

CISC 3325 - Information Security

Introduction

Adapted from *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved

CISC 3325 - Information Security

- Tzipora Halevi, Assistant Professor
email: halevi@cis.brooklyn.cuny.edu
Office Hours: Mondays, 2:30 - 4:30pm
Ingersol room 2156A
- Book:
 - Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies, *Security in Computing*, 5th edition, Prentice Hall imprint, Pearson Education, Inc., 2015

Course Structure

- Assignment+ project - 33%
 - Done individually or in small groups
- Exams + quizzes + participation – 33%
 - Done individually
- Final exam - 34%

Class Policies

- Late homework/project: reduced credit
- Never share homework, solutions, code, etc.,
 - Don't let any other student see them
 - Work on your own
 - unless assignment states otherwise
 - Don't look at other students' homework or past assignments you may find online
- Quote and properly cite references used in your work

Introduction

Adapted from *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved

Class Objectives

- Define *computer security* as well as basic computer security terms
- Introduce the C-I-A Triad
- Introduce basic access control terminology
- Explain basic threats, vulnerabilities, and attacks
- Show how controls map to threats

What Is Computer Security?

- The protection of the assets of a computer system
 - Hardware
 - Software
 - Data
- What is the value of the assets?
 - Is the asset easily replaced?
 - Cost of replacement.
 - Is the asset unique?

What is Computer Security?



- Traditionally, computers are protected against:
 - Theft/damage to hardware
 - Theft/damage to information
 - Disruption of service

Growing Importance of Computer Security

- Increasing reliance on computer systems and the Internet
- Use of wireless networks such as Bluetooth and Wi-Fi
- Expanding array of smart devices
 - and ‘Internet of Things’ (IoT) devices


Why is computer security important?

- Attacks Impact everyone's day-to-day life
 - Millions of compromised computers
 - Millions of stolen passwords
 - Risk of identity theft
- Serious financial damage caused by security breaches



CYBERCRIME REPORT

FROM THE EDITORS AT CYBERSECURITY VENTURES

 Follow @CybersecuritySF

2017 Edition

The Official 2017 Annual Cybercrime Report is sponsored by [Herjavec Group](#), a leading global information security advisory firm and Managed Security Services Provider (MSSP) with offices across the United States, Canada, and the United Kingdom. Read the [Official Press Release](#) or [Download a PDF Version of the Report](#).

DAMAGE COSTS

Cybersecurity Ventures predicts cybercrime damages will cost the world \$6 trillion annually by 2021

Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades.

– [Steve Morgan](#), Editor-In-Chief

Menlo Park, Calif. — Oct. 16, 2017

Cybercrime is the [greatest threat to every company](#) in the world, and one of the [biggest problems with mankind](#). The impact on society is reflected in the numbers.



NEWS

Cyber attacks cost U.S. enterprises \$1.3 million on average in 2017

IT security budgets, as well the costs of data breaches, are up for North American enterprises and SMBs.



