CSCI 1800 Cybersecurity and International Relations

Cyber Exploits

John E. Savage

Brown University

Outline

- Types of cybercrime
- Cost and extent of data breaches
- Types of threat
- Examples of major cyber attacks

Principle Security Goals – CIA

- Confidentiality
  - Keeping information secret
- Integrity
  - Ensuring that information is not modified
- Availability
  - Ensuring access to resources

Examples of Criminal Violations

- Confidentiality
  - Theft of data, e.g. identity or corporate secrets
  - Fraud – criminal deception for financial or personal gain
- Integrity
  - Corruption or destruction of attached resources, e.g. poisoned water, destruction of oil refinery, turning off electricity supply
  - Corrupting the supply chain
- Availability
  - Loss of access to resources, e.g. power, water, banks
- Other
  - Offenses, e.g. bullying, child pornography

Protecting Against Cybercrime

- Cybercrime is most serious threat to businesses
  - Cybercrime can be done remotely
- Must think about cybercrime before it happens
  - What are your most important assets?
  - Who has access to them?
  - What is the most common attack vector?
    - Email and humans
  - Have you installed the best defenses?
  - Should you be hunting for attackers all the time?

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than "desktop" equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.

Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.

Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, Macs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

Attack Modalities

- Port scanning
  - Test ports on a website to find an entry point
- Watering hole attack
  - Compromise a site visited regularly by a community
- Email is the primary vector for malware*

*See 2018 Verizon Data Breach Investigations Report

Social Engineering Attacks

- Pretexting
  - Creating an elaborate lie to solicit information
- Phishing attack – social engineering via email
  - Lure users into divulging valuable info
  - Spear phishing is aimed at “whales”
- Vishing – phishing by phone
- Tailgating
  - Following authorized person through security gate
- Quid Pro Quo
  - A favor offered in expectation of a return

Kevin Mitnick

- In 1995 was most wanted cyber criminal in US
- Notorious for vishing and phishing telcos and others.
- Videos: https://www.youtube.com/watch?v=c76ezYgIN28 or https://www.youtube.com/watch?v=CwKrsP2pzpg

2019 Cybercrime Landscape*

- 69% of cyber attacks perpetrated by outsiders
  - Organized crime responsible for 50% of breaches
  - Nation-state related actors accounted for 12%
- 34% of attacks involved insiders – hard to stop!
- 80% of web app attacks due to stolen creds

*See 2019 Verizon Data Breach Investigations Report

2018 Cybercrime Landscape*

- Time to execute a cyberattack:
  - 87% of foothold compromises took minutes or less
- Discovery of attacks:
  - Only 3% of attacks discovered in minutes
  - 68% of attacks took months or more to discover
- Fastest hackers are Russians† (WIRED, 2/2019)
  - From start to full-breach (breakout) in 19 minutes!
  - Data attributed to Dmitri Alperovitch, Crowdstrike

* See 2018 Verizon Data Breach Investigations Report

† https://www.wired.com/story/russian-hackers-speed-intrusion-breach/

Types of Threats

- Small-scale threats
  - Targets a broad audience
  - E.g. malvertising, phising, and spam
- Advanced persistent threats (APTs)
  - Targets an important target
  - E.g. Office of Personnel Management – 2015 loss of SF-86 security clearance background records on 21.5 million Federal employees
- Tactics, techniques, and procedures (TTPs) are different in these two cases

APT TTPs

- Reconnoiter – collect info on possible targets
- Acquire a point of entry – leave a "dropper"
  - Use dropper to download a remote access tool (RAT) from a command and control site
- Move laterally in a network to elevate privilege
- Conduct reconnaissance to find valuable data
- Collect, encrypt and exfiltrate collected data
- Retain long-term foothold

Examples of Major Cyber Attacks

- 1988 Morris Worm
- 2003 Titan Rain exfiltration attack
- 2007 Estonian DDoS attack
- 2009-2010 Stuxnet attack against Iran facility
- 2017 NotPetya most damaging attack to date
  - Cost Merck $1.3 Billion
  - Their insurance companies don't want to pay, claiming that it was a result of cyber conflict!

Morris Worm

- On 11/2/98 William Morris, Cornell student launched very early computer worm from MIT.
- Morris was the first person convicted under the 1986 Computer Fraud and Abuse Act.
- Purpose of worm was to learn size of Internet.
- It attacked Unix software.
- It was one of the first pieces of malware to exploit a buffer overflow vulnerability.

