# Computer Security

01. Introduction

Paul Krzyzanowski
Rutgers University
Spring 2017



## What is security?

**security**

*noun* se·cu·ri·ty \si-ˈkyu̇r-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?

1. Confidentiality
2. Integrity
3. Availability



## Confidentiality

- Keep data & resources hidden
  - 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
- Confidentiality: the ability to conceal messages or exchange messages without anyone else seeing them
- Ability to send messages anonymously
- Control other's use of information about you

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*



## 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

  } Find the bugs!

- Systems are complex
  - 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



## Some 2016 security breaches

- 2016 U.S. elections (maybe?)
- Jan 23, 2016: Lloyds Bank hit by a massive DDoS attack
- Nearly 120,000 BTC (~$60M) stolen from Bitfinex, a major Bitcoin exchange
- Data stolen from more than 1 billion accounts at Yahoo
  - Since 2013; disclosed in December 2016
- San Francisco's public railway system, Muni, infected with malware over Thanksgiving
- 412 million accounts compromised from AdultFriendFinder.com
- Cisco's Professional Careers website had a privacy hole that exposed personal information of job seekers

Sources: https://www.identityforce.com/blog/2016-data-breaches
http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP



## Some 2016 security breaches

- National Payment Corporation of India: 3.2 million debit cards across 19 Indian banks compromised
- User names, passwords, email address, and IP data stolen from 43 million Weebly users
- 68 million Dropbox users had usernames & passwords compromised
- More than 330,000 Oracle MICROS cash registers breached
- Newkirk Products, provider of healthcare ID cards had a data breach that affected up to 3.3 million people: names, mailing addresses, dates of birth, insurance information
- 117 million email & passwords stolen from LinkedIn in 2012 were made public

Source: https://www.identityforce.com/blog/2016-data-breaches



## Some 2016 security breaches

- Over 300 Wendy's restaurants affected in payment card data breach
- Phishing scam tricked a Snapchat employee into releasing personal information about 700 current and former Snapchat employees
- Over 270 million email usernames and passwords given away for free in the Russian criminal underground
  - 57 million Mail.ru accounts, 40 million Yahoo accounts, 33 million Hotmail accounts, and 24 million Gmail addresses
- Personal information of every voter in the Philippines (55 million people) was compromised by Anonymous.
- Ransomware held MedStar Health-operated hospitals in Maryland and Washington hostage

Source: https://www.identityforce.com/blog/2016-data-breaches

## Some 2016 security breaches

- IRS announced that the May 2015 data breach affected over 700,000 tax payers
- Financial data of over 80,000 University of California, Berkeley students, alumni, & employees was released
- Hackers released data on 10,000 Department of Homeland Security employees one day and then released data on 20,000 FBI employees the next day
- €50 million stolen from FACC, an Austrian-based aerospace parts manufacturer
- Verizon Enterprise Solutions, provider of IT services & data breach assistance, was hit by hackers who stole information of 1.5 million customers

Source: https://www.identityforce.c om /blo g/2 016 -d ata -br eac hes



## It's a daily event


January 23, 2017



## Even smart guys aren't safe




## Close to home


January 23, 2017



## Potential for real harm


January 10, 2017



## 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?



## Protection: Know Thine 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 fileserver?
- 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




## 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
  - *Modification of the system, denial of service, delays*
- Usurpation: Unauthorized control of some part of a system
  - *Modification, spoofing an identity, escalation of privileges*



## Types of threats

- Snooping: unauthorized interception of information
  - Form of disclosure
  - Counter with confidentiality mechanisms
- Modification or alteration: unauthorized change to data
  - Form of deception, disruption or usurpation
  - Counter with integrity mechanisms
- Masquerading or spoofing: impersonation of one entity by another
  - Form of deception and usurpation
  - Counter with integrity mechanisms
- Repudiation of origin: false denial that an entity sent or created something
  - Form of deception and usurpation
  - Counter with integrity mechanisms



## 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 and usurpation
  - Counter with availability mechanisms
- Denial of service: long-term inhibition of a service
  - Form of disruption and usurpation
  - Counter with availability mechanisms



## 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

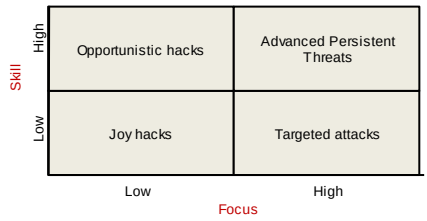
## Computer vs. real world risks

- Physical world risks are low (for most of us)
  - Most people are not attacked
  - Most people are not victims of espionage
- Digital world: same threats as real-world threats:
  - Theft, vandalism, extortion, fraud, coercion, con games
- Same motivation by criminals
  - But the mechanisms, risks, and access are different



## Threat matrix

Assess adversaries by skill vs. focus






## Types of attackers

- Joy hackers
  - Beginners, hacking for fun, little knowledge or focus
- Opportunistic attackers
  - May be skilled but will attack any vulnerable target
  - They're not out to get you specifically
- Targeters
  - They're out to get you
  - Will gather background info on you
  - But not high skill level
- Advanced Persistent Threats
  - Skilled & focused attackers
  - Most difficult to guard against
  - Skilled criminals to intelligence agencies



## 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
  - Get the scoop!
  - Social engineering, bribing, dumpster diving, track movement, 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
- 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
- Service 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

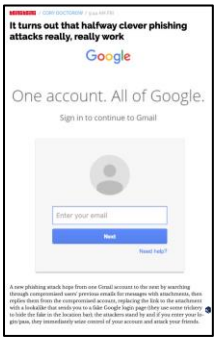


## The human element

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

Social engineering is a top threat


https://xkcd.com/1727/






## The end