CSE 410/565 Computer Security
Spring 2022

Lecture 1: Basic Security Concepts

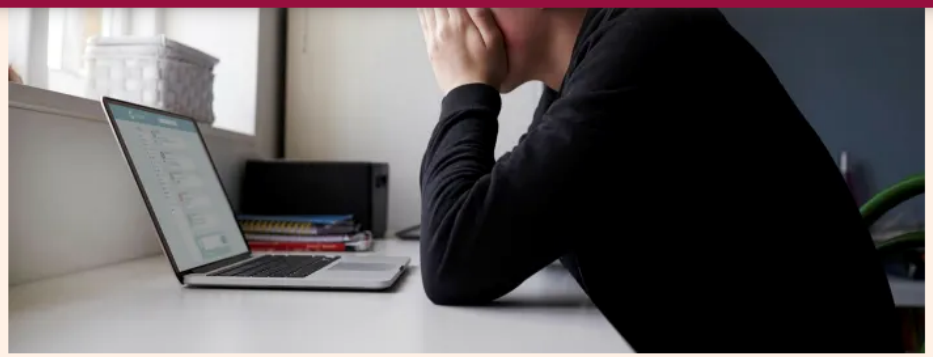
Department of Computer Science and Engineering
University at Buffalo

Academic Integrity

- Your first assignment is to to read the CSE and UB academic integrity policies
- Here are examples for your consideration
  - you work on your laptop at a library with friends and step away from your computer without locking it
  - you look at your neighbors' papers during an exam, but don't copy their answers
  - you take a piece of code from some website and give a link to the website at the end of the homework
  - you work on a homework problem with friends, type the solution at home, but it's the same as that of your friends

Examples of Citing

Special Report **Cyber Security and Society** Show articles



While large organisations often have defence barriers, individuals are largely left to fend for themselves © Alamy Stock Photo

Antonia Cundy JANUARY 25 2021

The jump in internet usage and homeworking prompted by the Covid-19 pandemic is opening new channels for online criminals, who have taken advantage of weak cyber security to inflict both financial and psychological damage to victims.

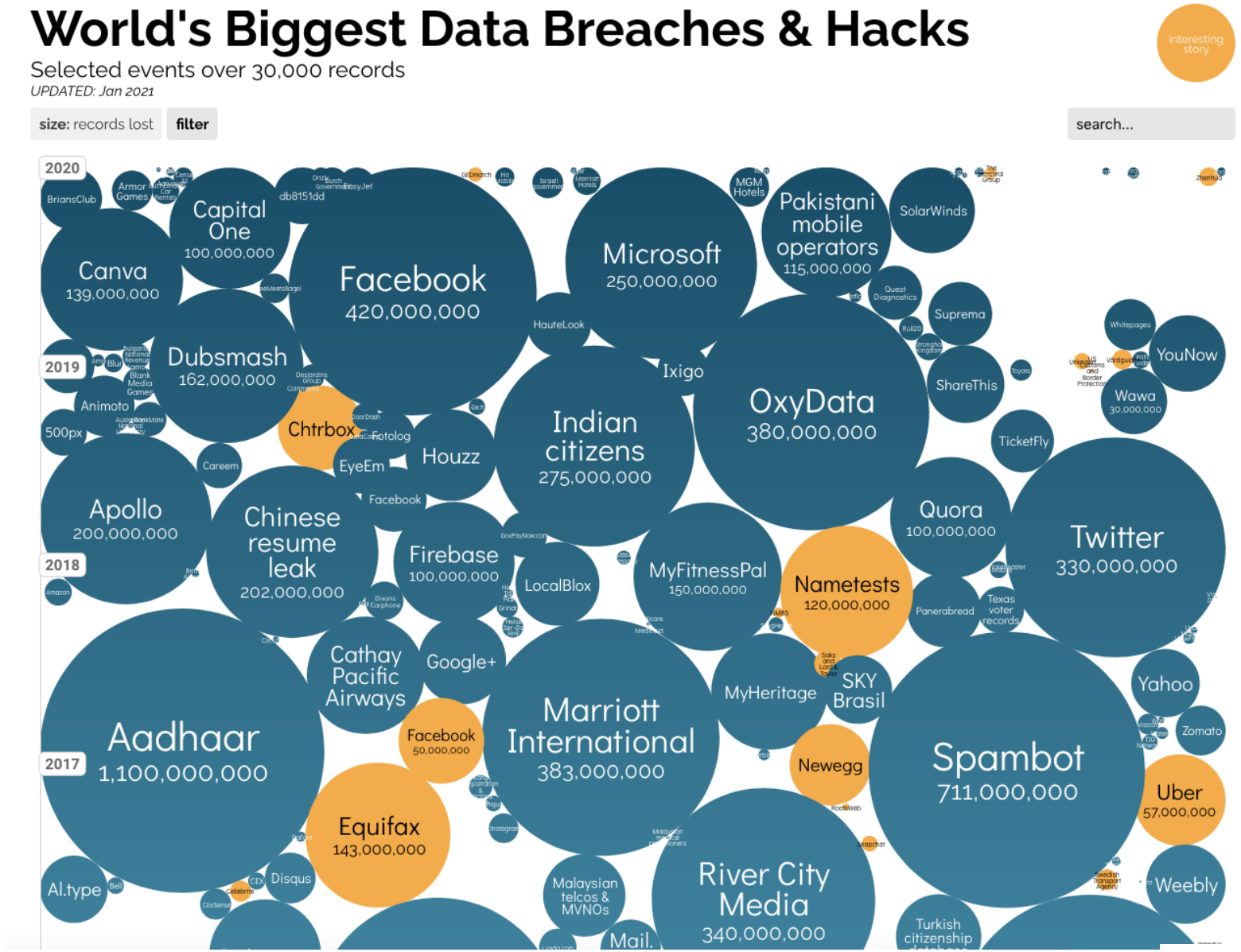
In the 12 months to June 2020, incidents of fraud and computer misuse in England and Wales rose from 4.84m incidents to 5.94m year-on-year, according to the Office for National Statistics. For every 1,000 people, there were 94 victims of fraud and 35 of computer misuse, up from 82 and 21 respectively in the previous 12-month period.