U.S. Army illustration

MORE LIKE THIS



Show the
it out with
Kaspersk
rumors



The curre
cybercrim

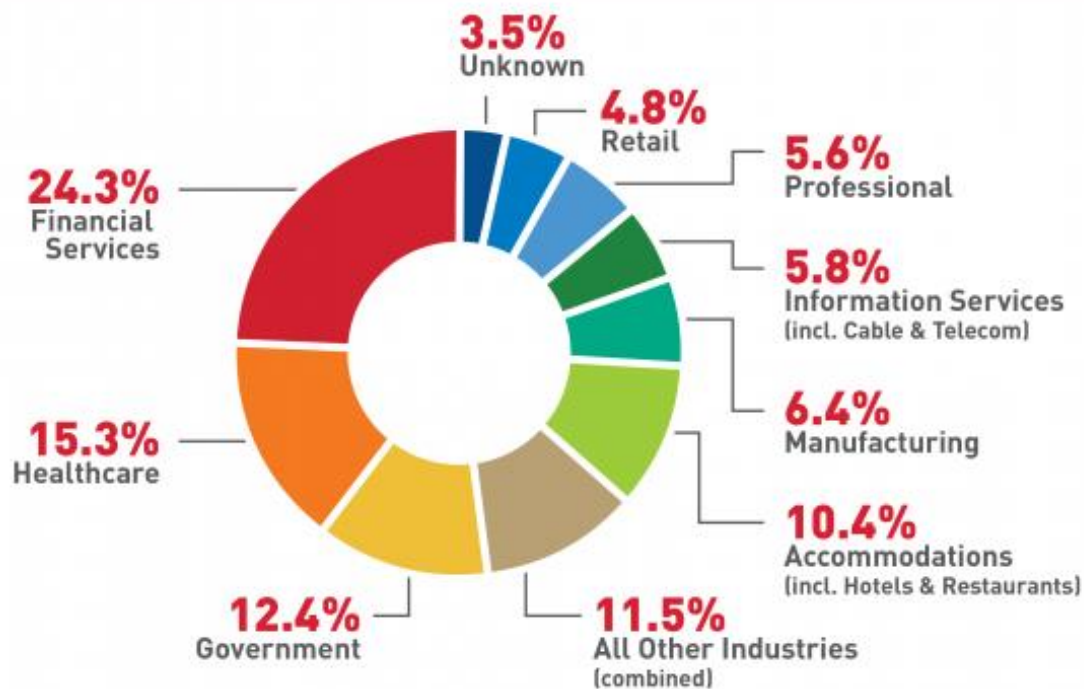


Who is a
ransomw



VIDEO
Office 36
examples
Hash Fn 1

Where Breaches Happen



Source: Verizon 2017 Data Breach Investigations Report

NRF® NATIONAL
RETAIL
FEDERATION®

nrf.com/datasecurity

<https://nrf.com/advocacy/policy-agenda/data-security>

How can we help?

- Security education can help us
 - Avoid attacks
 - Create safer systems
- We start by defining risk management

Risk Management



- High-level goals of computer security:
 - identification, evaluation, prioritization of risks
 - Defined as a threat model
 - Estimate the effects of uncertainty
 - Not perfect protection
 - Efforts concentrate on making it harder to attack
 - Finding ways to spend time & money efficiently
 - minimize the probability or impact of unfortunate events

Threat Model



- Key notion of threat model:
 - what/who are you defending against?
 - Determines which defenses to consider
 - E.g., where are valuable assets stored, where is the system most vulnerable to attacks, etc.

Security Threats History

- 1990's: fewer attacks, attackers gained fame,
 - Some attacks accidental,
- late 2000's: financially motivated
 - pharmaceuticals, credit card theft, identity theft
 - Phishing evolved into spear-phishing
 - More targeted form of attack
 - Uses target personal information to impersonate a trusted source
- 2010's: politically motivated
 - Government actors: Stuxnet, Flame, Aurora
 - Private activism: Anonymous, Wikileaks

Security Threats History

- Threats Have Evolved
 - Attackers have become more sophisticated;
- Arms race between attackers and defenders fuels rapid innovation in malware
- Many attacks aim for profit
 - are facilitated by a well-developed “underground economy” or cyber-crime organizations

Malware Evolution



◀ 3 of 30 ▶

Now you see me, now you don't: chasing evasive malware - Giovanni Vigna

How to protect from loss, destruction and illegal access

- Identify vulnerabilities – weaknesses that can be exploited to cause harm
- Monitor for threats – methods or situations that can cause harm
- Recognize an attack that exploits the vulnerabilities
- Take countermeasures or use methods to control an attack

Conclusions

- To protect computer systems, you must know your enemy
- Security is not about perfection: it's about defenses that are good enough to stop the threats you're likely to encounter

Fundamental Concepts

Computer Network



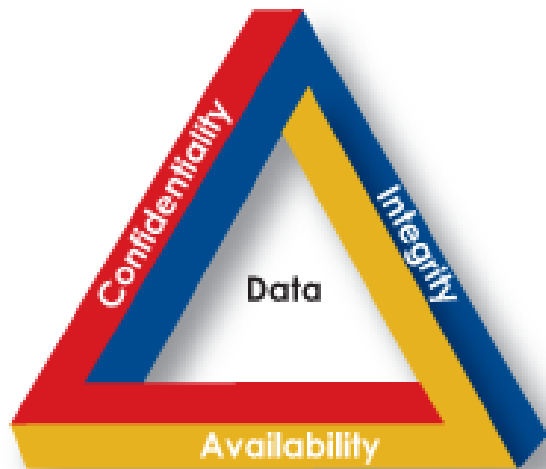
- A digital telecommunications network which allows nodes to share resources
- Networked computing devices exchange data with each other using a data link
- The connections between nodes are established using either cable media or wireless media

