Computer Security

01. Introduction

Paul Krzyzanowski
Rutgers University
Spring 2019
What is security?

security

noun security \si-ˈkyuˌr-ə-tē\ 

plural securities

the quality or state of being secure: such as

a: freedom from danger: safety

b: freedom from fear or anxiety

c: freedom from the prospect of being laid off
<job security>
What is computer security?

Keeping systems, programs, and data "safe"

The CIA* Triad:

1. Confidentiality

2. Integrity

3. Availability

*No relationship to the Central Intelligence Agency
Confidentiality

• Keep data & resources hidden
  – Data will only be shared with authorized individuals
  – Sometimes – conceal the existence of data or communication

• Traditional focus of computer security

Data confidentiality:

“The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity].”

– RFC 4949, Internet Security Glossary
Confidentiality vs. privacy

Privacy

– Limit what information can be shared with others
– Ability to send messages anonymously
– Control other’s use of information about you
– Freedom from intrusion
– **Secrecy**: the ability to conceal messages or exchange messages without anyone else seeing them

The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others.

*See: HIPAA, personal information, Privacy Act of 1974, RFC 4949, Internet Security Glossary*

Privacy is a reason for confidentiality
Integrity

- Enabling access to data and resources
- The trustworthiness of the data or resources
- Preventing unauthorized changes to the data or resources

- **Data integrity**
  - Data integrity: property that data has not been modified or destroyed in an unauthorized or accidental manner

- **Origin integrity**
  - Authentication

- **System integrity**
  - The ability of a system to perform its intended function, free from deliberate or inadvertent manipulation

Often more important than confidentiality!
Availability

• Being able to use the data or resources
• Property of a system being accessible and capable of working to required performance specifications

Turning off a computer provides confidentiality & integrity but hurts availability

Denial of Service (DoS) attacks target availability
Thinking about security

Security is **not**
- adding encryption
- … or using a 512-bit key instead of a 64-bit key
- … or changing passwords
- … or setting up a firewall

It is a systems issue
- Hardware + firmware + OS + app software + networking + people
- Processes & procedures, policies, detection, forensics

“Security is a chain: it’s only as secure as the weakest link”
  – Bruce Schneier
By applying a few basic rules, we do not have to worry about computer security
By applying a few basic rules, we do not have to worry about computer security
Security is hard

• Software is complex
  – Windows 10: ~50 million lines of code
  – Google services comprise ~2 billion lines of code
  – Linux distribution: ~200 million lines of code

• Systems are complex
  – Lots of layers: microcode + firmware + OS + libraries + apps + devices
  – Lots of elements: clients, servers, networks, embedded devices
  – Interaction with cloud services
  – Third party components
  – Complex interaction models
  – All parts are not always under control of one administrator

• Human factor
  – People make mistakes
Some big breaches
Some big breaches

• **2006: TJX Companies**
  – 94 million credit cards stolen; cards, banks, insurers lost close to $200 million

• **2008: Heartland Payment Systems**
  – 134 million credit cards processed by 175,000 merchants
  – Well known SQL injection attack – Discovered 10 months after attack

• **2011: Sony’s PlayStation Network**
  – 77 million PlayStation Network accounts hacked – site down for 1 month: $171 million loss
  – 12 million accounts had unencrypted credit card numbers

• **2011: RSA Security**
  – Data on estimated 40 million employees
  – Possibility that information on RSA's SecurID authentication tokens was stolen
  – Two separate hacker groups working with a foreign government launched a series of phishing attacks

• **2013: Target Stores**
  – Credit card & contact information of up to 110 million people

Some big breaches

• **2012-2014: U.S. Office of Personnel Management**
  – Personal information of 22 million current & former federal employees, including security clearance information, family info, every place people lived & traveled, & fingerprint data
  – Well known SQL injection attack – Discovered 10 months after attack

• **2013: Yahoo!**
  – Names, addresses, dates of birth, phone #s, passwords, security questions of 3 billion accounts

• **2013: Adobe**
  – Hackers stole nearly 3M encrypted credit card records & login information for ~150M users

