Joshua Lai (804449134)

Jin Wang

Computer Science 35L

02 December 2016

# The Cryptographic Key that Secures the Web

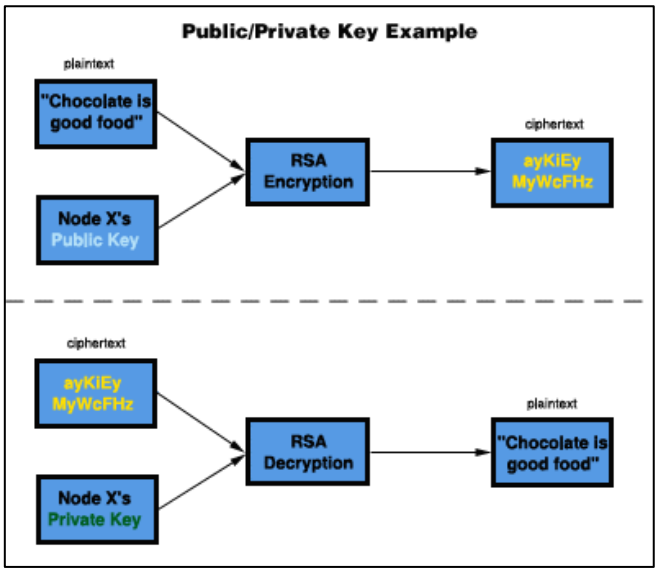
The late 1900's brought about the advent of the Internet, a means of communicating through a computer network. Society now had access to an unparalleled means of contact with those around the world and a bank of unlimited knowledge. Unfortunately, people found ways to use those means for their malicious purposes. In order to protect users, a key was developed in order to encrypt and decrypt information that was sent across the network. Yet, to this day, there are still issues that need to be addressed in order to protect users.

In order for users to go to a webpage (i.e. ww.google.com), the Internet needs to be able to direct the traffic to that specific webpage. In order to do so, the Internet uses the domain name system (DNS) protocol that will use the domain name provided and search for it in the domain name database, where every domain name and its IP address is stored. [1] Once the IP address is found, the DNS protocol will return the IP address and direct the traffic to that website. Although the concept behind the system was revolutionary, the original configuration had flaws, namely, it was not designed to protect its data.

One way to exploit the system is a technique known as DNS cache poisoning, where the protocol is forced to return an invalid IP address, and thus, redirect the traffic to the wrong website. In order to protect the system from these exploits, the Internet Corporation for Assigned Names and Numbers (ICANN) developed a key pair that not only encrypts and decrypts the data being sent across the network, but also checks for valid signatures.[2] Although

this new implementation did increase the protection on the system, the threat was still prevalent as it is possible that the key pair may have been compromised.

Since the founding of ICANN, the key pair has not been changed. Therefore, they found it best that it be changed in the event that the key pair has been compromised. According to ICANN, "We want to roll the key because it's good cryptographic hygiene." In addition to changing the key pair, they also will increase the difficulty of cracking the key pair by increasing its size from 1024 bits to 2048 bits. The public key will be eventually distributed to the public in order to utilize the new security measures.




With the implementation of the new key pair, users can know that their searches on the internet are now more secure. Yet with this increase in the security, there is always still the chance that the private key can be compromised at any time. Thus, it is always good to be cautious when browsing. Although the key pair used by ICANN may be used on a large scale, its concept can be applied to smaller areas, namely, software download and installation. When software is downloaded, there is no check on whether it is valid, and thus, could potentially contain a virus. If the software required a public key and private key for verification of signatures before being installed into the system, then they could be more secure.

---

[1] Paul V. Mockapetris, Kevin J. Dunlap, "Development of the Domain Name System," *SIGCOMM '88 Symposium: Communications, Architectures, and Protocols* (1988): 4-6.

[2] Joseph Cox, "The Cryptographic Key That Secures the Web Is Being Changed for the First Time," *motherboard.vice.com*, September 19, 2016, http://motherboard.vice.com/read/the-encryption-key-that-secures-the-web-is-being-changed-for-the-first-time