"People are much more focused on using IT to communicate so there are more opportunities for fraud and cyber crime. It's got a lot worse," says Mark Button, director of the centre for counter fraud studies at the University of Portsmouth.

What is Security?

- Security (failures) are constantly on the news
  - malware infections
  - ransomware
  - data breaches
  - espionage
  - cyberwar
- Everyone is affected
  - individuals
  - corporations
  - governments

Data Breaches are Extremely Common



https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

Current Internet Threat Trends

- Symantec Internet Security Threat Report
  - produced by Symantec on a regular basis
  - gathers information from over 175 million hosts in over 150 countries
- Global trends
  - release of devastating ransomware attacks
  - coin-mining on compromised computers is significant
  - mobile malware continues to surge
  - attacks against IoT devices significantly increase
  - attacks are increasingly diversified

Current Internet Threat Trends

- Some scary numbers (from 2019 report):
  - 1 in 10 web requests lead to malware
  - spam accounts for 55% of email
  - an average user receives dozens of viruses in email per year
  - credit card numbers are sold for $0.5–$25; 500 already used credit cards go for $1
  - 2,500 hacked email accounts sell for $1-$15
  - 500,000 email accounts with passwords from data breaches are $90
  - online banking accounts cost 0.5–10% of value
  - malware can be as cheap as $1
  - identity (name, SSN, DOB) goes for $0.1-$1.5

What is Security?

- Security is very broad as a field
- It covers areas such as
  - network security
  - database security
  - software security
  - safety in programming languages
  - access control
  - integrity and reliability
  - privacy
  - malware, digital crime, etc.