Cyber Vulnerabilities



- **Vulnerability** is a **cyber**-security term that refers to a flaw in a system that can leave it open to attack.
- A **vulnerability** may also refer to any type of weakness in a computer system itself
 - Either in a set of procedures, or in anything that leaves information security exposed to a threat
- Cutting down vulnerabilities provides fewer options for malicious users to gain access to secure information.

Confidentiality, Integrity and Availability (C.I.A.)



Confidentiality

- Avoidance of the unauthorized disclosure of information
 - Protect data, keep information secret
 - Provide access only to authorized users



Tools to ensure confidentiality

- Encryption:
 - Information encrypted using a secret key
 - Transformed info can be read using decryption key
 - Info essentially can not be read without this key
- Access Control:
 - Policies that limit access to confidential info
 - To people/systems with a “need to know”
 - May be based on person’s id, name or his role

Tools to ensure confidentiality (cont.)

- Authentication:
 - Determination of someone's ID or role
 - Maybe based on:
 - Something that the person has
 - Smart card, radio key, etc.
 - Something the person knows:
 - Password, etc
 - A physical trait of a person:
 - Fingerprints, etc.

Tools to ensure confidentiality (cont.)

- Authorization:
 - Is the person allowed access to the info?
 - Based on access control policy
 - Mechanism should be secure, prevent an attacker from tricking the system and gaining unauthorized access
- Physical Security:
 - Physical barriers that limit access to protected info
 - Such as locks, cabinets, doors.
 - Placing a computer in a windowless room.
 - Building a Faraday cage to prevent electromagnetic signals
 - To prevent side-channel attacks

Integrity

- Ensure information has not been altered in an unauthorized way
- Information may be compromised maliciously or by accident
 - Through hard drive crashes
 - Through a computer virus



Tools to protect integrity

- Regular backups
- Checksums – map the content to a numerical value and save that value. Read it back upon reading the information
- Data correcting codes: store data in such a way that small changes can be easily detected
 - And corrected
- The above tools all use redundancy
 - Replication of some of the information content or content

Availability



- Information is available when it is needed
 - Accessible and modifiable
 - to those authorized to do so
- Tools for ensuring availability:
 - Physical protections: housing that can withstand unexpected situations
 - Such as earthquakes, storms, etc.
 - Powered with generators
 - Computational redundancies:
 - Extra disks or web servers, such that failure of a single device will not degrade availability of data

C-I-A Triad - Summary

- Confidentiality – only those individuals or accounts who have permission can access a system.
- Integrity – a system or account can be altered only by authorized users
- Availability – a system/account is available when expected
- Sometimes two other desirable characteristics:
 - Authentication
 - Nonrepudiation

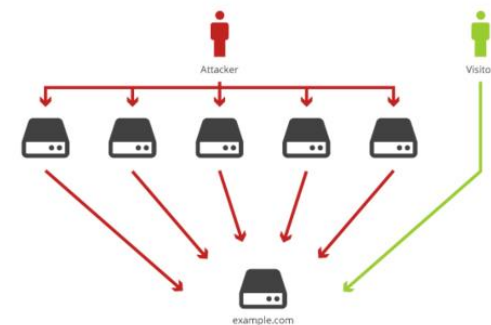
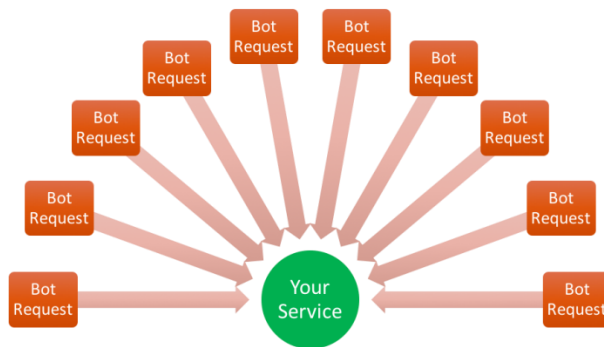
Threats and Attacks

- Eavesdropping: interception of information during transmission
 - Includes side channel attacks
 - May be audio, electromagnetic, power, etc.
- Alteration: unauthorized modification of information
 - False information may be installed



Threats and Attacks (cont.)

