CS50's Introduction to Cybersecurity

OpenCourseWare

Donate (https://cs50.harvard.edu/donate)

David J. Malan (https://cs.harvard.edu/malan/)
malan@harvard.edu
(https://www.facebook.com/dmalan) (https://github.com/dmalan)
(https://www.instagram.com/davidjmalan/) (https://www.linkedin.com/in/malan/)
(https://www.reddit.com/user/davidjmalan) (https://www.threads.net/@davidjmalan)
(https://twitter.com/davidjmalan)

Lecture 2

Securing Systems

- This is CS50's Introduction to Cybersecurity.
- This week, we are going to focus on networks and systems.
- Last time, we introduced encryption as a way by which to secure information.

Wi-Fi

- Chances are, you have recognized that there are secured and unsecured networks.
- Secured networks utilize encryption to protect data between you and other devices.
- *Wi-Fi Protected Access* or *WPA* is a form of encryption utilized to secure networks.

HTTP

- *Hypertext Transfer Protocol*, or *HTTP*, is an unencrypted way by which to transfer data.
- Utilizing HTTP, one is vulnerable to *Man-in-the-Middle* attacks where an adversary could inject additional HTML code into what one is downloading. Advertisements could be injected into all the web pages you are accessing via HTTP. Further, malicious code could be inserted as well.
- Indeed, there are other threats too. *Packet sniffing* is a way by which an adversary may look inside data that is being transferred between parties. You can imagine how a credit card number placed within an unsecured packet could indeed be detected and stolen by an adversary.
- *Cookies* are small files that websites put on your computer. Cookies may be used by websites to keep track of who you are, present your emails, or keep track of your shopping cart. Cookies make one vulnerable to *session hijacking*, whereby an adversary could inject a *supercookie* to track you.
- How might one defend against such a threat?

HTTPS

- *HTTPS* is a secure protocol for HTTP.
- Traffic between parties is encrypted.
- This is accomplished through *TLS* through public key cryptography.
- A website has a public key that is signed by a third-party called a *certificate* of type *X.509*. These websites also have a private key.
- *Certificate authorities* or *CAs* are trusted third-party companies that issue certificates.
- When you visit a website, your browser downloads the certificate of that website, runs it through an algorithm, and creates a hash.
- Then, it uses the public key of the website and the signature of that certificate provided to an algorithm to verify that it creates the exact hash found prior.
- If these match, the web browser application is satisfied that this is a secured website.

- HTTPS mathematically does keep us secure, but there are exceptions.
- *SSL Stripping* is an attack by which an adversary uses HTTP on a website to redirect traffic to a malicious website. An adversary may even redirect one to an HTTPS-secured domain that is not the intended website.
- One way of mitigating this threat is by implementing *HSTS* or *HTTP strict transport security*, whereby the server tells the browser to direct all traffic to a secure connection.

VPN

- A *VPN*, or *virtual private network*, establishes an encrypted channel between two points.
- Within a VPN, all traffic is encrypted.
- However, there are some side effects.
- Because the pipeline between two parties results in receiving an IP address from the second party, it will appear to services throughout the web that your IP address is that of the second party: not your original IP address!
- Indeed, people often use a VPN to masquerade as being in another country.

SSH

- *SSH* is a secure protocol by which you can execute commands on a remote server.
- If one wants to communicate with a remote computer and execute commands there, one may issue an `ssh` command. The following is an example of using the SSH command to connect to a server at Stanford University. You would still need appropriate credentials and permissions to successfully connect.

  ```
  ssh stanford.edu
  ```

- If one has the appropriate access rights, one can execute commands directly on a remote server.

Ports

- *Port* numbers are used to direct web traffic toward specific services on a server.
- For example, port `80` directs to HTTP, `443` to HTTPS, and `22` to SSH.
- Servers listen to these ports for incoming traffic.
- Accordingly, adversaries may engage in *port scanning* where all potential ports are tried to see if they are accepting traffic.

- *Penetration testing* is an activity that a professional may engage in to check for port-related security vulnerabilities.
- *Ethical hacking* is the legal business of testing for such vulnerabilities.
- A *firewall* is a piece of software that protects various services by blocking unauthorized access, including from compromised services on a device.
- Firewalls utilize *IP addresses*, unique numbers assigned to each computer on a network, to prevent outsiders from participating in traffic.
- Firewalls can also use *deep packet inspection*, where they examine the data within packets for material that may be of interest to your company. This can be used to check to see if you are emailing the press or other parties that may be considered adversaries by your company.
- Deep packet inspection is used via *proxy*, where a device in the middle is used as the path by which traffic comes in an out of the network. It is on this proxy that your school or company may change URLs, log what URL you are attempting to browse to, and, hopefully, protect you against potentially harmful behavior.

Malware

- *Malware* is malicious software that damages a computer or compromises its security.
- A *virus* is a piece of software that attaches itself to your computer. Once installed, it can do nearly anything!
- A *worm* is a malicious piece of software that can move from one computer to another via holes in security.
- A *botnet* is malicious software that, once installed on your computer, infects other computers and can be used by an adversary to issue commands to thousands of infected computers.
- Computers infected by botnets can be used to issue *denial-of-service attacks* whereby lots of requests can be issued to a server for the purpose of slowing or shutting it down. Because so many computers are in a botnet, this type of attack can be called *distributed denial-of-service attacks* from thousands of IP addresses.

Antivirus

- *Antivirus* software detects viruses and hopefully can remove them.
- *Automatic updates* must be enabled to fix security holes in previous iterations of the software.
- Still, one may be vulnerable to *zero-day attacks*, which exploit unknown vulnerabilities in software before the software company has had a chance to create a fix.

Summing Up

In this lesson, you learned about securing systems. You learned…

- How networks are secured in wireless networks;
- How unsecured and secured protocols can be used to send and receive data within a network;
- How virtual private networks can encrypt network traffic;
- About ports and the vulnerabilities that adversaries use to exploit them;
- About malware of various kinds;
- How antivirus software can assist in preventing malicious software from being installed on your computer.

See you next time!