CS458: Introduction to Information Security

Notes 1: Introduction

Yousef M. Elmehdwi

Department of Computer Science

Illinois Institute of Technology

yelmehdwi@iit.edu

August 23rd, 2018

Slides: Modified from: Computer Security: Principles and Practice, 4th Edition. By: William Stallings and Lawrie Brown, Ewa Syta, "CPSC 257: Information Security in the Real World", at Yale University & Kevin Jin IIT

Welcome to CS458

Who we are. . .

- **Course Info**
  - Course Webpage: under construction
  - Syllabus: Course Blackboard
- **Instructor**
  - Yousef Elmehdwi
    - Second year at IIT, first time teaching CS458☺
    - Email: yelmehdwi at iit dot edu
    - Research: data privacy and security
    - Office: Stuart Building, room 337D
    - Office Hours: T 6:20-7:20pm/F 5:10-6:10pm (and by appointment)

Reading

- **Textbook:**
  - Computer Security: Principles and Practice by William Stallings and Lawrie Brown, any edition (4th).
  - Resource for students from the official textbook website http://williamstallings.com/ComputerSecurity/CompSec4e-Student/
- Additional Readings (useful but not required)
  - Computer Security: Art and Science by Matt Bishop
  - Applied Cryptography by Bruce Schneier
  - Information Security Risk Analysis by Thomas Peltier
  - Threat Modeling by Frank Swiderski
  - Security in Computing by Charles P. Fleeger
  - Security Engineering: A Guide to Building Dependable Distributed Systems by Ross Anderson
  - Network Security - Private Communication in a Public World, 2nd Edition (2002), by Charlie Kaufman, Radia Perlman, and Mike Speciner

What is expected from you

- Attend lectures
- Be active and think critically
- Do homeworks
  - Start early and be honest
- Study for tests and exams

Outline

- Introduction to the major topics in computer security
  - human factors in security policy
  - basic applied cryptography, public key cryptography
  - key and identity management, authentication, access control
  - network security, database security, operating system security
  - denial-of-service attacks, malware ...
  - program security and design principle, malicious software
  - more ...

Course Objectives

- To provide a basic understanding of the problems of information assurance and the solutions that exist to secure information on computers and networks

What this course

- This is a lecture/exam-based class
- For those are more interested in hands-on experience
  - CS558 Advance Computer Security
    - A semester-long, hands-on project
    - In-depth knowledge for particular chosen topics

Lectures

- Lecture slides in PDF format will be posted shortly before or after the lecture
- Lecture slides cover essential material
- Not intended to be self sufficient
- Going through lecture slides will NOT be enough to master course materials
- Try to cover same thing in many ways: Lecture, homework, exams

Workload and Grading

- **Exams**
  - Midterm I (25%): Septemper 27^{th}
  - Midterm II (25%): November 8^{th}
  - Final (40%)
- **Homework Assignments (preparation for exams!) - 10%**
- **Course project/Labs 5% (bonus)**
  - Individual work

Letter Grade Distribution

Points	Grade
90 - 100	A
80 - 89	B
70 - 79	C
60 - 69	D
0 - 59	E

Attendance

- I dislike mandatory attendance but attendance makes your life easier.
- Students are expected to attend all classes and are responsible for all material covered in class, even when absent.
- Students should understand that some material discussed in class is not covered in the textbook.

Fraud and Late Assignments

- All work has to be original!
  - Cheating = 0 points for assignment/exam
  - Possibly **E** in course and further administrative sanctions
  - Every dishonesty will be reported to office of academic honesty
- Late policy
  - -20% per day
  - No exceptions!

Acknowledgement

- Class materials modified from
  - Computer Security: Principles and Practice, 4th Edition. By: William Stallings and Lawrie Brown
  - Ewa Syta, “CPSC 257: Information Security in the Real World”, at Yale University
  - Kevin Jin, IIT

Rest of Today

- Introduction to computer security

- Essentials of Information Security

Achieving Security

- In the ideal world, we would like to achieve perfect security of information.
- It is impossible to protect everything against every attacker under all circumstances while maintaining usability (utility of the system).

Achieving Security

- Security is a trade-off of what we want to achieve and what we can achieve.
- Security is about risk management.