- Denial-of-service: interruption or degradation of data or information
 - This is an attack on availability
 - For example, email spam, which fills the mailbox



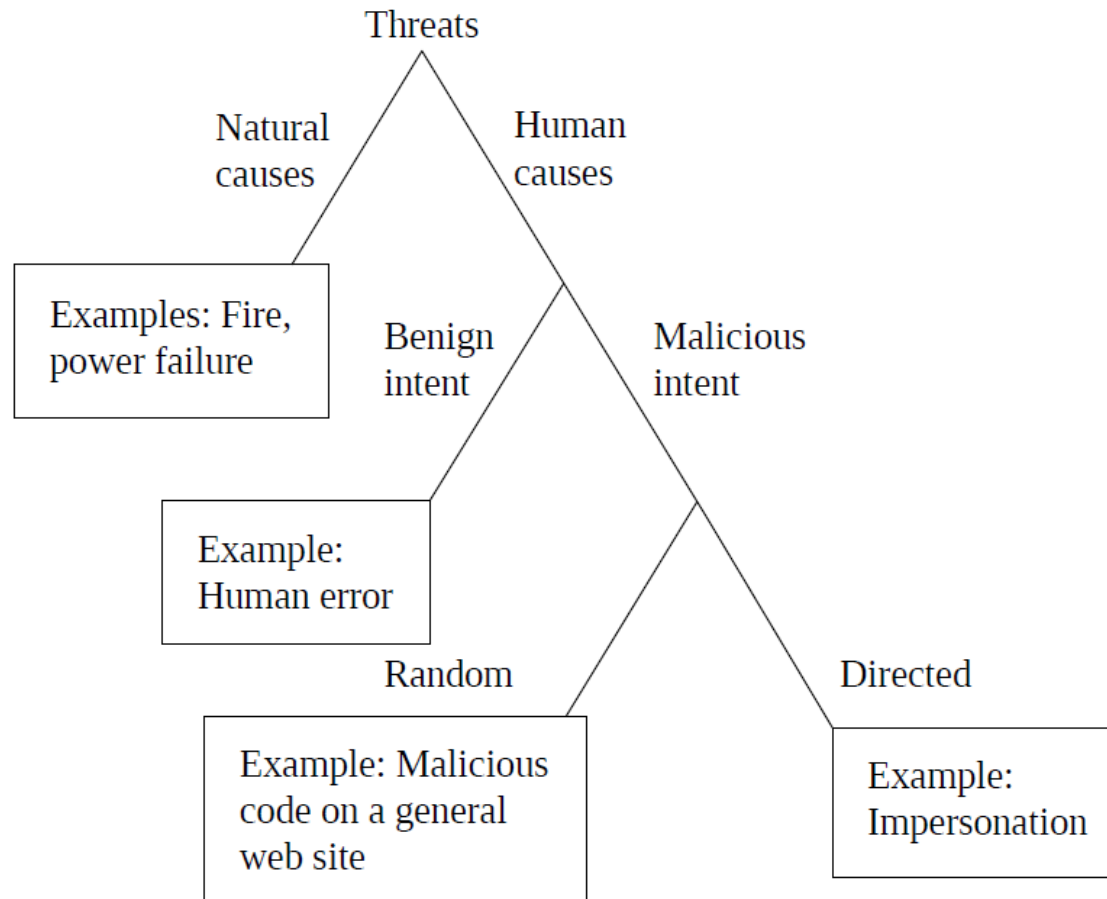
<https://www.cyberdominance.com/cybersecurity/your-local-supermarket-holds-the-key-to-defending-against-distributed-denial-of-service-attacks/>

<https://steemit.com/ddos/@clumsysilverdad/dos-and-ddos-attacks>

Threats and Attacks (cont.)

