Lecture 1
Overview

Print version of the lecture in *CPS633 Computer Security*

presented on Week of September 3, 2019

by Ali Miri ©2019from Department of Computer Science at Ryerson University

1.1

Learning Objectives (page 12)

- To become familiar to some of the security terminologies and principles,
- To better understand computer security functional requirements, designs and architectures,
- To know different types of security threats and countermeasures.
- To learn more about security standards

This set of slides closely follows Chapters 0 and 1 of the textbook. 1.2

Contents

1.3

1 Preliminaries

1.1 Disclaimers

Disclaimer 1
The course slides will be based on the material in the textbook, and its accompanying resources. Best attempts will be made to identify any other sources used.

Disclaimer 2
In this course, we will study various security systems, and their vulnerabilities. This study is to better understand the foundations of security, and to design more secure systems. Any misuse of this learning will be at your own risk and is prohibited, and can potentially lead to appropriate actions by authorities.

1.4

Disclaimer 2
From *Ryerson Student Computing Guidelines:* at `https://www.ryerson.ca/ccs/about/policies.html/`

"For an idea of the types of behaviour that are emphatically **not** acceptable, refer to this list:

Do Not:

- Obtain or use someone else's password.
- Help someone gain unauthorized access to Ryerson's computers or networks.
- Attempt to gain access to files and resources to which you have not been given permission.
- Try to "crash" or slow down, the network or computing systems.
- Knowingly introduce a computer virus or other disruptive program.
- ...

1.5

Disclaimer 2
It is also completely unacceptable to use any Ryerson owned resource including computing and/or communications equipment to do any of of the above **outside** of Ryerson. For example, just as you may not send obscene, prejudicial, offensive, or harassing messages to anyone within Ryerson, you also may not use Ryerson's communications or computing facilities to send these types of messages outside of Ryerson.

Misuse of computer services and facilities by any user is an offence. Such offences may be dealt with under Section IV of the Code of Student Conduct.

Any tampering with or unauthorized use of Ryerson's computing facilities is indictable under sections 301 and 387 of The Criminal Code (Bill C-19). "

1.6

Disclaimer 2

From *Criminal Code of Canada, 342.1.* ***Unauthorized use of computer*** *(page 364)* at `http://laws-lois.justice.gc.ca/PDF/C-46.pdf`

" 342.1 (1) Every one who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service,

(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or

(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c).

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction."

1.7

Question: Given possible consequences, why one should study the topic?

- Must try to think like bad actors, and study their methods,
- Understand limitations and mistakes of (good) users,
- But, we **cannot act** like the bad guys!

" It is about time somebody wrote a book to teach the good guys what the bad guys already know." (Bruce Schneier)

1.8

It is now considered part of a comprehensive computer science education

It is in fact one of the recommended core topics of recommended *Computer Science Curricula 2013* by ACM and IEEE! (see `http://www.acm.org/education/CS2013-final-report.pdf`)

Also check more recent

Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (see `https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf`)

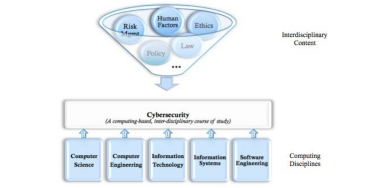
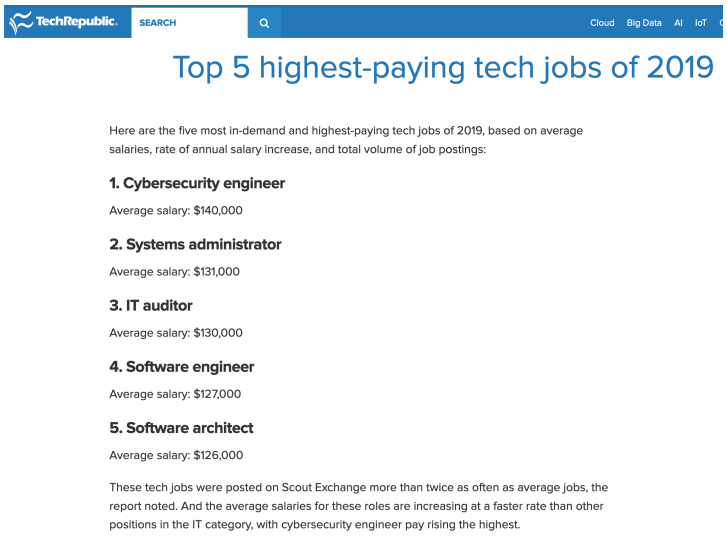


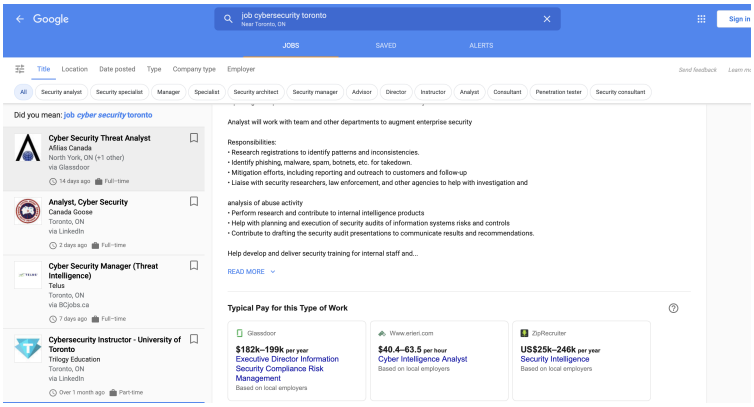
Figure 2. Structure of the cybersecurity discipline.