Cost-Benefit Analysis

- In the real world, everything is about making the best possible choice: balancing costs and benefits.
  - Evaluate what level of security is necessary, appropriate, or desirable.
  - From adversary's perspective
    - Cost of launching a particular attack vs. value of attack to an adversary.
  - From company's perspective
    - Cost of damages from an attack vs. cost of defending against the attack.
  - Likelihood of a particular attack.

Information as an Asset

- Information is a strategic business asset.
  - Transaction information.
  - Client information.
  - Proprietary information.

Information Security

- Protecting information is a major challenge in the digital world.
- Massive compromises of confidential data are disclosed almost daily.
  - Identity theft.
  - Industrial espionage.
  - Cyberwarfare (actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption)
  - Major web sites taken down by denial-of-service attacks.
  - Massive government surveillance.
  - Massive harvesting of personal data by large internet companies such as Google and Facebook.

Threat examples

- Some risks and possible countermeasures:
  - Eavesdropping on private conversations:encryption.
  - Unauthorized use of a computer: passwords, physical security.
  - Unwanted email: spam filters.
  - Unintentional data corruption: checksums and backups.
  - Denial of service: redundancy, isolation.
  - Breach of contract: nonrepudiable signatures.
  - Malicious data corruption: backups, access controls, cryptographic hash functions.
  - Disclosure of confidential data: access controls, encryption, physical security.

How is security achieved in the real world?

- Prevention: Physical barriers, access controls, encryption, firewalls, human awareness, etc.
- Detection: Audits, checks and balances.
- Legal means: Laws, patents, trademarks, copyrights, sanctions against wrongdoers.
- Concealment: Camouflage, steganography

Security Mindset

- Security is not a product, it is a process [1]
- We need to learn to think with a "security mindset"
  - How could this system be attacked?
  - Who could attack this system?
  - Are they likely to attack the system?
  - What is the weakest point of attack?
  - How could this system be defended?
  - How effective will a given countermeasure be?
  - What is the trade-off between security, cost, and usability?

[1] https://www.schneier.com/crypto-gram/archives/2000/0515.html

Security Mindset

- You see an advertisement for a new product. What is your reaction?
  - *"Wow! This is such a cool product. I can't wait to use it!!!"*
  - *"Wow! This is a neat product but I wonder what are the potential consequences of using it? Does it work as advertised? Is it safe? Can something go wrong while using it? Can someone else exploit it?"*

Example: Nest Learning Thermostat

YouTube: How Nest Learning Thermostat Learns

Security of an Information System

- We cannot protect information on its own.
- You need to look at the entire system within which the information exists.
- A system is only as strong as its weakest component.

Security of an Information System

- Understand the system and its components.
- Identify assets.
- Identify vulnerabilities.
- Identify attacks.
- Identify adversaries.

Assets

- Asset: Anything of value
  - Physical Assets: Buildings, computers
  - Logical Assets: Intellectual property, reputation
- You need to know what there is to protect.
- You need to know what is worth protecting

Vulnerabilities

- Vulnerabilities are weaknesses that could be exploited to cause damage to assets.
  - Bad passwords
  - Buggy software
  - Untrained employees
  - Lack of encryption

Attacks

- Attacks are ways of exploiting a vulnerability
  - Bad passwords: using password crackers.
  - Buggy software: launching an SQL injection attack.
  - Untrained employees: tricking them to share their credentials.
  - Lack of encryption: eavesdropping on communications.

Attacks

- There are several ways to classify attacks.
- By damage to the assets: Confidentiality, integrity, availability.
- By the source of the attack: Insider vs outsider
- By the actions: Interception, interruption, modification, fabrication.

- Real-world adversaries and their attacks

Adversaries

- Adversaries are entities that may carry out attacks.
  - Hackers
  - Governments
  - Terrorists
  - Competitors
  - Clients
  - Employees
- All types of adversaries are often referred to as hackers.

Adversaries

- An adversary must have three things:
  - **Method**: the skills, knowledge, tools, and resources.
  - **Opportunity**: the time and access to accomplish the attack.
  - **Motive**: a reason to want to perform this attack against this system (Fun, Financial gain, Moral Compass)

Actions and Motivations of Adversaries

- **Political**: destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.
- **Economic**: theft of intellectual property or valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.
- **Socio-cultural**: philosophical, theological, political, and even humanitarian goals, curiosity, and a desire for publicity or ego gratification.