Security Objectives

- What is computer security anyway?
  - protection afforded to a computer system (including hardware, software, firmware, data, and communications) to maintain security objectives
- Security objectives can be formulated crisply
  - Confidentiality (C): confidential or private information is not disclosed or made available to unauthorized parties
  - Integrity (I) : unauthorized modification of data is not permitted
  - Availability (A): resources are promptly available to authorized parties

More on Security Objectives

- Confidentiality covers
  - data confidentiality: sensitive information is available to authorized parties only
  - privacy: individuals can control what information about them can be collected and stored and to whom it is made available
- Integrity covers
  - data integrity: information and software can be modified only in a predetermined and authorized manner
  - system integrity: a system performs its intended functions in an expected manner and has not be manipulated in an unauthorized way

More on Security Objectives

- Additional security concepts
  - Authenticity: the property of being genuine and being able to be verified and trusted
    - entity authentication: the entity is who it claims it is
    - data authentication: the data is coming from a trusted source
  - Access control: only authorized parties can use specific resources in compliance with their privileges
  - Non-repudiability (repudiability): inability (ability) to deny communication or actions
  - Accountability: the requirement that all actions of an entity are traced uniquely to that entity
    - covers non-repudiability, intrusion detection, fault isolation, etc.

How do We Achieve These Goals?

- The means of achieving these objectives greatly differ
  - cryptographic techniques
  - access control policies
  - software checking tools
  - virus scanners
  - firewalls
  - spam filters, etc.
- Each system must be evaluated uniquely in terms of its requirements
  - security mechanisms must be adequately chosen in accordance with those requirements

Why Security is Hard

- Identifying security requirements of a system is non-trivial
  - must take into account services, environment, etc.
- Finding adequate (often complex) solutions is not easier
  - the decision must take into account known attacks and threats
  - security mechanisms must be logically placed
- Securing a system is not a one-time task
  - the system must be constantly monitored in face of changing threats
  - security mechanisms need to be re-evaluated

Why Security is Hard

- Managers do not perceive value in security investment (until a security failure occurs)
  - system administrators might not influence decisions or not make good decisions
- Users view security measures as an obstacle on the way of getting their work done
  - we would like security mechanisms to be as intuitive and robust as possible
- Adding security to an existing system might not be pretty
  - ideally, security is an integral part of the design

What You Need to Remember

- Security is not absolute
  - assets can have different security grades depending on the impact of a security breach that can range from low to high
  - by building more secure systems, we make it harder for an attacker to breach security
  - the more resources we can invest in a system, the more secure we can make it
  - there is a trade-off between security and resources (money, equipment, personnel, training)
  - training must cover all users, as security can often be easiest breached by exploiting human error

More Definitions

- Asset (or resource)
  - software, hardware, data, communication lines and equipment that we want to protect
- Security policy
  - a set of rules or practices that specify how a system or organization is prescribed to protect its assets
- Vulnerability
  - a flaw or weakness in system's design, implementation, or operation that could be exploited to violate the security policy
- Threat
  - a potential for violation of security, i.e., a possible danger that might exploit a vulnerability

More Definitions

- Attack
  - a deliberate and intelligent attempt to violate the security policy of a system or get around security services
- Adversary (or attacker)
  - an entity that attacks a system or is a threat to it
- Countermeasure
  - an action, procedure, or technique that reduces a threat or vulnerability, prevents or mitigates an attack
- Risk
  - an expectation that a particular threat will exploit a particular vulnerability with a particular harmful result

More Definitions

- Types of adversaries
  - passive: observes information without intervention
    - e.g., passively monitoring a communication link
  - active: alters system resources or affects their operation
    - e.g., changing messages, replaying old messages on the network, corrupting users, etc.
  - insider: is legitimately a part of the system with access to internal data or is inside the security perimeter
  - outsider: is outside of the security perimeter or is not a legitimate user

Policies and Mechanisms

- Policy defines "security" for the site, system, etc.
  - composition of policies is non-trivial
  - if policies conflict, discrepancies can create security vulnerabilities
- Mechanisms enforce policies
- Security goals w.r.t. policies
  - prevention: prevent attackers from violating security policy
  - detection: detect attacks' violation of security policy
  - recovery: stop attack, assess and repair damage; continue to function even if attack succeeds