Morris Worm

- Because it infected each machine a large number of times, it slowed Internet to a crawl.
- US Government Accountability Office estimated the cost of the damage at $10M – $100 M.
- DARPA was prompted to establish Computer Emergency Response Team (CERT) Coordination Center at CMU as a result.

Titan Rain

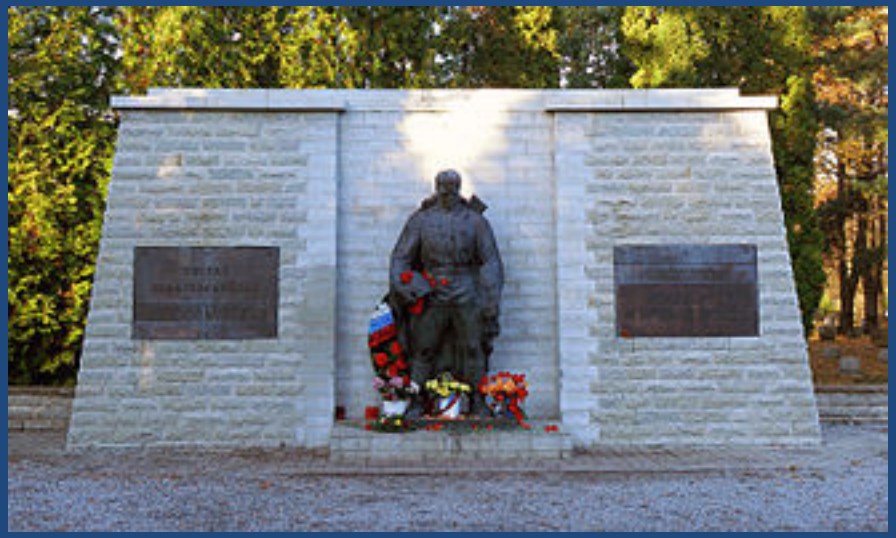
- U.S. government name for attacks on American computers believed to come from China circa 2003-2006
- Purpose was exfiltration of information.
- Hackers penetrated computers at State Department, Homeland Security, Lockheed Martin, Sandia National Labs, NASA, etc..
- Identity of Titan Rain attackers unknown although they used Chinese computers.

Early Experience with Cyber Intrusions

- Sandia Labs analyst Shawn Carpenter followed Titan Rain hackers into routers in Guangdong, China
- Discovered stolen schematics of propulsion systems, Mars Orbiter technology, and more.
- Titan Rain attacks were made against Britain, Canada, Australia, New Zealand.
- Carpenter was initially welcomed by FBI but later declared persona non grata and fired by Sandia.
- Did he violate US law or threaten USG?

Estonian Attack

- In April 2007 Estonia moved Soviet-era "Monument to the Liberators of Tallinn" from city center to a cemetery, provoking outrage among ethnic Russians. (Now called the "Bronze Soldier.")



Cyber Attack on Estonia

- In April, May 2007 Estonian parliament, banks, ministries, papers, & broadcasters under DDoS.
- Second-largest instance of apparent state-sponsored attack at the time.
- Attack appears to come from Russia although at least half the packets originated in US.
- Led to creation of NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) in 5/'08
  - It runs annual Intl. Conf. on Cyber Conflict (CyCon)

2007 DHS Aurora Generator Test

Video is at https://www.youtube.com/watch?v=fJyWngDco3g

DHS Simulated SCADA Attack

- Supervisory Control & Data Acquisition (SCADA)
- In March 2007 Idaho National Lab conducted a test (dubbed Aurora) showing that an electrical power generator could be destroyed by taking control of its control computer.
- Watch the 60 Minutes video on YouTube.

Video is at https://www.youtube.com/watch?v=fJyWngDco3g

Stuxnet

- Computer worm* discovered in July 2010; existed for ≥ 1 year.
- It targets a highly specific industrial control system.
- Designed to degrade and destroy centrifuges at the Natanz uranium refinement facility in Iran.
- Stuxnet a game changer – first serious cyber weapon.

* A computer worm is self-replicating malware

Stuxnet Objective

- Stuxnet targeted systems used to separate U235 from U238 using centrifuge tubes spinning at high speeds.
- Speed of tubes is critical.
  - Too fast and they disintegrate
  - Too slow & separation rate is low
- Stuxnet manipulates speed.
- About 60% of its targets in Iran.