Real-World Security Breaches by Motivation

- **By another government**
  - In December 2014, Sony Pictures was hacked.
  - A group called "The Guardians of Peace" took responsibility for hacking Sony over the released of "The Interview", a movie about an assassination of Kim Jong Un, the leader of North Korea.
  - FBI attributed the attack to the North Korean government.

Real-World Security Breaches by Motivation

- **By hackers whose motivation was financial**
  - In January 2014, Target was hacked.
  - Hackers stole credit and debit card numbers, expiration dates, the three-digit CVV security code, and even PIN data for up to 70 million customers.

Real-World Security Breaches by Motivation

- **By dishonest employees**
  - In January 2015, Korea Credit Bureau's data was leaked.
  - An employee of KCB has been arrested and accused of stealing 20 million customer records from three credit card firms while working for them as a temporary consultant

Real-World Security Breaches by Motivation

- **By employee**
  - In March 2015, Australian Immigration Department's data was accidentally revealed [2].
  - An employee of the agency inadvertently sent the passport numbers, visa details and other personal identifiers of the world leaders attending the G20 summit to the organizers of the Asian Cup football tournament.
  - Barack Obama, Angela Merkel, Vladimir Putin, David Cameron and many others were affected.

[2] https://www.theguardian.com/world/2015/mar/30/personal-details-of-world-leaders-accidentally-revealed-by-g20-organisers

- CIA and beyond

Computer Security

- What is computer security?
  - Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated[3]
- Computer Security is about understanding and improving the behavior of computing technologies in the presence of adversaries
- Deals with various measures to protect computer related assets against a variety of threats

[3] The NIST Internal/Interagency Report NISTIR 7298 (Glossary of Key Information Security Terms , May 2013)

Key Security Concepts

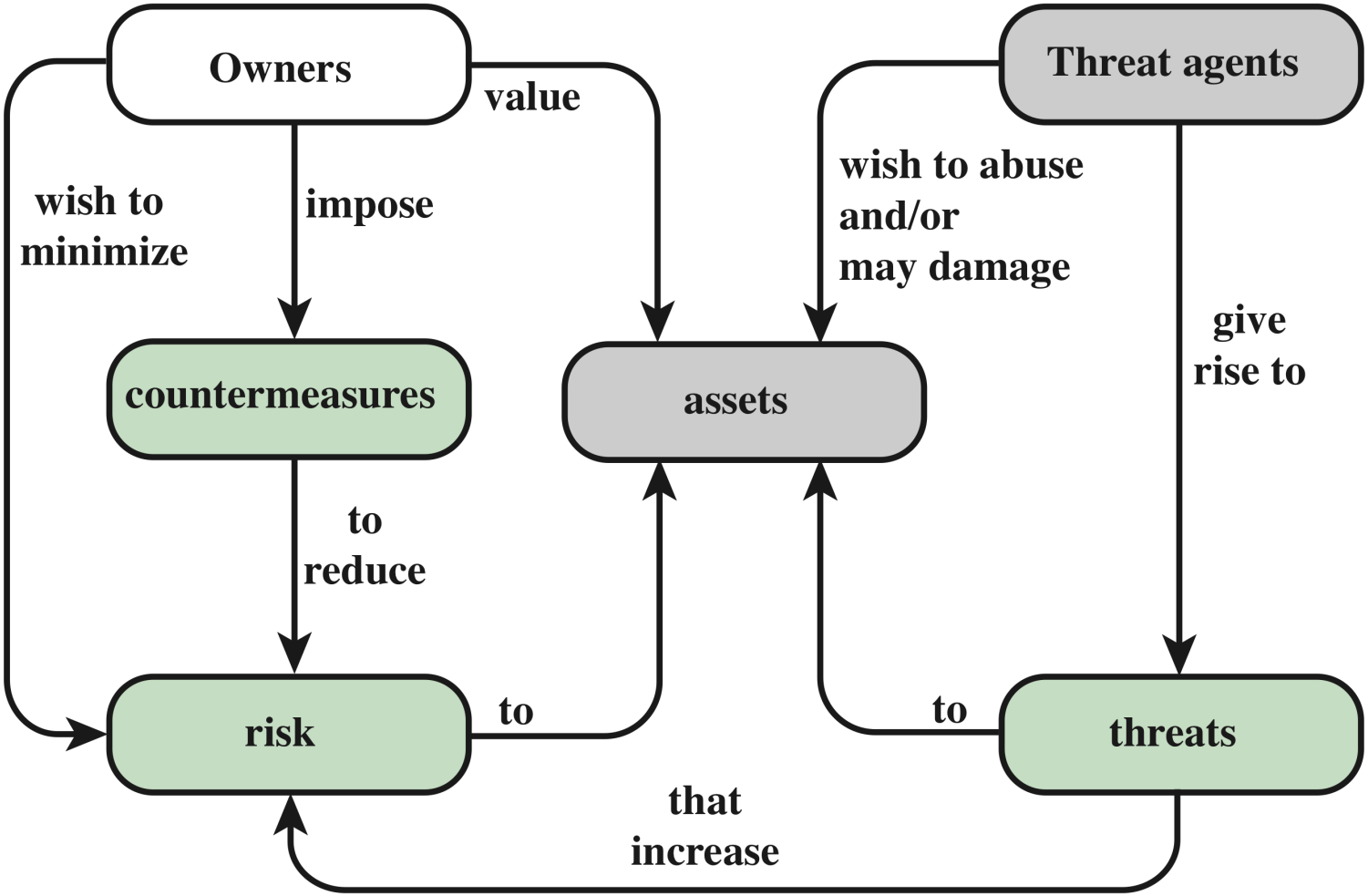
- This definition introduces three key objectives that are at the heart of computer security:
  - Confidentiality: This term covers two related concepts:
    - **Data confidentiality**: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
    - **Privacy**: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
  - Integrity: refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change.
    - **Data integrity** (the content of the information): Assures that information and programs are changed only in a specified and authorized manner.
    - **Origin integrity** (the source of the data, often called authentication): assurance of the source of data
  - Availability: Assures that systems work promptly and service is not denied to authorized users.

