Nguyen, Theodore

704-156-701

CS35L Fall 2014 Project 10 Review

Review of "Reinventing the Internet to Make It Safer," By Nicole Perlroth

Despite its looks, advancements, and technology, the Internet at its core is actually an aged, 40-year old entity. In "Reinventing the Internet to Make It Safer," author Nicole Perlroth covers this facet of the Internet, its implications to cybersecurity, and DARPA's efforts to implement a security solution arising from this situation.

The internet was indeed laid out 40 years ago. Then DARPA researchers Vinton Cerf and Robert Khan met together in a Hyatt hotel to lay down the foundations of the Internet - which still exist today, encompassing the backbone of the Internet. These foundations were more specifically the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which made up part of the Internet Protocol Suite (IPS); The two published these findings in their paper called "A Protocol for Packet Network Intercommunication."

Here's a gist of how the IPS works: It consists of four layers - the link layer, the internet layer, the transport layer, and the application layer. The TCP makes up the transport layer, while the IP makes up the internet layer. The two parts essentially work together to transport a file from one host to another. The TCP first breaks down a file into several packets, which are then labeled, to be sent; after the file is received by the other host, the TCP allows the file to be reassembled through the previous labels in order to get the original file. The IP works in this process by imprinting the IP address of the receiving host on the packets; it then essentially does all it can to send the packets to the receiving host in the most efficient manner. In summary, the IP works to get the files from host A to host B, while the TCP works to make sure that the files are in its original form for host B.

Now we have a gist of how IPS works, we return back to the article; despite all the advances in performance we've made throughout the past 40 years, we still have the same Internet, using the same TCP/IP; this may not affect performance, but it very well affects security. The Internet was not built with security in mind, but with performance and cost-effectiveness in mind - that was because 40 years ago, the cost for chips and other technological components were considerably higher than they are now.

Because the Internet was not created with security in mind, the only way to integrate security is through a programmer's code. This is, of course, not exactly ideal - a small programming mistake can render an entire system insecure, and, thus, this puts a lot of pressure and responsibility on the programmer. The programmer must intricately implement security.

A small mistake can really result in a major catastrophe. In April 2012, a serious vulnerability found in the OpenSSL cryptographic software library rendered the service vulnerable to remote attackers, allowing them to perform attacks and retrieve sensitive, private information. This vulnerability came to be known as "The Heartbleed Bug." The software was more or less used by an extremely large amount of commercial organizations and corporations; therefore, as a result of this, several large businesses, including Amazon, Google, and Apple, all had their systems compromised, with private company and customer information leaked - all because of a programming mistake, a single bug.

The catastrophes don't stop there - the Shellshock bug, discovered in September 2014 after 22 years of being undiscovered, was found in GNU's bash shell allowing attackers to run commands remotely on a system. Any and all systems that used GNU's bash shell were compromised, affecting countless businesses and individuals. Just these two vulnerabilities - the Shellshock bug and the Heartbleed bug - affected more than half of all of the Internet, representing how leaving security to the programmer may pose a major risk.

Thus, although occurring before these two major bugs, the Defense Advanced Research Projects Agency, or DARPA, created the Clean Slate program five years ago in order to find out what the Internet might be like if it was created with security in mind. They did this by implementing the ideas of security step by step as they created computer systems from the ground up. Clean Slate consisted of two projects: (1) Crash (Clean-Slate design of resilient, adaptive, secure hosts), and (2) MRC (Mission oriented Resilient Clouds). Crash created self-sufficient systems that could continue to function, adapt, and then repair itself upon being breached with respect to its environment; MRC did essentially the same thing, but with applications to cloud computing and networking.

DARPA also had another project unrelated to Clean Slate, called Active Authentication. Unlike Clean Slate, which allows the machine to respond to its environment, Active Authentication allows the machine to respond to its user. Generally, when a user logs into a system, the user is authenticated once at the username and password input. This approach is susceptible to stolen passwords and other login information. Active Authentication provides a strong alternative to this, as it will analyze the user's behavior while logged into the system; an attacker would thus not be authenticated as the system will know that the attacker is not the user.

Because we have come so far in developing the Internet over the past 40 years, it is not feasible to replace the current infrastructure with a completely new one just for security purposes. Instead, developing a methodology to use existing software with more security settings is more practical. One program part of the Crash project, known as the Clean Slate Trustworthy Secure Research and Development, or Custard, aims to do exactly this. Custard allows software and other technologies to run in a safer mode and choose who has permissions for which operations. Custard can also, quite amazingly, completely eliminate all Buffer Overflow attacks. In the past year, there happily has been an increased demand for Custard in several private corporations, nonprofits, and public academia.

Before reading this article, I thought the Internet was actually pretty secure; I knew that putting sensitive things on the Internet was always just a bad idea as a rule of thumb, but I would always trust big, funded corporations online services to a large extent. This article enlightened me to the fact that Internet security isn't as strong as I think it would be. I have strong ideas about personal privacy in that each person has a right to their own personal information to not be disclosed, and since most of our personal information is stored electronically these days, this article's talk about internet security gives a lot of insight into the concepts.

In conclusion, I must agree that it is definitely impractical to completely replace the current infrastructure for security's sake. However, there will be and should be a higher demand for long-term security as information - and everything - becomes more online and more digital than it already is. There will be a greater need to protect each individual 's and group's person privacy, data, and well -being.

References

[1] *The Heartbleed Bug*, http://heartbleed.com/

[2] *Vulnerability Notes Database*, https://www.kb.cert.org/vuls/

[3] Perlroth, Nicole, "Reinventing the Internet to Make It Safer," *The New York Times,* http://bits.blogs.nytimes.com/2014/12/02/reinventing-the-internet-to-make-it-safer/ December, 2014.

[4] Gilbert, H. *Introduction to TCP/IP,* http://www.yale.edu/pclt/COMM/TCPIP.HTM Feb, 1995.

[5] *#Shellshocker,* https://shellshocker.net/

[6] *Billslater.com*, http://www.billslater.com/internet/