the public if they want to allow encryption, it would seem that the resounding answer is "absolutely."

Works Cited

[1] Timm, Trevor. "Banning All Encryption Won't Make Us Safer, No Matter What David Cameron Says." The Gaurdian. January 13, 2015. Accessed February 7, 2015. http://www.theguardian.com/commentisfree/2015/jan/13/banning-encryption-david-cameron-not-safer.

[2] Timm, Trevor. "The Government Wants Tech Companies to Give Them a Backdoor to Your Electronic Life." Accessed February 7, 2015. http://www.theguardian.com/commentisfree/2014/oct/17/government-internet-backdoor-surveillance-fbi.

[3] Timm, Trevor. "Your IPhone Is Now Encrypted. The FBI Says It'll Help Kidnappers. Who Do You Believe?" The Gaurdian. September 14, 2014. Accessed February 7, 2015. http://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default.

[4] Cheredar, Tom. "NSA Views Encryption as Evidence of Suspicion and Will Target Those Who Use It, Security Journalist Says." Venturebeat.com. March 10, 2014. Accessed February 8, 2015. http://venturebeat.com/2014/03/10/nsa-views-encryption-as-evidence-of-suspicion-and-will-target-those-who-use-it-security-journalist-says/.

[5] Finley, Klint. "Encrypted Web Traffic More Than Doubles After NSA Revelations | WIRED." Wired.com. March 16, 2014. Accessed February 8, 2015. http://www.wired.com/2014/05/sandvine-report/.

[6] "Major Computer Security Firm RSA Took $10 Mln from NSA to Weaken Encryption - Report." RT USA. December 20, 2013. Accessed February 8, 2015. http://rt.com/usa/rsa-nsa-deal-weaken-encryption-581/.

[7] "Encrypted Internet Traffic Surges in a Year, Research Shows | TorrentFreak." TorrentFreak RSS. May 14, 2014. Accessed February 8, 2015. https://torrentfreak.com/encrypted-internet-traffic-surges-140514/.

[8] Sidel, Robin, Danny Yadron, and Sara Germano. "Target Hit by Credit-Card Breach." WSJ. Accessed February 8, 2015. http://www.wsj.com/articles/SB10001424052702304773104579266743230 2

[9] "Open Letter From UK Security Researchers." Bristol Cryptography Blog:. Accessed February 8, 2015. http://bristolcrypto.blogspot.co.uk/2013/09/open-letter-from-uk-security-researchers.html.

Other Consulted Works

Ball, James. "Cameron Wants to Ban Encryption - He Can Say Goodbye to Digital Britain." The Gaurdian. Accessed February 8, 2015. http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror.

Gillmor, Dan. "Is the Computer Fraud and Abuse Act the 'worst Law in Technology'?" The Gaurdian. Accessed February 8, 2015. http://www.theguardian.com/commentisfree/2013/mar/20/computer-fraud-abuse-act-law-technology.

Jaycox, Mark. "Electronic Frontier Foundation." Electronic Frontier Foundation. January 16, 2015. Accessed February 8, 2015. https://www.eff.org/deeplinks/2015/01/obamas-computer-security-solution-mish-mash-old-outdated-policy-solutions.

O'Connor, Nuala. "Center for Democracy & Technology | Keeping the Internet Open, Innovative and Free." Encryption Makes Us All Safer. October 8, 2014. Accessed February 8, 2015. https://cdt.org/blog/encryption-makes-us-all-safer/.