CIA

- `CIA == Confidentiality, Integrity, and Availability`
- Confidentiality:
  - Prevent unauthorized reading of information
  - A loss of confidentiality is the unauthorized disclosure of information.
- Integrity:
  - Prevent unauthorized writing of information
    - Data integrity (integrity)
    - Origin integrity (authentication)
  - A loss of integrity is the unauthorized modification or destruction of information

  Availability:
  - Ensures data is available in a timely manner when needed
    - Availability is a "new" security concern
    - Due to denial of service (DoS) threats
  - A loss of availability is the disruption of access to or use of information or an information system.

Security Concept Relationshipst



- We start with the concept of a system resource , or asset , that users and owners wish to protect.

Assets of Computer Systems to Protect

- Hardware
  - Including computer systems and other data processing, data storage, and data communications devices
- Software
  - Including the operating system, system utilities, and applications.
- Data
  - Including files and databases, as well as security-related data, such as password files.
- Communication facilities and networks
  - local and wide area network communication links, bridges, routers, and so on.

vulnerabilities, Threats and Attacks

In context of security, our concern is with the vulnerabilities of system resources.

- Categories of vulnerabilities of a computer system or network asset:
  - The system can be corrupted, so it does the wrong thing or gives wrong answers (loss of integrity)
    - For example, stored data values may differ from what they should be because they have been improperly modified.
  - leaky (loss of confidentiality)
    - For example, someone who should not have access to some or all of the information available through the network obtains such access.
  - Unavailable or very slow (loss of availability)

vulnerabilities, Threats and Attacks

- Threats
  - That are capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- Attacks is a threat that is carried out (threat action) and, if successful, leads to an undesirable violation of security, or threat consequence.
  - Passive: attempt to learn or make use of information from the system that does not affect system resources
  - Active: attempt to alter system resources or affect their operation
- We can also classify attacks based on the origin of the attack
  - Insider: initiated by an entity inside the security perimeter (an "insider").
    - The insider is authorized to access system resources but uses them in a way not approved by those who granted the authorization
  - Outsider: initiated from outside the perimeter by an unauthorized or illegitimate user of the system (an "outsider").

