**Phil Zimmerman: The Incriminated Hero**

In the modern age of technology, humans send several messages through the use of various devices. These include email, text messages, phone calls, and more. While it is impossible to argue against the convenience of these mediums, the safety of them is another issue entirely. Using technology to send sensitive messages can be worrisome, as it can be intercepted and obtained by malicious people.

Some may not worry about the security of their messages, while others flat out refuse to include sensitive information when sending them. However, it would be unwise to simply view the latter as paranoid, given the amount of attacks in the past and in the present. Some recent data breaches include popular companies like eBay and JPMorgan Chase, both which have information that belongs to millions of customers.

The fight to stop these attacks and limit data breaches is a battle that will theoretically go on forever. However, there is one essential tool that helps stop these thieves dead in their tracks: encryption. Encryption is the process of converting plaintext, or a normal readable message, into cipher text, which is a code that is intentionally very difficult to decipher. The math used to generate these cipher texts are what differentiates encryption systems from one another.

While there is are several different encryption systems out there, they can be split into two general categories: symmetric, and asymmetric (or public-key cryptography). Symmetric encryption involves scrambling a message using a secret key that can also be used for *unscrambling* the same message. As a result, they’re generally used for personal needs, as the secret key usually accompanies the data itself. Some symmetric systems that are popular include Data Encryption Standard (DES), Rivest Cipher 4 (RC4), and Advanced Encryption Standard (AES).

However, once asymmetric systems were introduced, symmetric encryption became significantly less useful. Rather than using one key for encryption and decryption, asymmetric systems introduce the idea of *key pairs*, where one key is private and the other key is public. If a message is scrambled using a public key, then the only person who can decrypt it is the person with the private key. The same system can also be used vice versa for message *signing* (MacDonald, *Make it harder for prying eyes to peep your data: Shield it with asymmetric encryption,* 5). If a message is scrambled using a private key, then anyone who decrypts it using the public key will know exactly who the message is from. This is because the private key will only belong to one party, making it an effective way to verify the author of the message.

Symmetric encryption systems definitely have their use cases, but there is no denying that asymmetric systems have become favored for communications over the internet. When it comes to sensitive information like passwords and bank information, it is much more secure to have one private key be held by a trusted party, rather than having a public key floating around and be accessible to the public. An example of an asymmetric system that became popular was Transport Layer Security (TLS).

Public-key cryptography has undoubtedly led to a safer internet, but it has come at the expense of heavy scrutiny by the U.S. government. In 1991, the U.S. Senate attempted to pass a bill that encouraged network industry leaders to install backdoors into their network equipment. (Winder, *The US government has come close to making it illegal to use secure communications online*, 118) This would’ve allowed them to potentially access user data if the government requests for it. The government would benefit greatly from this, as they would be able to get information in case of an investigation or a similar time of need. However, as a result, consumer privacy would always be at the risk of being invaded, which was a major turnoff for most people.

Luckily, the bill never saw the light of day. However, the government’s stance on encryption has remained fairly similar; supportive, but power hungry. This bill caught the attention of Phil Zimmerman, a computer science graduate and software engineer from Camden, New Jersey. Zimmerman was responsible for creating Pretty Good Privacy (or PGP) in 1991, which went on to become the most popular email encryption system on the planet. PGP used a mix of hashing, symmetric cryptography and asymmetric cryptography to create military-level grade protection. It could be used for encryption, decryption, certificate signing and more. Its strength led to a quick surge in popularity, and it still plays a big part in encryption to this day. (Zimmerman, *PGP User's Guide, Volume I: Essential Topics*)

Being the creator of such a popular encryption algorithm, Zimmerman wasn’t fond of the government’s beliefs on how encryption should be handled. In response, he sent the PGP source code, along will all of the documentation, to some of his friends, in hopes that it would eventually become freely available to everyone. It wasn’t long before fellow programmer Kelly Goen uploaded the software to Usenet, an unmoderated newsgroup that was public to the world. To spread it even further, he also uploaded it to a series of forums on the web, and it wasn’t long before PGP was accessible to everyone.