• **2014: Yahoo!**
  – Names, addresses, dates of birth, phone #s of 500M users

• **2014: eBay**
  – Names, addresses, birthdays, encrypted passwords of 145 million users
  – Hackers used credentials of three employees and had complete inside access

• **2014: JP Morgan Chase**
  – Contact & internal info of 76 million households & 7 million small businesses
  – Israeli hackers gained root privileges on >90 of the bank’s servers
  – JP Morgan spends $250 million on security every year!
Some big breaches

- **2014: Home Depot**
  - 56 million credit cards
  - Malware that posed as anti-virus software

- **2014-2018: Marriott**
  - Contact info, passport numbers, travel information, credit cards of 100M customers

- **2015: Anthem Insurance**
  - Contact info, birth dates, and social security numbers of 78.7 million current and former customers

- **2016: Adult Friend Finder**
  - 20 years of data from six databases covering 412.2 million accounts

- **2017: Equifax**
  - Names, addresses, social security #s, birth dates, etc. of 143 million customers
  - Application vulnerability

- **2016: Uber**
  - Personal information of 57 million Uber users and 600,000 drivers
  - Uber’s GitHub account accessed, which gave hackers access to Uber’s AWS account
  - Uber paid the hackers $100,000 to destroy the data (with no proof that was done!)

Just a few recent security breaches
Some 2018 Attacks

- **Iranian attacks on universities**
  - Nine Iranian hackers indicted for attacks on more than 300 Universities in the U.S. and abroad, as well as private companies, the United Nations, the U.S. Federal Energy Regulatory Commission, Hawaii, and Indiana
  - Stole 31 TB of data
  - Attacks used spear phishing emails with malicious links to obtain login credentials

- **Under Armour**
  - MyFitnessPal app breached in late February 2018
  - Names, email addresses, and passwords of 150 million users

- **VPNFilter**
  - Russian hacking campaign impacted more than 500,000 routers worldwide
  - VPNFilter malware coordinates devices to create a massive botnet
  - Infects routers from Netgear, TP-Link, Linksys, ASUS, D-Link, Huawei

https://www.wired.com/story/2018-worst-hacks-so-far/
January 2018

• **Unique Identification Authority of India hacked**
  – Personal data of more than 1 billion people made available for purchase

• **Text messages, call logs, and files from journalists, military officers, corporations in 21 countries stolen**
  – Six-year campaign by hackers with ties to the Lebanese General Directorate of General Security

• **Japan-based cryptocurrency exchange lost $530 million**
  – Largest cryptocurrency heist
February 2018

• Russian hackers penetrated voter registration rolls of several U.S. states prior to 2016 election
  – Confirmed by U.S. Department of Homeland Security in 2018
  – 13 Russians and three companies indicted

• 17 GB of data stolen from Germany’s foreign and interior ministries
  – Russian hacking group – undetected for a year
March 2018

- North Korean hacking group has been targeting major Turkish banks and government finance agencies
  - Same group linked to SWIFT financial network attacks

- Under Armor data breach compromised information of 150 million users of its MyFitnessPal app

- FBI and Department of Homeland Security issue joint alert to warn of Russian cyber attacks against critical U.S. infrastructure
  - Water, energy, nuclear, aviation, manufacturing

- Iran indicted of stealing intellectual property from >300 universities, government agencies, and financial services companies

- Baltimore’s 911 dispatch system taken down for 17 hours
  - Ransomware attack

- Online services for Atlanta were disrupted
  - Ransomware attack that demanded $55,000
  - Cost $2.6 million to recover
April 2018

- North Korean group responsible for SWIFT attacks targeted Central American online casino
- All government services of St Maarten were taken offline for a week after a cyber attack (third attack in a year)
- UK has been conducting offensive cyber operations against ISIS
- US & UK warn that Russia has been compromising home & business routers
- Chinese state-sponsored hacking groups targeted Japanese companies to get info on Japan’s policies toward North Korea
- North Korean hackers targeted critical infrastructure, finance, healthcare, and other industries in 17 countries
- Indian hacking group had been targeting government & research agencies in China and Pakistan since 2013
May 2018