Classes of Threats: Threat consequences

Following describe four kinds of threat consequences and the kinds of attacks that result in each consequence:

- **Unauthorized disclosure**: Unauthorized access to information;
  - Exposure: Sensitive data is directly released to an unauthorized entity.
  - Interception: An unauthorized entity directly accesses sensitive data in transit.
  - Inference: an unauthorized entity indirectly accesses sensitive data by reasoning from characteristics or byproducts of communications.
  - Intrusion: An unauthorized entity circumvents system's security protections
- **Deception**: Acceptance of false data
  - Masquerade: An unauthorized entity poses as an authorized entity.
  - Falsification: False data deceives an authorized entity.
  - Repudiation: An entity deceives another by falsely denying responsibility for an act.

What security goal (CIA) does each class violate?

Classes of Threats: Threat consequences

- **Disruption** : Interruption or prevention of correct operation
  - Incapacitation: Prevent/interrupt system operation by disabling a system component
  - Corruption: adversely modifying system functions or data
  - Obstruction: interrupts delivery of system services by hindering system operation.
- **Usurpation**: Unauthorized control of some part of a system
  - Misappropriation: unauthorized logical or physical control of a system resource.
  - Misuse: Causes system to perform a function or service detrimental to security.

What security goal (CIA) does each class violate?

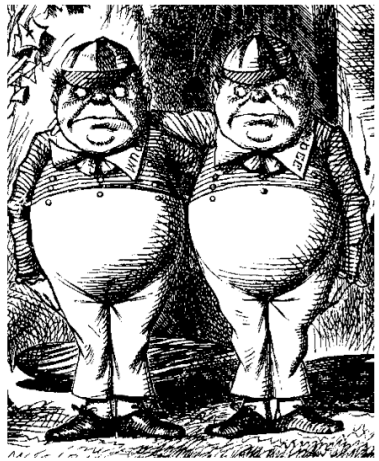
Countermeasures

- any means taken to deal with a security attack.
  - Prevent: prevent a particular type of attack from succeeding.
  - Detect and Recover: When prevention is not possible, or fails in some instance, the goal is to detect the attack and then recover from the effects of the attack.

The Cast of Characters

- Alice and Bob are the **good guys**

- Eve is the **bad guy**



- Eve is our generic “intruder”

Alice's Online Bank

- Alice opens Alice's Online Bank (AOB)
- What are Alice's security concerns?
- If Bob is a customer of AOB, what are his security concerns?
- How are Alice's and Bob's concerns similar? How are they different?
- How does Eve view the situation?

Computer Security Goal: AOB

- AOB must prevent Eve from learning Bob's account balance
- **C**onfidentiality: prevent unauthorized `reading` of information
  - Cryptography used for confidentiality
  - Encryption, key distribution, authentication.

Computer Security Goal: AOB

- Eve must not be able to change Bob's account balance
- Bob must not be able to improperly change his own account balance
- Integrity: detect unauthorized `writing` of information
  - Cryptography used for integrity
  - Hash functions, check sums, digital signatures.

Computer Security Goal: AOB

- AOB's information must be available whenever it's needed
- Alice must be able to make transaction
  - If not, she'll take her business elsewhere
- **A**vailability: Data is available in a timely manner when needed
  - Denial of service (DoS) attacks
  - Extremely dificult to deal with.
  - Crypto doesn't help.

Beyond CIA: Crypto

- Crypto is used as protocols executed between two or more parties
- How does Bob's computer know that "Bob" is really Bob and not Eve?
- Bob's password must be verified
  - This requires some clever cryptography
- What are security concerns of passwords?
- Are there alternatives to passwords?

Beyond CIA: Protocols

- When Bob logs into AOB, how does AOB know that "Bob" is really Bob?
- As before, Bob's password is verified
- Unlike the previous case, **network** security issues arise
- How do we secure network transactions?
  - Protocols are critically important.
  - Crypto plays critical role in security protocols

Beyond CIA: Access Control

- Once Bob is authenticated by AOB, then AOB must restrict actions of Bob
  - Bob can't view Charlie's account info
  - Bob can't install new software, etc.
- Enforcing these restrictions: **authorization** (What are you allowed to do)
- Access control includes both authentication (who are you) and authorization

Beyond CIA: Software

- Cryptography, protocols, and access control are all implemented in software
  - Software is foundation on which security rests
- What are security issues of software?
  - Real-world software is complex and buggy
  - Software flaws lead to security flaws
  - How does Eve attack software?
  - How to reduce flaws in software development?
  - And what about malware?