To many, Zimmerman was considered a hero. He released a military grade encryption system that anyone can use for free, and opened a can of worms that not even the government could contain. People who wanted to secure their files were able to do so for free, and no longer had to worry about a third party potentially gaining access to their information. The cherry on top was that it was actually secure, rather than an obsolete or outdated system.

With that being said, PGP still had its fair share of criticisms. For many users, PGP was far too complicated and not user friendly. There was even a paper written that documented the difficulties of using PGP named, “Why Johnny Can’t Encrypt.” (Brody & Sinclair, *Protecting Data Privacy With User-Friendly Software*, 1). In the paper, Alma Whitten and J.D. Tygar found that some users had problems even accomplishing simple tasks like encrypting and decrypting messages, which eliminated its use completely. It’s no easy feat to create a privacy tool that can also be easily understood by the masses, but it was still unfortunate to see that PGP was yet another failure at doing so.

An even more serious criticism was that from the U.S. government. A few years after PGP was released as freeware, Zimmerman and his friends were contacted by US Customs and charged with “exporting protected munitions” without a license. Zimmerman was also indicted by a grand jury and was put under criminal investigation. PGP was labeled as a weapon, since encryption was a common tool used to mask enemy communications, and uploading it freely onto the web was an act of “exporting” the weapon internationally.

All of this was fairly extreme, to say the least. In an effort to protect society from criminals and terrorists, the government was also going against the freedoms of U.S. citizens to protect themselves. (Lerch & Gray, *Cryptography in America*, 1545) The public was outraged, as it was arguably a violation of the First Amendment. Although the First Amendment states that no law shall abridge the freedom of speech, Zimmerman’s case showed that not all acts of speech are actually covered by the amendment. (Post, *Encryption Source Code and the First Amendment*, 713)

It took 3 years for a decision to be made, and during the course of those 3 years, no one knew what the future would be like for cryptography in America. The case was definitely concerning, but in the end, nothing came out of it. The investigation was dropped somewhat suddenly, and no specific reason was given for the decision. When they were asked about why they dropped the case, they refused to comment on the matter.

The general public was somewhat unfazed by the decision, but the internet activists were ecstatic. Zimmerman was a celebrity in their eyes, as he was seen as the small individual who overcame being bullied by big government. PGP was a system that was made for the people, and it survived the government’s onslaught. Zimmerman eventually went on to create PGP Inc, which was acquired by Network Associates in 1997.

PGP has since been cracked and surpassed by other public key systems today, but it’s importance in history cannot be overstated. As time goes on, governments will continue to try to maintain power over cryptography, but Zimmerman and the PGP case will be a solid milestone worth referencing.

BIBLIOGRAPHY

Brody, Sara “Scout” Sinclair. *Protecting Data Privacy With User-Friendly Software.* Council on Foreign Relations, 2016. <http://www.jstor.org/stable/resrep05701>.

Lerch, Irving, and Mary Gray. "Editorial: Crytography in America." *Science* 278, no. 5343 (1997): 1545. <http://www.jstor.org/stable/2894831>.

MacDonald, Matthew. "Make it Harder for Prying Eyes to Peep Your Data: Shield it with Asymmetric Encryption." *Inside Microsoft Visual Basic,*06, 2005, 5-8, <https://search-proquest-com.libezproxy2.syr.edu/docview/191098900?accountid=14214>.

Post, Robert. "Encryption Source Code and the First Amendment." *Berkeley Technology Law Journal* 15, no. 2 (2000): 713-23. <http://www.jstor.org/stable/24116703>.

Winder, Davey. "The US Government has Come Close to Making it Illegal to use Secure Communications Online." *PC Pro,*07, 2017, 118-120, <https://search-proquest-com.libezproxy2.syr.edu/docview/1984752178?accountid=14214>.

Zimmermann, Philip. "PGP User's Guide, Volume I: Essential Topics." PGP User's Guide, Volume I: Essential Topics. October 11, 94. Accessed October 18, 2018. <https://web.pa.msu.edu/reference/pgpdoc1.html>.