Building a System

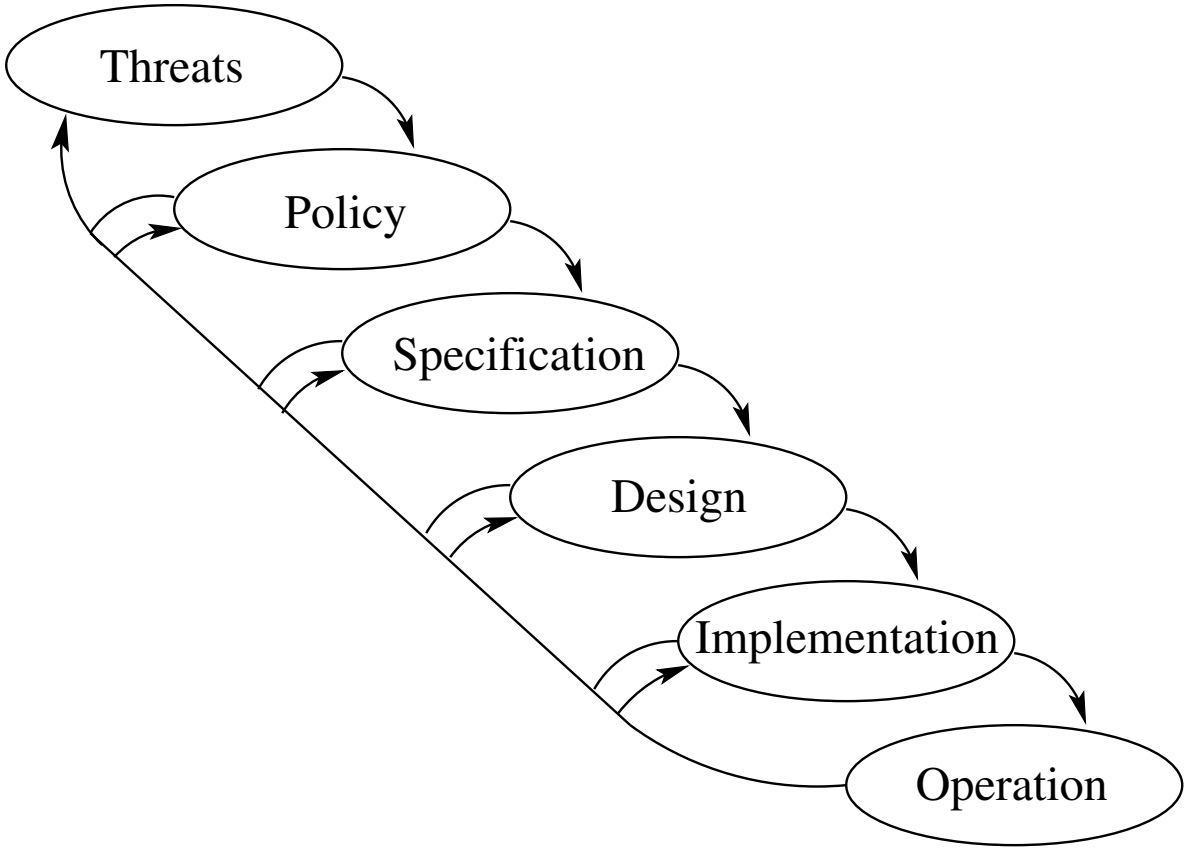
- Trust and assumptions underlie all aspects of security
  - policies are assumed to correctly capture security requirements
  - mechanisms are assumed to enforce policy
- Specification is a statement of desired functionality
  - it is based on requirements analysis
- Design specifies how the system will meet specifications
- Implementation is supposed to correctly carry out the design

Operational and Human Issues

- Operational issues
  - cost-benefit analysis: is it cheaper to prevent or recover?
  - risk analysis: should we protect this resource? how much should we protect it?
  - laws and customs: are desired security measures legal? will people do them?
- Human issues
  - organizational problems: power and responsibility; financial benefits
  - people problems: outsiders and insiders; social engineering

Tying It All Together

- Building a secure system



Security Design Principles

- Fundamental security design principles include
  - economy of mechanism
  - open design, modularity
  - layering
  - complete mediation
  - fail-safe defaults
  - separation of privilege, least privilege
  - least common mechanism
  - psychological acceptability, least astonishment
  - isolation, encapsulation

Summary

- Security is a broad field
- Building and maintaining a secure system is a complex task
  - security requirements are determined at early stages of product development
  - the design should be guided by security specifications
  - maintaining secure operation is also non-trivial
- Security threat trends are constantly changing