- US announces withdrawal from the Iran nuclear agreement
  - News results in an immediate increase in Iranian hacking activity

- Turkish government hackers use surveillance software to infect Turkish dissidents & protesters

- Pakistani military used Facebook Messenger to distribute spyware to targets in the Middle East, Afghanistan, and India

- North Korean hackers had been targeting defectors through compromised Android apps hosted on Google Play market
June 2018

- Chinese government hackers compromised networks of a U.S. Navy contractor

- North Korean hackers targeted a South Korean think tank focused on national security issues
  - Used a zero-day exploit to compromise website & insert a back door for injecting code

- Chinese hackers were found to be engaged in a cyber espionage campaign
  - Collect data from satellite, telecom, and defense organizations in the U.S. and Southeast Asia

- Ukraine police claim that Russian hackers have been targeting Ukrainian banks, energy companies, and other organizations
  - Establish backdoors in preparation for a wide-scale strike against the country

- Data breach at marketing firm Exactis
  - Leaked information of 340 million people, including political preferences, browsing habits, & purchase data
July 2018

- Chinese hackers had been actively spying on political actors on both sides of the upcoming Cambodian elections
- Ukrainian intelligence officials claim to have thwarted a Russian attack on the network equipment of a chlorine plant in central Ukraine
- Singapore’s largest healthcare institution was targeted by state-sponsored hackers
  - Personal information for 1.5 million patients leaked
- Russian hackers targeted the Italian navy with malware designed to insert a backdoor into infected networks
- Microsoft reveals that Russian hackers had targeted the campaigns of three Democratic candidates running for the 2018 midterm elections
- Iranian hacking group had been targeting the industrial control systems of electric utility companies in the U.S., Europe, East Asia, and the Middle East
August 2018

- Microsoft announces that Russian hackers had targeted U.S. Senators and conservative think tanks critical of Russia
- Iranian hackers had targeted the websites and login pages of 76 universities in 14 countries
- North Korean hackers stole $13.5 million from India’s Cosmos Bank
  - Break into bank’s systems & authorize thousands of ATM withdrawals and money transfers through the SWIFT financial network
September 2018

• **Iranian hackers have been surveilling Iranian citizens since 2016**
  – Part of a mobile spyware campaign directed at ISIS supporters and members of the Kurdish ethnic group

• **Two Russian spies caught in the Netherlands**
  – Had been preparing to use cyber tools to sabotage the Swiss defense lab analyzing the nerve agent used to poison former Russian Agent Sergei Skripal

• **The U.S. State Department suffers a breach of one of its unclassified email systems**

• **36 different governments deployed Pegasus spyware against targets in at least 45 countries, including the U.S., France, Canada, and the UK**

• **Russian hacking group had used malware to target the firmware of computers at government institutions in the Balkans and in Central and Eastern Europe**
October 2018

- Security Service of Ukraine announced that a Russian group had carried out an attempted hack on the information and telecommunication systems of Ukrainian government groups.

- Centers for Medicare and Medicaid Services announced that hackers had compromised a government computer system.
  - Accessed personal data of 75,000 people ahead of the ACA sign-up season.


- U.S. Department of Justice indicted Chinese intelligence officers and hackers working for them for engaging in a campaign to hack into U.S. aerospace companies and steal information.

- Head of Iran’s civil defense agency announced that the country had recently neutralized a new, more sophisticated version of Stuxnet.
November 2018

• Australian defense shipbuilder Austal hacked
  – Theft of unclassified ship designs which were later sold online

• Iranian domestic surveillance campaign identified
  – Monitors dissent targeting Telegram and Instagram users

• Pakistani Air Force targeted by nation-state hackers with access to zero-day exploits

• Ukraine’s CERT discovered malware in the computer systems of Ukraine state agencies believed to be implanted as a precursor for a future large-scale cyber attack

• Russian hackers impersonating U.S. State Department officials attempted to gain access to the computer systems of military and law enforcement agencies, defense contractors, and media companies