- Masquerading: fabrication of information, purported to be from some who is not the actual author
 - For example, phishing and spear-phishing attacks
- Repudiation: denial of commitment or data receipt
 - Attempt to back out of a contract

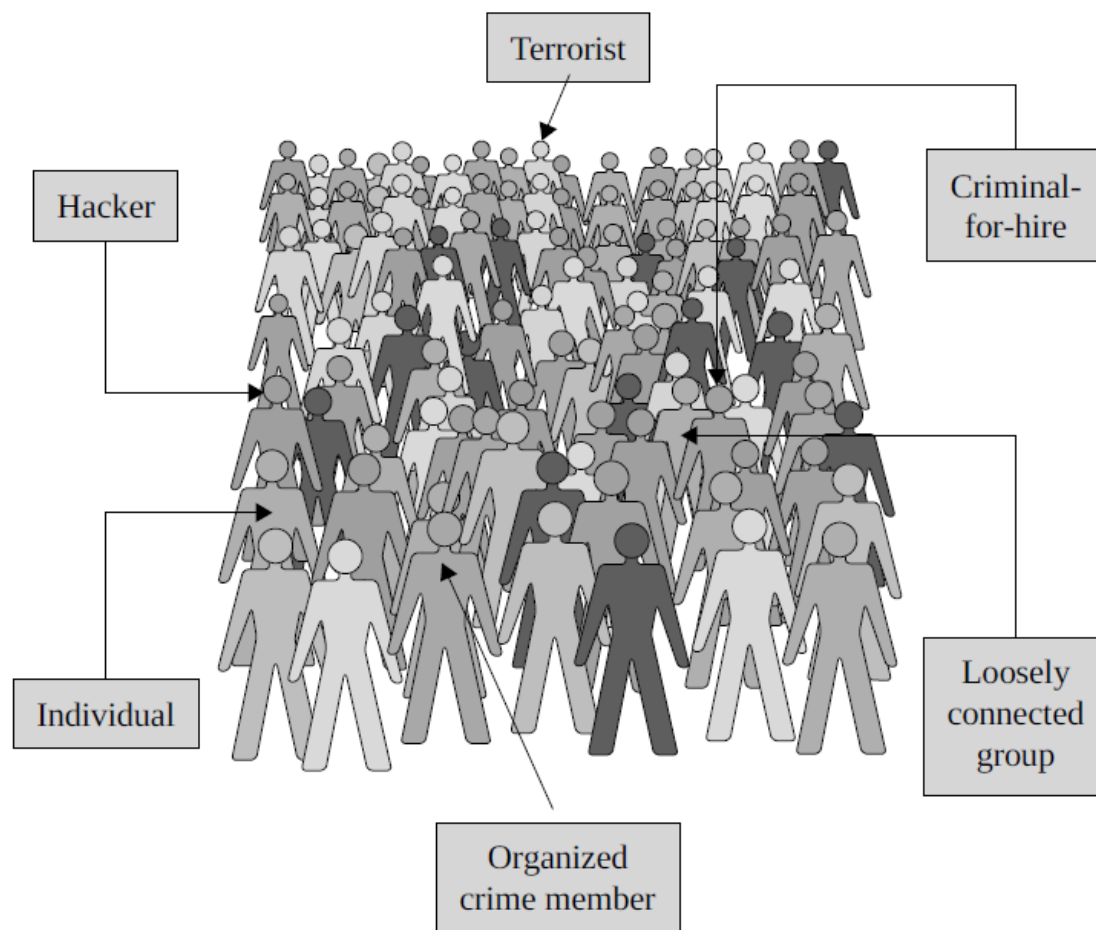
Source of the threat



Advanced Persistent Threat (APT)

- An attack that lasts for a long period of time
 - Organized
 - Directed
 - Well financed
 - Patient
 - Silent

Who are the attackers?



