Week 1: Part 3
Internet-Enabled Threats
“The internet was designed to be open, transparent, and interoperable. Security and identity management were secondary objectives in system design. This lower emphasis on security in the internet’s initial design not only gives attackers a built-in advantage. It can also make intrusions difficult to attribute, especially in real time. This structural property of the current architecture of cyberspace means that we cannot rely on the threat of retaliation alone to deter potential attackers. Some adversaries might gamble that they could attack us and escape detection.”

– William J. Lynn III, Deputy Defense Secretary, 2010

The Internet Makes It Easier To Attack

• Security was not a design consideration
• Intelligence is at the edges of the network – distributed among many players
• Access and routing not centrally managed
  – Routing decisions distributed
  – No access control: any system can be added to the Internet
• Bad actors can hide!
How the Internet Creates Vulnerabilities

- **Action at a distance**
- **Asymmetric force**
- **Actors can be anonymous**
- **There are no borders or checkpoints**
  - China and North Korea are the only counties that control data flow to/from their country.
- **No distinction**
  - Hard to distinguish valid data from attacks
  - Can’t tell what code will be harmful until it’s executed
People can now be beyond our control or visibility.
Information Technology has “opened up a whole new asymmetry in future warfare”

— William J. Lynn III, Deputy Defense Secretary, 2010

• Pentagon’s 15,000 networks and 7+ million computers are being probed thousands of times daily

• Traditional deterrence models of retaliation do not apply in cyberspace
Asymmetric Force

• Actors can project or harness greater force. Low barriers to entry. Offense can be more effective than defense. A small number of actors can have a large effect.

• E.g., The Anonymous hacking group that tries to take down corporations or governments, people who send fraud or spam email, or those who send Facebook requests for money.

• Sending millions of messages costs almost nothing

• Small counties can now inflict damage on countries like the US or China
Botnets

- **Botnet = collection of computers owned by innocent people but infected with malicious software**
  - The botnet program periodically contacts a command & control server for directions on what additional software to download and what to run and whom to attack

- **Three common uses are:**
  1. Distributed Denial of Service (DDoS) attacks
     - One company has only so many servers
     - Send too much traffic to the servers and the server gets overloaded
     - Now nobody can get through – even legitimate traffic
     - Data is not destroyed but service is disrupted
     - Attacks come from the network of zombies
  2. Spam mailing
     - Send of tens of millions of malicious emails
  3. Cryptocurrency mining
     - Use the computing power of the zombies
Zeus Botnet

Meet Meris, the new 250,000-strong DDoS botnet terrorizing the internet

- Russian security firm Qrator Labs discover Meris, a new massive IoT botnet abused for DDoS attacks.
- Qrator estimates the size of the botnet at around 250,000 infected devices, most from Latvian vendor MikroTik.
- The Meris botnet broke the record for the largest volumetric DDoS attack twice this summer.
- Its most recent attack peaked at 21.8 million RPS and was aimed at a Russian bank hosting infrastructure on Yandex servers.

Necurs Botnet
2008 Cyberattack on the U.S. Military

- Significant compromise of classified military computer networks
- Started with an infected USB flash drive inserted into a U.S. military laptop at a base in the Middle East
- Malicious code uploaded to a network run by U.S. Central Command
  - Spread onto other systems, allowing data to be transferred under foreign control via a remote command and control server
- Served as an important wake-up call for the U.S. Department of Defense
- Author unknown – suspected Russian hackers because of common code from previous attacks

http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html
Anonymity

• Internet protocols don’t require identification

• We often can’t identify the attacker
  – Nobody knows who ran some of the biggest botnets or cyber attacks.
  – Identifying a source can be difficult.
  – Attack with impunity. We don’t know who fired the missile.

• Make guesses
  – Reverse engineer the code, compare to other malware
  – Identify location of command & control server & who is accessing it
  – Trace packets & propagation

• Sometimes we will never know

• Trust becomes a challenge
  – Are you really communicating with your bank?

Lack of Borders & Checkpoints
We expect you to show up in court...

Allegedly part of hacking team responsible for WannaCry ransomware, attack on Sony Pictures, and others

Allegedly responsible for stealing terabytes of data, including coronavirus research, from western companies in 11 nations
Lack of Distinction in Data

• All bits look the same
• How can you tell which data is malicious?
Attacks
Social engineering

- Manipulating or deceiving targets to get them to take some action that isn’t in their best interest.
  - Example: download software, plug in an infected USB device

- Phishing & spear phishing are forms of social engineering
  - Phishing
    - Email that looks reputable sent to a broad group of people with a malicious link or attachment
  - Spear Phishing
    - Focused attack via email on a particular person or organization

- Social Media or public (or leaked) databases
  - Not always an attack but a great source of information for hackers: vacation schedules, employment info, family, ...
  - Adversary can use this info for impersonation or spear phishing

- Deceptive software: file, scripts
  - Unsafe in many cases as they can open an app and cause it to take action on malicious content
  - Example: execute Visual Basic programs from Microsoft Office documents
Areas of Attack

• **Compromised access, code/command injection**
  – Exploit known (often stolen) credentials – you can buy these
  – Take advantage of coding errors to provide input to execute arbitrary code
  – Includes keystroke logging, camera monitoring, content upload, ransomware

• **Eavesdropping & Man-in-the-middle (MitM) attacks**
  – Intercept traffic to gather login credentials, snoop on data, manipulate data, or take over a communication session

• **Web sites**
  – Offer free downloads: software, books, movies … which will contain malware
  – Reputable sites can get infected … or have ads that take you to malware
  – **Drive-by downloads** – malicious programs that get installed without your consent
Networked Computer vs. Real-World Risks

- Attacking in the computer world via networks is easier & less risky
  ⇒ Computer attacks are more common than real-world attacks

- Privacy rules may be the same but getting data is easier
  - E.g., collect data on recent real-estate sales automatically

- Attack from a distance
  - Cowards can attack – little danger of physical capture

- Easy to cast a wide net
  - Scripting lets you knock on millions of doors
  - Automation enables attacks on a large scale
  - Attacks with small chances of success or small returns are profitable
    - Email scams, phishing, transferring fractional cents, looking for weaknesses
Networked Computer vs. Real-World Risks

• Physical world risks are low (for most of us)
  – Most people are not attacked
  – Most people are not victims of espionage

• Same threats in cyberspace as real-world threats:
  – Theft, vandalism, extortion, fraud, coercion, con games

• Same motivation by criminals
  – But the mechanisms, risks, and access are different
The End