• North Korean hackers were found to have used malware to steal tens of millions of dollars from ATMs across Asia and Africa

• Chinese state media reports that the country had been the victim of multiple attacks by foreign hackers in 2018
November 2018: Marriott Hotels

- **Information of approximately 500 million guests stolen**
  - Name, address, phone, email, passport, … for 327 million guests

- **Chinese hackers suspected**

- **But the credit card data was encrypted!**

  “For some, the information also includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken.”
December 2018

- Chinese hackers were found to have compromised the EU’s communications systems
  - Access to sensitive diplomatic cables for several years

- North Korean hackers stole the personal information of almost 1,000 North Korean defectors living in South Korea

- U.S., Australia, Canada, the UK, and New Zealand, accused China for conducting a 12-year campaign of cyber espionage
  - Targeting the IP and trade secrets of companies across 12 countries

- State-sponsored Middle Eastern hacking group targeted telecommunications companies, government embassies, and a Russian oil company located across Pakistan, Russia, Saudi Arabia, Turkey, and North America

- Italian oil company Saipem was targeted by hackers
  - Hundreds of systems in the UAE, Saudi Arabia, Scotland, and India taken down
Some more things to worry about
Hacking

When a tanker vanishes, all the evidence points to Russia

In June, 37,000-tonne tanker vanished from GPS off the Russian coast. All the evidence points to Russia. But what’s really going on?

By MATT BURGESS
21 Sep 2017

Credit iStock / MarioGiulii

or Gurvan Le Meur it started out as a regular voyage. In June this year, the captain of the 37,000-tonne Atria tanker directed his ship through the Marmara sea, along the narrow Bosphorus strait, and into the vast Black Sea. It was a straightforward one-and-a-half day journey. But this changed when Le Meur
Oct 2017 – Spear phishing from govt servers

A New Spear Phishing Attack Uses Compromised Government Email Servers And DNS

by Stu (KnowBe4) on Oct 15, 2017 at 9:13 AM
Brand Representative for KnowBe4

Cisco's Talos malware researchers posted about a highly sophisticated, targeted spear phishing attack using malicious Word attachments, spoofed to look like it was from the U.S. Securities and Exchange Commission EDGAR filing system, and used DNS to create a bidirectional Command & Control channel. The Word attachments contained SEC logos and branding, social engineering the user to believe that the emails were legit and click on prompts.
Fall 2018-now – Cryptojacking

Cryptojacking, which exploded in popularity this fall, has an ostensibly worthy goal: Use an untapped resource to create an alternative revenue stream for games or media sites, and reduce reliance on ads. It works by embedding a JavaScript component in a website that can leverage a
Jan 2018 – Meltdown & Spectre

• Intel chips do not do full memory protection when doing speculative execution

• Vulnerability existed for 20 years!

• Meltdown
  – Allows processes to access kernel memory

• Spectre
  – Allows processes to steal data from the memory of other processes

• Also affects ARM & AMD CPUs
Hacking has consequences

Justice Department Announces Charges And Guilty Pleas In Three Computer Crime Cases Involving Significant Cyber Attacks

Defendants Responsible for Rutgers University Hack, Creating Mirai and clickfraud Botnets, Infecting Hundreds of Thousands of Devices with Malicious Software

TRENTON, N.J. – The Justice Department announced today guilty pleas in three cybercrime cases. In the District of New Jersey, one defendant also pleaded guilty to launching a cyber attack on the Rutgers University computer network, and in the District of Alaska, that defendant and two others pleaded guilty to creating and operating two botnets, which targeted “Internet of Things” (IoT) devices.

Acting U.S. Attorney William E. Fitzpatrick of the District of New Jersey; Acting Assistant Attorney General John P. Cronan of the Justice Department’s Criminal Division; Special Agent in Charge Timothy Gallagher of the FBI’s Newark Division; U.S. Attorney Bryan D. Schroder of the District of Alaska; and Special Agent in Charge Marlin L. Ritzman of the FBI’s Anchorage Division and made the announcement.
Potential for physical harm

US warns of unusual cybersecurity flaw in heart devices

The Homeland Security Department warned Tuesday about an unusual cybersecurity flaw for one manufacturer’s implantable heart devices that it said could allow hackers to remotely take control of a person’s defibrillator or pacemaker.

