ENCRYPTION AS A MUNITION

The World Wide Web is considered to be the "killer app" of the Internet. Because of Sir Tim Berners-Lee's invention, computer networking moved from the world of the military, universities and research institutions, and into everybody's home and business. Electronic commerce followed, but many people do not realise that in early days an important ingredient was missing from the mix. That missing ingredient was strong encryption, and only because we have it now — built in to every browser and every electronic commerce web server — that we are able to think about the Internet as a place to do business. Without using encryption for privacy on the Internet, anyone using the World Wide Web or sending an electronic mail message is effectively sending a postcard. When you send a postcard through the post office, you are sending data that is meant for your recipient, and metadata that is meant for the post office. The data is the picture of a beach on the front and the "Wish you were here!" message on the back, and the metadata is the address and stamp on the back. Only the metadata needs to be seen by the post office to deliver the postcard, but in fact everything is revealed to them. Starting with the invention of the pre-paid adhesive postage stamp in 1840, people started to predominantly use sealed envelopes for private communications, writing only the address as metadata on the outside of the envelope for the post office to see. Today, no one would think to send an important contract or a love letter on a postcard, and the concept of private data and public metadata is well-entrenched in the use of the postal mail.

The same is not true when it comes to the Internet. Following the model of pre-existing technology, the Internet works by sending packets of data with addressing metadata wrapped around. This is called "encapsulation." Each layer is interpreted and unwrapped, until the core of data is revealed to the application (like a web browser) that wanted to communicate over the Internet in the first place. Like the post office, there are many intermediate handlers of a packet. The sequence of bits that is meant for the application running on the remote machine will pass through routers and across networks controlled by different Internet Service Providers, and along the way the sequence of bits will be examined for meaningful metadata, such as an Internet Protocol address indicating the final destination.

What do all those intermediate routers and different ISPs need to see? They only need to see the metadata which is wrapped around the packet of data, because that is what is useful to them to move the packet along towards its final destination. That's just like saying all the post office needs to see is the outside of the envelope in order for them to do their job. But in fact, the entire sequence of bits, including the encapsulated data, is revealed to the "man-in-the-middle" — so sending packets on the Internet is just like sending a postcard. Intermediate entities may not care about what is inside all that addressing information, but if they care to look it is plain to see.

This is where encryption comes in. The man-in-the-middle doesn't need to see what is inside your packet to deliver it. He just needs to see the addressing information on the outside. So what if we obscure the application data inside the packet, using a secret that we share only with our final recipient, and send the packet that way? When the recipient gets the packet (because the addressing metadata is always public and in a plainly-readable form), he will use the shared secret to unscramble the application data, and see what you intended him to see. Now, you are sending letters on the Internet, and no longer sending postcards.

Using strong encryption algorithms to obscure application data inside Internet packets transformed the World Wide Web from a public library type of structure into an engine for electronic commerce. No one would would think of doing on-line banking or purchasing goods and services on-line using a credit card if all of that confidential information was revealed publicly as if it was written on a postcard. Yet, curiously enough, this essential progression almost never came to pass.

For a long time, strong encryption algorithms have been associated with the military. The idea of truly private communications, intelligible exclusively to the two parties to a conversation and completely unintelligible to the man-in-the-middle, has obvious value to the military and to governments. That is why, for much of the twentieth century, governments have tried to keep the algorithms themselves a secret, and not an object for open research. The United States government even went so far as to classify strong encryption as a "munition" and sought to ban its export to countries they did not like. A

touchstone moment occurred in 1991 when Phil Zimmerman created “Pretty Good Privacy”, which he developed entirely from publicly-available information, and proceeded to give away, for free, along with the source code. The U.S. government was horrified, and launched a criminal investigation into Zimmerman for “exporting a munition without a license,” because it was clear that his source code was being distributed everywhere in the world. Zimmerman was never arrested or charged, but he was “investigated” for several years. The U.S. lost its advantage in the world of encryption and its use on the Internet, because researchers elsewhere were developing strong algorithms and deploying them to great effect. Researchers in Finland developed the secure shell, which became a replacement for the venerable telnet and rsh utilities. Dutch researchers developed the Rijndahl algorithm that ironically was adopted by the U.S. government as the “Advanced Encryption Standard” to replace the obsolete “Data Encryption Standard.” And everywhere (except in the U.S.) people were starting to use browsers with 128-bit encryption or stronger, and beginning to use the Internet for electronic commerce.

We now know that the United States government was playing a fool’s game. Cryptography today has very little in common with Enigma machines and U-boats and World War II, as it did seventy years ago. It is a difficult concept to grasp, but it is true. Even when the details of an encryption algorithm are known fully and publicly, the privacy of communications is not weakened. The threat posed by the man-in-the-middle is not that he knows what encryption algorithm you are using, but that he might get a hold of your shared symmetric key. That is why good web sites are carefully constructed with certificates signed by trusted authorities.

It is still early days, and there have been stumbles along the way, like treating strong encryption as a “munition.” But we are well on the way to stopping using the Internet as if we are writing postcards, and starting to use it as if we are writing private letters.

Source : https://www.exitcertified.com/blog/michael/2012/encryption-as-a-munition/