Infrastructure Security

COMP620

"If you spend more on coffee than on IT security, then you will be hacked. What's more, you deserve to be hacked."

Richard A. Clarke

former National Coordinator for Security,

Infrastructure Protection and Counter-terrorism

Infrastructure Security

- Infrastructure security is the security provided to protect infrastructure, especially critical infrastructure, such as airports, highways, rail transport, hospitals, bridges, transport hubs, network communications, media, the electricity grid, dams, power plants, seaports, oil refineries, and water systems

Wikipedia.org/Infrastructure_security

What percent of corporate revenue is spent, on average, on IT security?

A. 8%
B. 1%
C. 0.5%
D. 0.007%
E. 0.0025%

Natural or Intentional

- Natural disasters can impact the infrastructure
  - Hurricanes, tornados and storms
  - Earthquakes
  - Trees falling on power lines or roads
  - Squirrels
- Angry people or organizations can attack the infrastructure

Local or Foreign

Attacks against our infrastructure can come from:

- Individuals – A single individual with the necessary knowledge could disrupt the infrastructure
  - To promote a political agenda
  - To extort the utility
- Terrorist groups – Angry organizations with limited budgets can still launch a cyber attack
- Nation States – Most countries are very concerned about infrastructure security vulnerability in a cyber war

Connectedness

- Almost all services and utilities use networked computers for operation
- Some services are relatively isolated and independent
  - Small town water or sewage system
- Other infrastructure is highly connected
  - Power grid
  - Phone and network
- A highly interconnected utility would appear to be more vulnerable to attack

Power Grid

- Electrical power is fundamental to modern society
- The federal government of the United States admits that the electric power grid is susceptible to cyberwarfare
- Power companies are linked together so they can move supply to where the load is heaviest
- There have been instances of cascading power failure

Infrastructure Attack

- Utilities are vulnerable to all of the cyber attacks we have previously discussed
- Social engineering is still a very powerful tool to attacking any group
- An attacker can sometimes leave software in the utility system that will respond at a later date

Cyberwarfare

- Richard Clarke defines cyberwarfare as “actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption”
- Some countries have made cyberwarfare an integral part of their offensive and defensive strategy

Wikipedia.org/Cyberwarfare

Offense

- Many major countries have organizations trained to attack an opponent if necessary
- The Nation Security Agency (NSA) states that they have both a defensive and offensive role

Defensive Goals

- The goals of a cyberwarfare defensive system include:
  - Prevent cyber attacks against critical infrastructure
  - Reduce national vulnerability to cyber attacks
  - Minimize damage and recovery time from cyber attacks
  - Minimize the impact of misinformation campaigns

Wikipedia.org/Cyberwarfare

Types of Cyberwarfare Threats

- Espionage
- Sabotage
- Propaganda
- Economic disruption

Espionage

- Traditional espionage is not an act of war, nor is cyber-espionage
- Many countries are probably involved
- Cyber espionage may attack either government or civilian targets
  - The usual government secrets
  - Intellectual property and trade secrets

Examples of Cyber-Espionage

- Edward Snowden revealed that the NSA reviewed metadata about phone calls to and from suspect individuals or countries
- NSA recorded nearly every cell phone conversation in the Bahamas and also Kenya, Philippines, Mexico and Afghanistan
- In June 2015 the U.S. Office of Personnel Management (OPM) realized 21.5 million records of personal information was stolen, probably by China

Sabotage

- Cyberwarfare systems can attack both military or civilian systems
- An attacker will want to minimize the opponent's effectiveness
  - Disable communication
  - Disable utilities
  - Disable mobility
  - Cause problems that require the opponent to divert resources

Propaganda

- Attackers often want to get their message to the opponent’s population
- An attacker may masquerade as an official to spread misinformation
- Attackers can also cause panic that can cause significant problems

Economic Disruption

- Attackers can impede the way companies work causes a significant drop in productivity
- Attack against financial institutions can stop commerce
- Manipulation of the markets can cause difficulties

Stuxnet

- Stuxnet is malware that caused physical damage to Iranian uranium purification systems
- Through Windows systems, it located Siemens controller software to increase the speed of centrifuges so they would destroy themselves
- Thought to be created by the United States and Israel
- Does little harm to computers that do not meet specific requirements

Stuxnet Attack

- Stuxnet used multiple previously unknown vulnerabilities
- Initial infection was through a USB flash drive
- It spread quickly across networks using a printer sharing vulnerability and other methods
- It installed device drivers that were digitally signed using stolen certificates
- There were command and control servers in Denmark and Malaysia to update and record information

Found Thumb Drive

- A popular way to spread malware is to put it on a USB thumb drive and leave it in a public location
- Many people will insert it in their computer and, thus, spread malware
- An attacker once put thumb drives in people's mailboxes
- Often the thumb drive will pop-up an advertising offering some fictitious great deal

Which type of attack might cause more damage?

A. Espionage
B. Sabotage
C. Propaganda
D. Economic disruption

Titan Rain

- Titan Rain was a string of cyber operations that compromised a number of agencies within the U.S. and UK government from 2003 to 2007
- Thought to be the largest state-sponsored cyber attack
- Chinese state-sponsored actors are suspected of breaching unclassified networks and U.S. defense contractor networks including those at Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, and NASA

Who Dun It

- Titan Rain was the first instance of state-sponsored espionage from China that was made public
- China denies it lead the attack and suggests that others may have routed the attack through vulnerable Chinese servers

Cyberattacks on Estonia

- In April 2007, Russia launched a cyber attack against Estonia
- Russians were upset about the relocation of an elaborate Soviet-era grave marker and war graves

Which is larger?

A. Georgia the country
B. Georgia the state

Results of the Attack

- Targeted websites of the Estonian parliament, banks, ministries, newspapers and broadcasters
- Many of the attacks were Distributed Denial of Service
- The NATO Cooperative Cyber Defence Centre of Excellence was created shortly after the cyber attack
  - Headquarters are in Tallinn, Estonia

CCDCOE

Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

Who Dun It

- A Commissar of the Nashi pro-Kremlin youth movement in Moldova and Transnistria, Konstantin Goloskokov claimed responsibility
- One ethnic-Russian Estonian national has been charged and convicted

Cyberattacks during the Russo-Georgian War

- Starting on August 7, 2008, Russian troops crossed into Georgia starting a five day war
- Starting July 20, 2008, a Russians attacked Georgian computers
- This may be the first instance of cyberwarfare as part of a shooting war

Russian Cyber Attacks

- In July, the Georgian president’s website was disabled
- On August 5, a Turkish oil pipeline blew up
  - The Kurdistan Workers' Party (PKK) took responsibility
  - Circumstantial evidence indicates it was caused by a cyber attack on the control and safety systems
- On August 8, DDOS attacks peaked
- On 9 August 2008, key sections of Georgia's Internet traffic was rerouted through servers in Russia and Turkey, where the traffic was blocked or diverted

Results

- Many Georgian government and civilian systems were attacked
- Georgians attacked at least one Moscow newspaper website
- Estonia and Poland offered hosting for Georgian governmental website and cyber defense advisors
- The StopGeorgia.ru website had software and instructions for launching a DDOS attack
  - Anyone around the world could participate

Summary

- The usual methods of cyber attack can be used against critical infrastructure
- Disabling the infrastructure can significantly reduce the effectiveness of the opponent
- Reports indicate that the U.S. has insufficient safe guards to protect our infrastructure