Jan. 10, 2017, at 7:07 p.m.

By TAMI ABDOLLAH and MATTHEW PERRONE, Associated Press

WASHINGTON (AP) — The Homeland Security Department warned Tuesday about an unusual cybersecurity flaw for one manufacturer’s implantable heart devices that it said could allow hackers to remotely take control of a person’s defibrillator or pacemaker.

Information on the security flaw, identified by researchers at MedSec Holdings in reports months ago, was only formally made public after the manufacturer, St. Jude Medical, made a software repair available Monday. MedSec is a cybersecurity research company that focuses on the health-care industry.
Nation State Attacks
What about our spies?

Government agencies try to develop – and pay for – the best attacking & defense techniques

But…
The American Military Sucks at Cybersecurity

A new report from US military watchdogs outlines hundreds of cybersecurity vulnerabilities.

Matthew Gault • January 23, 2019

The Department of Defense is terrible at cybersecurity. That’s the assessment of the Pentagon's Inspector General (IG), who did a deep dive into the American military’s ability to keep its cyber shit on lockdown. The results aren’t great. “As of September 30, 2018, there were 266 open cybersecurity-related recommendations, dating as far back as 2008,” the Inspector General said in a new report.

The new report is a summary of the IG’s investigations into Pentagon cybersecurity over the previous year. It looked at 20 unclassified and four classified reports that detailed problems with cybersecurity and followed up to see if they’d been addressed. Previously, the IG had recommended the Pentagon take 159 different steps to improve security. It only took 19 of them.

https://motherboard.vice.com/en_us/article/7xy5ky/the-american-military-sucks-at-cybersecurity
March 2017 – Wikileaks publishes CIA Vault 7

- 8,761 documents stolen from the CIA
- Document spying operations & hacking tools
- iOS and Android vulnerabilities
- Bugs in Windows
- Ability to turn some smart TVs into listening devices
April 2017 – Theft from the NSA

• Shadow Brokers – the group that leaked a gigabyte of the National Security Agency's weaponized software exploits over an eight-month period

• Most vulnerabilities were patched … but lots of systems never get updated
Sept 2017 – TAO tools theft from NSA

- Former NSA contractor stole >50 TB of highly sensitive data
- Includes 75% of hacking tools belonging to NSA's Tailored Access Operations
- "took NSA materials home so that he could become better at his job"
- "Theft came to light during the investigation of a series of NSA-developed exploits that were mysteriously published online by a group calling itself Shadow Brokers."
Some Nation-State Attacks (probably)

• **2005-2010: Stuxnet**
  – Attack on Iran’s nuclear power program
  – Malware designed to target Siemens SCADA systems and damage 984 uranium enrichment centrifuges
  – Demonstrates capabilities of a nation state attack on infrastructure
  – Israel & the U.S. allegedly responsible

• **2015: First known successful cyber attack on a power grid**
  – 30 substations were switched off and 230,000 people were without power for 1-6 hours
  – Attacks carried out from computers with Russian IP addresses

• **2018 and earlier: Russian accesses U.S. infrastructure**
  – Russian hackers had direct access to an American power company’s control systems
  – Lays groundwork for future attacks

• **2017: NotPetya malware attacks on Ukraine (and other places): >$10B damages**
  – Banks, ministries, newspapers, and electricity firms affected
  – Originated from an update to a Ukrainian tax accounting package called MeDoc

• **U.S. & UK governments identify China’s ZTE and Huawei as national security risks**

Nation-State Attacks: WannaCry ransomware

2017

• Hits 100s of thousands of computers
  – Mostly in the UK’s NHS

• Ransomware
  – Encrypted contents of data
  – Demanded bitcoin payment

• Blamed on North Korea

• Exploited leaked Shadow Brokers Windows vulnerabilities
Security Goals & Definitions
Security Goals