President Mahmoud Ahmadinejad at Natanz, in March 2007

Spread of Stuxnet

- Stuxnet targeted five different Iranian sites.
- First spread by USB drive.
  - By July 2010 any Windows machine could have been infected.
  - Spreads whether or not systems are up to date or whether anti-virus software running.
  - Five different vulnerabilities, four were zero-day.
  - Hides its tracks.

Spreading of Stuxnet

- Stuxnet dormant unless it is on computer that
  - Runs a version of Windows,
  - Runs Siemens Step 7 software,
  - Connected to Siemens programmable logic controllers (PLCs) or
  - Control Fararo Paya (Iran) or Vacon (Finland) frequency controllers.

A PLC is a simple ruggedized computer designed for control systems.

Frequency controllers control centrifuge speed.

Stuxnet Degraded Operation

- Normal controller frequency range: 807Hz–1210 Hz.
- Stuxnet cycles frequency from 1064 Hz (normal) up to 1410 Hz (too high); down to 2 Hz; up to 1064 again, etc.
  - It is in abnormal range for ≤ 50 minutes each time.
  - System is sabotaged by this variation in frequency.
- Typically Stuxnet waits ~13 days after infection before starting sabotage. Additional steps every ~27 days.
- Variation either causes centrifuges to disintegrate or produces low-grade results.
- Meant to suggest that Iran bought inferior centrifuges!

Stuxnet Damage

- Stuxnet code targeted 984 frequency converters
  - When IAEA* inspectors visited Natanz in late 2009, they found 984 centrifuges had disappeared.
- President Ahmadinejad confirmed in November 2010 that cyber attack had damaged centrifuges.
  - But centrifuges were replaced and operations resumed.
- On 11/29/10 Prof. Shahriari, head of Iranian team combating the Stuxnet virus, was assassinated by motorcyclists on streets of Teheran.
- On 1/11/12 Ahmadi-Roshan, supervisor of Iranian uranium enrichment department, was assassinated.

* International Atomic Energy Agency

Clues to Origins of Stuxnet

- Kaspersky Lab speculates Israel behind Stuxnet.
- Value 19790509 is used to decide whether to infect a machine; it may denote May 9, 1979.
  - Date when Jewish-Iranian businessman, Habib Elghanian, executed in Iran after convicted of spying for Israel.
- Code has file b:\myrtus\src\...\guava.pdf
  - Wikipedia says “Esther was originally Hadassah (which) means ‘myrtle’ in Hebrew.” Esther “told the king of Haman’s plan to massacre all Jews in the Persian Empire” who pre-empted the plot by killing plotters.
- But Stuxnet has a primitive command & control system, not typical of a sophisticated Western power.

Origins of Stuxnet

- U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site*, David Sanger (NYT, Jan 10, 2009)
  - Article says President Bush deflected Israeli request to provide it with bunker-busting bombs to attack Iran's main nuclear complex.
  - Says US refused Israeli request to fly over Iraq & into Iran
  - Instead, it "embraced more intensive covert operations actions aimed at Iran"
- Iran later admits it has run into serious problems at Bushehr nuclear reactor, a site it has admitted infected by Stuxnet.

* See http://www.nytimes.com/2009/01/11/washington/11iran.html

New York Times Scoop

- 2012 NYT Report* that Pres. Obama ordered attacks on Iran's nuclear enrichment facilities.
- Code-named Olympic Games in Bush admin.
- Although Stuxnet gets loose in summer 2010, Obama lets 2 new Stuxnet versions be launched.
- Obama said to be aware of Stuxnet precedent!
- For years CIA had injected faulty parts/designs into Iranian facilities without much effect.

* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

More on New York Times Scoop

- US develops software to "phone home" the electrical blueprints of Natanz centrifuge plant.
  - Is this Flame*, espionage malware found in 2012?
- NSA and Israeli Unit 8200 develop Stuxnet worm
- US tests worm on its Pakistani P-1 centrifuges
- Stuxnet first cyber attack to cause physical damage, said Michael Hayden, former CIA chief.
- Iranians confused by random failures.

* http://en.wikipedia.org/wiki/Flame_(malware)

US Electricity Grid at Risk

- US Blames Russia for cyberattacks on power grid – 2018*
  - "Homeland Security officials say that Russia tried to penetrate the US energy power grid, and left tracks to show its hackers had the ability to shut down the grid, but didn't. CNN's Jim Sciutto reports."

* https://www.youtube.com/watch?v=GjsesbT7U-o

Review

- Types of cybercrime
- Cost and extent of data breaches
- Types of threat
- Examples of major cyber attacks
- iClicker questions