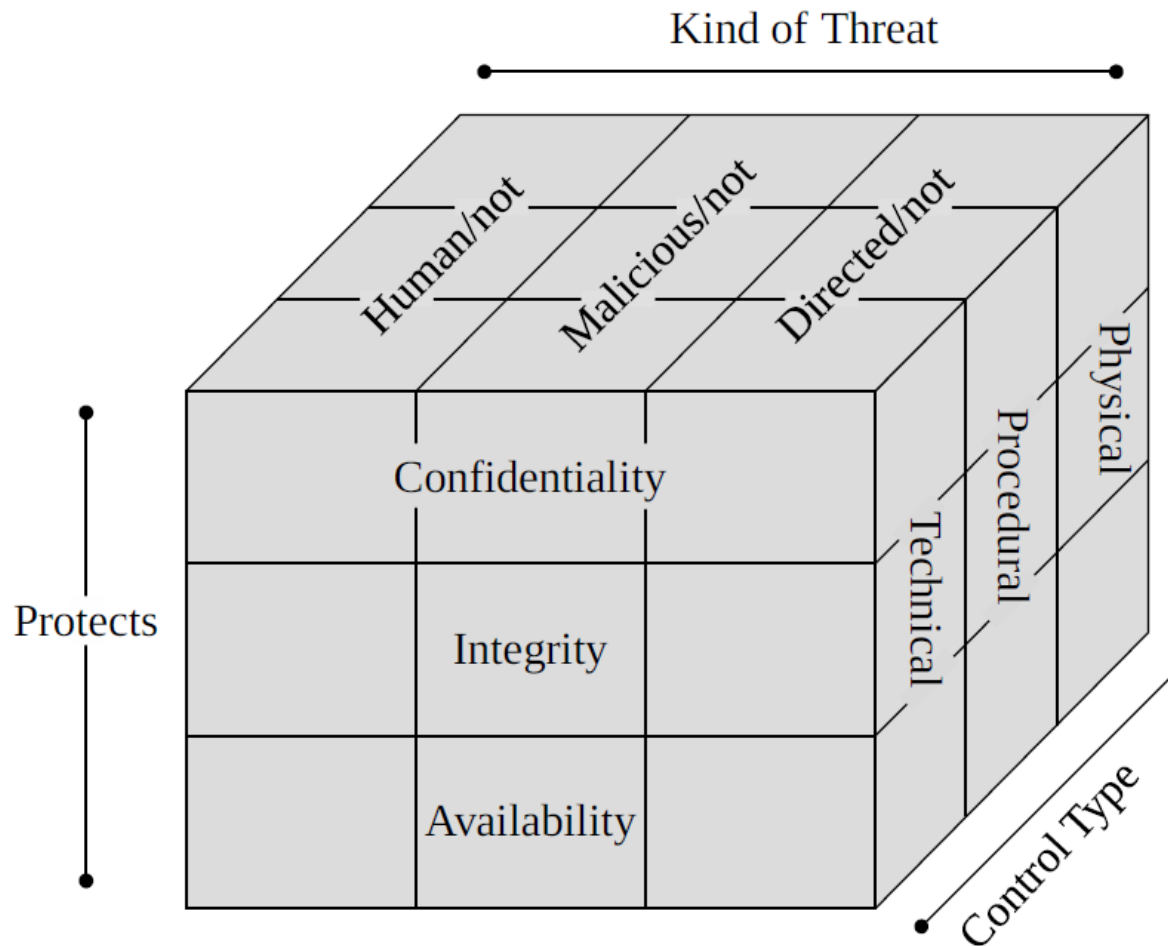
Vulnerabilities Databases

- <http://cve.mitre.org> - a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cybersecurity issues.
- <https://nvd.nist.gov> - the U.S. government repository of standards-based vulnerability management data

How are attacks accomplished?

- Method of attack:
 - * a group or individual uses their knowledge of the hardware or software to access the system
 - a group or individual downloads the information needed to access the system
- Opportunity for an attack – unsecured access or data
- Motive – why is the attack occurring

Controls/Countermeasures



Risk Management

- Can not protect against every attack:
 - Decide what is most valuable and analyze how to protect it
 - Estimate how likely an attack is
 - What is the impact of the attack

How to prevent or respond to an attack

- Block the attack or remove the vulnerability
- Make the attack harder to accomplish
- Decrease the attractiveness of the target
- Have counter measures that make the attack less severe
- Detect that an attack is in progress and take counter measures
- Have a plan to recover from an attack

Summary

- Vulnerabilities are weaknesses in a system; threats exploit those weaknesses; controls protect those weaknesses from exploitation
- Confidentiality, integrity, and availability are the three basic security primitives
- Different attackers pose different kinds of threats based on their capabilities and motivations
- Different controls address different threats; controls come in many flavors and can exist at various points in the system

Questions?