• **Prevention**: prevent attackers from violating security policy
  – Implement mechanisms that users cannot override
  – *Example*: ask for a password

• **Detection**: detect & report attacks
  – Important when prevention fails
  – Indicates & identifies weaknesses with prevention
  – Also: detect attacks even if prevention is successful

• **Recovery**: stop the attack, repair damage
  – … Or continue to function correctly even if attack succeeds
  – Forensics: identify what happened so you can fix it
  – *Example*: restoration from backups
Policies & Mechanisms

**Policy**: what is or is not allowed
- Can be expressed in natural language (“this is our security policy”)
- Mathematics
- Policy language - to provide precision together with ease of understanding

**Mechanisms**: implement and enforce policies
- E.g., password entry & authentication

- *What mechanisms do we need to secure a system?*
- *What level of assurance is associated with them?*
Security Engineering

• Security Architecture
  – How do we put a secure system together?
  – How do we identify potential weaknesses?

• Security Engineering
  – Implement mechanisms & policy into a system

• Engineering = making compromises
  – Understand tradeoffs
  – Security vs. cost, performance, acceptability, usability, security
  – Cost-benefit analysis
    • Is it cheaper to prevent an attack or recover?
    • Who pays & who gets punished?
      – Microsoft is not responsible for dealing with your loss
Protection: Know Your Enemy!

Different attackers

... Who have different goals

... And different skill levels

What we want to – or need to – guard against?
What are you securing your system against?

And from whom?

– Yourself accidentally deleting important system files?
– Your colleagues not being able to look at your files on a file server?
– A company trying to find out about you and get personal data?
– A phone carrier tracking your movement?
– A grenade destroying your system?
– Video surveillance on streets?
– The NSA?
Risk analysis

• **Should** we protect something?
• How carefully?
• How much should we spend?

**Laws & customs**

• Are any security measures illegal?
  – Example: types of encryption

• Are any measures unlikely to be used?
  – Example: retina scans, urine tests
  – Conformance: balance security vs. effort
Definitions

• Vulnerability
  – A weakness in the implementation or operation of a system

• Attack
  – A means of exploiting a vulnerability

• Threat
  – an adversary that is capable of attacking
Vulnerabilities

• Failures in the system
• Bugs
• Big focus in security classes

What if a system had no vulnerabilities?
Would you not worry about threats?
Threats

• Lot of variations

• Different attackers have different abilities

• Are enemies sufficiently motivated to attack you?

• Attackers can often resort to the three Bs:
  – Burglary, Bribery, or Blackmail

https://xkcd.com/538/
Threat categories

- **Disclosure**: Unauthorized access to data
  - *Snooping (wiretapping)*

- **Deception**: Acceptance of false data
  - *Injection of data, modification of data, denial of receipt*

- **Disruption**: Interruption or prevention of correct operation
  - *Denial of service, data deletion, or modification*

- **Usurpation**: Unauthorized control of some part of a system
  - *May lead to modification, spoofing, delay, denial of service*
Types of threats

- **Snooping**: unauthorized interception of information
  - Form of disclosure
  - Counter with confidentiality services

- **Modification or alteration**: unauthorized change of information
  - Form of deception, disruption or usurpation
  - Counter with integrity services

- **Masquerading or spoofing**: impersonation of one entity by another
  - Form of deception and usurpation
  - Counter with integrity services

- **Repudiation of origin**: false denial that an entity sent or created something
  - Form of deception and usurpation
  - Counter with integrity services
Types of threats

• **Denial of receipt**: false denial that an entity received data or a message
  – Form of deception
  – Counter with integrity & availability mechanisms

• **Delay**: temporary inhibition of a service
  – Form of disruption (possibly via usurpation)
  – Counter with availability mechanisms

• **Denial of service**: long-term inhibition of a service
  – Form of disruption (possibly via usurpation)
  – Counter with availability mechanisms
“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!
Conficker worm: 2008

• Used bugs in Microsoft Windows and dictionary attacks on passwords to propagate and form a botnet

• Infected millions of computers in over 190 countries
  - United Kingdom Ministry of Defence, Bundeswehr (German armed forces), French Navy, Manchester City Council, Manchester Police Network

• Origin: unknown (speculation is Ukraine)
How the Internet Creates Vulnerabilities

- **Action at a distance**
  - People can be beyond our control or visibility.