The People Problem

- People cause lots of problems...
- Users are surprisingly adept at damaging the best laid security plans
- People often break security
  - Both intentionally and unintentionally
  - Here, we consider the unintentional
- For example, suppose you want to buy something online
  - To make it concrete, suppose you want to buy `Computer Security: Principles and Practice, 3rd edition` from `amazon.com`

The People Problem

- To buy from amazon.com, you can use your Web browser to securely contact Amazon using the SSL protocol, which relies on various cryptographic techniques.
  - Your browser uses the SSL protocol
  - SSL relies on cryptography
  - Many access control issues arise
  - All security mechanisms are enforced in software
- Suppose all of this security stuff works perfectly
  - Then you would be safe, right?

The People Problem

- What could go wrong?
- Eve tries `man-in-the-middle` attack
  - SSL is secure, so attack does not "work"
  - But, Web browser warns of problem (issues a warning)
  - What do you, the user, do?
- If user ignores warning, attack works!
  - None of the security mechanisms failed
  - But user unintentionally broke security
- The security can be broken due to user error, despite the fact that the cryptography, protocols, access control, and software all performed flawlessly.

Things to cover in CS458: Cryptography

- Classic cryptography
- Symmetric ciphers
- Public key cryptography
- Hash functions
- Advanced cryptanalysis

Things to cover in CS458: Access Control

- Authentication
  - Passwords
  - Biometrics
  - Other methods of authentication
- Authorization
  - Access Control
    - Lists/Capabilities
    - Role-Based Access Control
    - Mandatory Access Control
- Multilevel security (MLS), inference control
- Firewalls, intrusion detection (IDS)

Things to cover in CS458: Protocols

- "Simple" authentication protocols
  - Focus on basics of security protocols
  - Lots of applied cryptography in protocols
- Real-world security protocols
  - SSL, IPSec, Kerberos

Things to cover in CS458: Software

- Security-critical flaws in software
  - Buffer overflow
- Malware
  - Viruses, worms, botnets
  - Prevention and detection
- Software reverse engineering (SRE)
  - How hackers “dissect” software

Things to cover in CS458: Software

- Operating system security
- Database security
- Software is a BIG security topic
  - Lots of material to cover
  - Lots of security problems to consider
  - But not nearly enough time available?

What's next?

- CS558 Advance Computer Security
  - Cover specific and advanced topic Like Botnet, Spam, DoS, Cyber physical Systems, SDN, hot topics you name it
  - Spring 2018 class website https://sites.google.com/site/cs558spring2018/

Key Points

- Must look at the big picture when securing a system
- Main components of security
  - Confidentiality
  - Integrity
  - Availability
- Differentiating Threats, Vulnerabilities, Attacks and Controls

Think Like Eve

- In the past, no respectable sources talked about “hacking” in detail
  - After all, such info might help Trudy
- Recently, this has changed
  - Lots of info on network hacking, malware, how to hack software, and more
  - Classes taught on virus writing, SRE, ...

Think Like Eve

- Good guys must think like bad guys!
- A police detective
  - must study and understand criminals
- In information security
  - We want to understand Eve's methods
  - We might think about Eve's motives
  - We'll often pretend to be Eve

Think Like Eve

- Is it a good idea to discuss security problems and attacks?
- Bruce Schneier, referring to Security Engineering, by Ross Anderson:
  - "It's about time somebody wrote a book to teach the good guys what the bad guys already know"

Think Like Eve

- We must try to think like Eve
- We must study Eve's methods
- We can admire Eve's cleverness
- Often, we can't help but laugh at Alice's and/or Bob's stupidity
- But, we cannot act like Eve
  - Except in this class
  - and even then, there are limits

Think Like Eve

- Think like the bad guy
- Always look for weaknesses
- Find the weak link before Eve does
- It's OK to break the rules
- Think like Eve
- But don't do anything illegal!