Reinventing the Internet to make it Safer

CS35L Fall 2014 presentations

Theodore Nguyen

Abstract

- The internet was not created with security in mind; programmers have had to incorporate security in their code
- The design of the internet has not changed, and still contains these security flaws, but it is not feasible to start from scratch
- DARPA's Clean Slate program modeled building systems, clouds, and networks with security in mind – kind of like starting over with a clean slate

Outline

- Internet background
- Oldness of computer systems
- Security breaching due to programming mistakes
- DARPA's Clean Slate program
- Thoughts and Conclusion

Internet Background

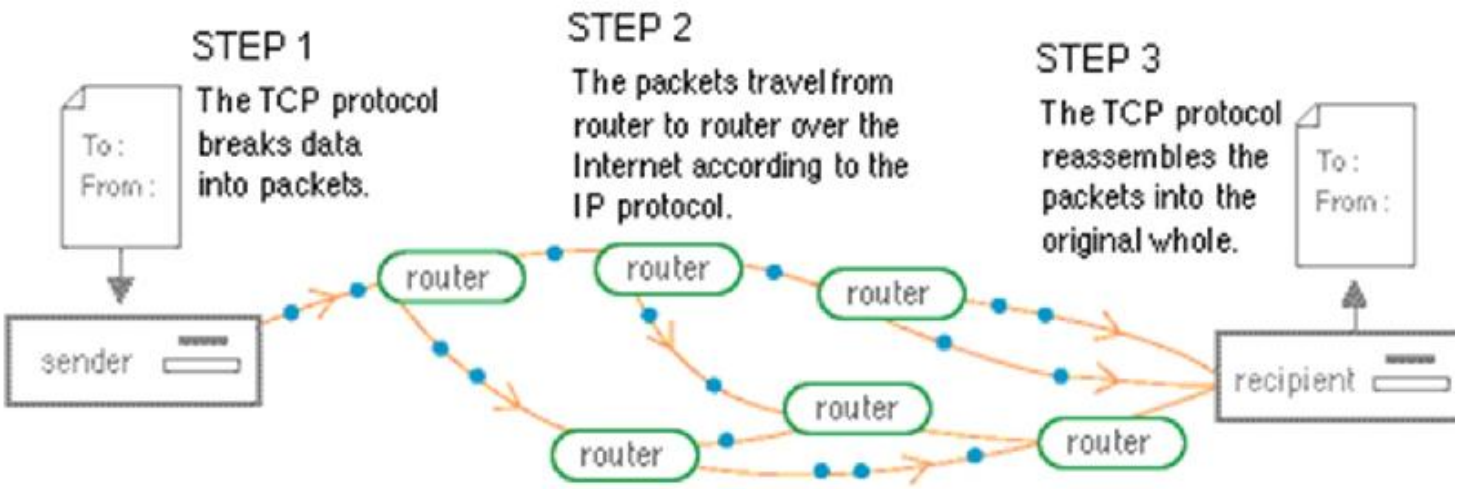

- Vint Cerf, while doing his Ph.D at UCLA, met Robert Kahn, both working on the ARPANET project
- The two came together in a hotel conference room and laid the foundations and backbone of the Internet which still exist today
- More technically, the two created the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which made up the Internet Protocol Suite

Internet Background

- The two published their findings in their paper “A Protocol for Packet Network Intercommunication”
- The Internet Protocol Suite consists of four layers: link, internet, transport, and application
- TCP made up the transport layer, while IP made up the internet layer

Internet Background

- The TCP fragments a file before sending it, and once it is received by the other host, reassembles the file to its original form
- The IP handles the transfer of the data, sending it to a specific IP address in the most efficient manner



Oldness of Computer Systems

- This same Internet concept has formed the backbone of the Internet today, despite all of our advances
- The concept was not created with security in mind, but with cost-effectiveness in mind
  - They had no way to anticipate the future advances, and costs were high at the time

Incorporating Security

- Because the Internet was not designed with security in mind, the programmer must accommodate for security in his code
- However, a small programming mistake could easily make a system insecure
- The lack of security design on the system means the programmer must intricately implement security

The Heartbleed Bug

- Disclosed in April 2012 after two yrs
- Serious vulnerability found in the OpenSSL software library
  - Used by several high profile companies, such as Amazon, Google, etc.
- Compromised sensitive material for all users of OpenSSL, including consumer passwords, and private information used in impersonation

The Shellshock bug

- Disclosed in Sept 2014, after 22 years
- Another serious vulnerability, found in GNU's bash shell allowing remote attackers to run commands on a system
- Affects major businesses as well, but more so any individual or corporation that uses GNU's bash shell

Incorporating Security

- Nevertheless, these are two very serious and recent examples of how leaving security solely up to the programmer poses a serious risk
- These two bugs affect > 50% of the internet
- A small vulnerability in software can have catastrophic widespread results if the software is very popular
- So, its worth wondering whether an Internet with a security backbone in mind can fare well

DARPA's Clean Slate Program

- Five years ago, DARPA started its Clean Slate Program
- The latter essentially had the idea of building computers over, but with security – not performance – in mind integrated in backbone

DARPA's Clean Slate Program

- Clean Slate consisted of two projects:
  - (1) Crash (Clean-Slate design of resilient, adaptive, secure hosts): aimed at making systems that were more resilient and could repair itself upon being breached
  - (2) MRC (Mission-oriented Resilient Clouds): essentially was the same thing as Crash, but applied to networking and cloud computing

DARPA's Clean Slate Program

- Active Authentication: A separate project at DARPA that analyzes human behavior to authenticate the user, rather than just have a one time authentication – the machine is aware of the user
  - Appears to be a good deterrent of stolen passwords
- Clean Slate, on the other hand, makes the machine aware of its environment

DARPA's Clean Slate Program

- Because it is infeasible to replace the existing internet infrastructure with one built with security in mind, developing a methodology to use existing software with more security settings is more plausible
- One program part of the Crash project is called "Clean Slate Trustworthy Secure Research and Development" (aka Custard)

DARPA's Clean Slate Program

- Custard allows software and other technologies to run in a safer mode to choose who had permissions for which operations
  - Can completely eliminate Buffer Overflow attacks
- There has been increased demand for Custard in private companies, nonprofits, and academia research institutions

My Thoughts

- The article enlightened me to the fact that the Internet in its creation was wholly insecure
- I agree that internet security is a very important topic, especially in today's digital age
  - Internet security is directly related to our personal privacy, since all our information is now stored electronically

Conclusions

- It is definitely infeasible to replace the current Internet infrastructure where it is right now
- However, more than likely, there will be a higher demand for long-term security as everything becomes more technologically advanced, and more online

Citations

- http://heartbleed.com/
- https://www.kb.cert.org/vuls/
- http://bits.blogs.nytimes.com/2014/12/02/reinventing-the-internet-to-make-it-safer/?_r=0
- http://www.yale.edu/pclt/COMM/TCPIP.HTM
- https://shellshocker.net/
- http://www.billslater.com/internet/