- **Asymmetric medium**
  - 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., Anonymous, fraud spam email, or Facebook requests for money.
  - Sending millions of messages costs almost nothing
  - Small counties can hurt countries like the US or China.

- **Actors can be anonymous**
  - Nobody knows who ran Conficker. Identifying a source can be difficult.
  - Attack with impunity. Trust becomes a challenge. Are you really communicating with your bank? We don’t know who fired the missile.

- **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
Asymmetric force

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

• Example: Distributed Denial of Service (DDoS)
  – One company has only so many servers
    • Overload the servers and the server gets overloaded
    • Nobody can get through
    • Nothing happens to the data but service is disrupted
  – Attacks come from a network of helpers
    • Many attacks are carried out by botnets - computers owned by innocent people with malware
    • The botnet program periodically contacts a command & control server for directions
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

• Defense against this was named Operation Buckshot Yankee

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

• **Social engineering**
  – Manipulating, influencing, or deceiving targets to get them to take some action that isn’t in their best interest.
  – E.g., 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
  – Often from bank or shipping company asking you to click on a link and fill out a form – or has a malicious attachment

• **Spear Phishing**
  – Small, focused attack via email on a particular person or organization
  – Often contains highly specific information known to the target: account number, name of friend
Areas of Attack

• **Malware**
  – Umbrella term for malicious software
  – Includes keystroke logging, camera monitoring, content upload, ransomware

• **File types**
  – 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

• **Web sites**
  – Offer free downloads: software, books, movies
  – Reputable sites can get infected
  – Drive-by downloads

• **Social Media**
  – Not an attack but a great source of information for hackers
  – E.g., post when you’re going on vacation or going on a conference
  – Adversary can use this info for impersonation or spear phishing
Computer vs. Real-World Risks

• Attacking in the computer world 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
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
Types of attacks

• Joy hacks
  – Beginners, hacking for fun, little knowledge or focus

• Opportunistic attacks
  – May be skilled but will attack any vulnerable target
  – They’re not out to get you specifically

• Targeted attacks
  • They’re out to get you
  • Will gather background info on you
  • But not high skill level

• Advanced Persistent Threats
  – Skilled & focused attackers
  – Undetected for an extended period
  – Most difficult to guard against
  – Skilled criminals to intelligence agencies
Assess adversaries by skill vs. focus

- **High Skill, Low Focus**: Joy hacks
- **High Skill, High Focus**: Advanced Persistent Threats
- **Low Skill, Low Focus**: Opportunistic hacks
- **Low Skill, High Focus**: Targeted attacks
Characteristics of attackers

• Goals
  – Damage, financial gain, get information
  – Knowing goals helps develop countermeasures

• Levels of access
  – Insiders vs. outsiders

• Risk tolerance
  – Are you willing to die? Go to jail?

• Resources
  – With money, you can buy computers & expertise – or bribe someone
  – Time is also a resource

• Expertise

• Economics
  – A rational adversary will balance time, money, risk, and likelihood of success
Who are the adversaries?

• Hackers
  – Good or evil
  – Test boundaries of the system – get to know system better than designers
  – Only a small % are smart; the rest are script kiddies

• Lone criminals
  – Individuals or small groups
  – Don’t necessarily reap huge $ but are often creative

• Malicious insiders
  – Insidious because they are indistinguishable from legitimate, trusted insiders
  – Perimeter defenses don’t work
  – Often have high levels of access
  – E.g., Edward Snowden (sysadmins can have a LOT of access)
Who are the adversaries?

• Industrial spies
  – Product designs, trade secrets, project bids, finances, employee info
  – Can hire/bribe employees to reveal trade secrets or become inside attackers
  – … or resort to dumpster diving
  – Risk averse: reputation of company (or country) damaged if caught

• Press (& politicians)
  – Get the scoop!
  – Social engineering, bribing, dumpster diving, track movements, eavesdrop, break in
  – Also generally risk averse for fear of losing one’s reputation & career
Who are the adversaries?

• Organized crime
  – More opportunities to make money!
    Steal & sell cell phone IDs, credit card #s, debit card info, get cash
  – Money laundering easier with EFT and anonymous currency like bitcoin

• Police
  – Risk averse but have law on their side (e.g., search warrants, seizing evidence)
  – Not above breaking law: wiretaps, destruction of evidence, disabling body cameras, illegal search & seizure

• Terrorists (freedom fighters)
  – Motivated by geopolitics, religion, or a set of ethics
  – Examples: Earth First, Hezbollah, ISIS, Aryan Nations, Greenpeace, and PETA
  – Usually more concerned with causing harm than getting specific information
  – Usually (not always) low budgets & low skill levels
Who are the adversaries?

• National intelligence organizations
  – Huge money & long-term goals
  – Somewhat risk averse
    • Bad public relations
    • Do not want leaks to reveal attack techniques
  – Often have a lot of influence
    • NSA was instrumental in the adoption of 56-bit keys for DES or the Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator)
    • Lenovo computers, owned partially by the Chinese government’s Academy of Sciences has been accused of “malicious circuits” built into the computers
    • NSA planted backdoors into Cisco routers built for export that allows the NSA to intercept any communications through those routers.

• Infowarriors – cyber warfare
  – Huge money & short-term goals
  – Disrupt power grids, commerce, transportation
  – EMP weapons, spread selective information, misinformation, blackmail
Attacks & threats: Criminal attacks

• Fraud

• Theft (financial)

• Scams
  – Pay $$ and get little or nothing back: pyramid schemes, fake auctions

• Destruction
  – Sometimes we want to make data accessible but keep control of its distribution: software, music, movies, photos, books

• Intellectual property theft

• Identity theft

• Brand theft
Attacks & threats: Privacy violations

- Surveillance
- Databases
- Traffic analysis
- Large-scale surveillance
  - E.g., ECHELON
Other attacks & threats

- Publicity attacks
- Availability attacks
  - DoS, DDoS
Threat models

• Set of assumptions about the abilities of an adversary

• A way to identify & prioritize potential threats from an attacker’s point of view
  – Think about things that could go wrong
  – Bad guys don’t follow rules: they don’t care about your policies
  – We need to understand what types of attacks are possible

• Assess
  – What’s valuable?
  – Where will you be likely to be attacked?
  – What are the most significant threats?

• Think about entities in the system, how they communicate & store data
  – Where are the trust boundaries?
  – Where and how is protection enforced?
Trusted Computing Base (TCB)

• TCB
  – All hardware & software of a computing system critical to its security
  – “The totality of protection mechanisms within it, including hardware, firmware, and software, the combination of which is responsible for enforcing a computer security policy.”
    – Orange Book
      U.S. Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)

• If the TCB is compromised, we can no longer guarantee the security of a system

• Software that is part of the TCB must protect itself against tampering
  – Operating system memory protection is an example of this: an application may be compromised but the operating system is still intact and unaffected
The human element

Humans are
- Bad at storing keys
- Poor at estimating risk
- Not accurate
- Careless
- Gullible

Social engineering is a top threat

DEAR DIARY,
HELLO. I AM THE CROWN PRINCE OF NIGERIA. I HAVE RECENTLY COME INTO A LARGE FORTUNE, BUT...

https://xkcd.com/1777/

It turns out that halfway clever phishing attacks really, really work

A new phishing attack hops from one Gmail account to the next by searching through compromised users' previous emails for messages with attachments, then replies them from the compromised account, replacing the link to the attachment with a lookalike that sends you to a fake Google login page (they use some trickery to hide the fake in the location bar); the attackers stand by and if you enter your login/pass, they immediately seize control of your account and attack your friends.
The end