1.9

It can be part of a rewarding career



https://www.techrepublic.com/article/top-5-highest-paying-tech-jobs-of-2019/ 1.10



1.11

Textbook Outline

- Part One: Computer Security Technology and Principles
- Part Two: Software Security and Trusted Systems
- Part Three: Management Issues
- Parts Four & Five: Cryptographic Alg. & Network Security.

The book covers all the subject areas specified for *Certified Information Security System Professionals (CISSP)* 1.12

1.2 Standard Bodies

Standard Bodies & Their Publications

1. National Institute of Standard & Technology (NIST):
    - Federal Information Processing Standard (FIPS)

- Special Publication (SP)

2. Internet Society (ISOC)
   - Requests for Comments (RFC)
3. International Telecommunication Union (ITU):
   - ITU-T ← Recommendations
4. International Organization for standardization (ISO)
   - ISO

1.13

2 Security Concepts

2.1 Relations

Three fundamental questions:

1. What are the assets that we need to protect and what are their values to us? Are there any vulnerabilities that can effect these assets?
2. Who are (potential) attackers, what are their resources, and what assets they are after?
3. What are the countermeasures to (potential) threats, and how and where they should be employed?

1.14

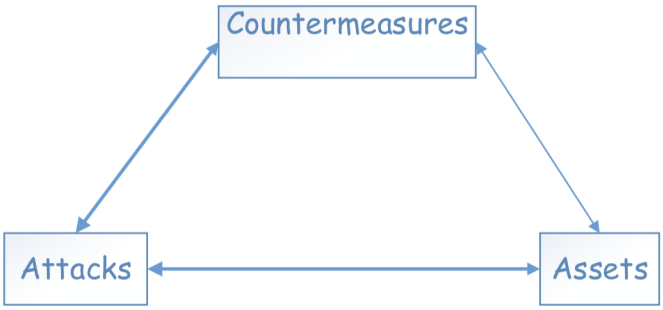
Typical Evaluation Process

1.15

Typical Evaluation Process

1.16

Typical Evaluation Process

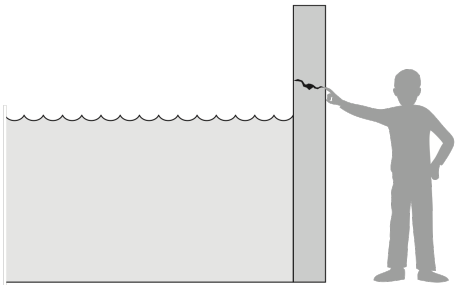


1.17

Computer Security Terminology

RFC 4949: *Internet Security Glossary*

- **Vulnerability:** A flaw or weakness that can be exploited.
- **Threat:** A possible danger of a vulnerability exploit.



(from a figure in 'Security in Computing', Fifth Edition (2015), by Charles P. Pfleeger, *et al*)

Computer Security Terminology

RFC 4949: *Internet Security Glossary*

- **Vulnerability:** A flaw or weakness that can be exploited.
- **Threat:** A possible danger of a vulnerability exploit.
- **Risk:** An expectation/measure of loss as a result of a vulnerability ← adverse effect + its likelihood.
- **Attack:** Actual instantiations of threats.
- **Adversary** (or a threat agent)**:** An entity that attacks, or is a threat to, a system.

Security Concepts and Relationship

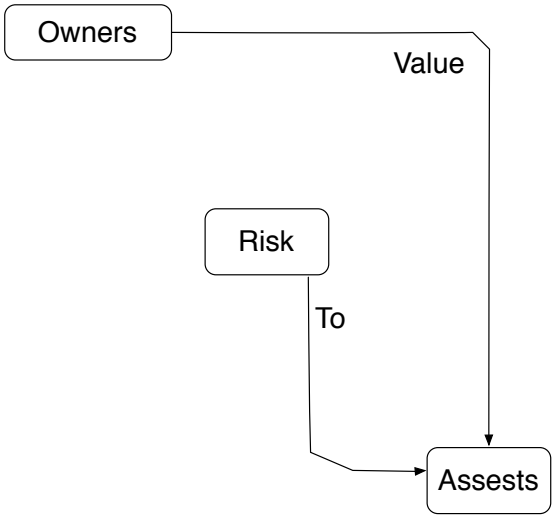


Figure 1.1 security Concepts and Relationship

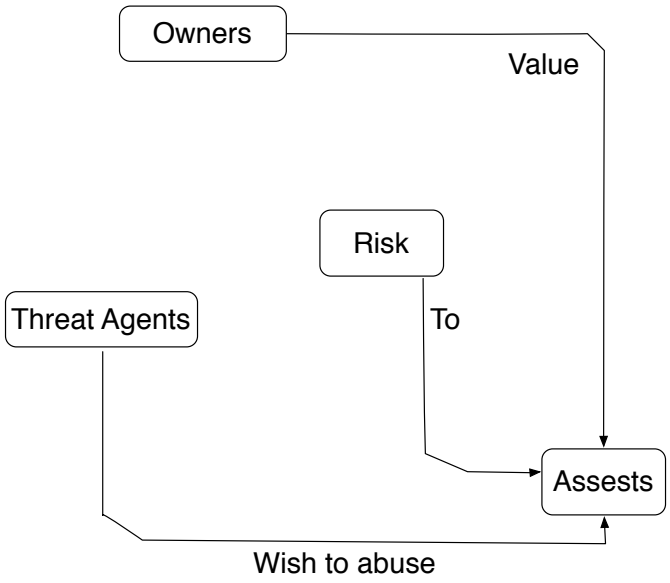


Figure 1.1 security Concepts and Relationship

1.21

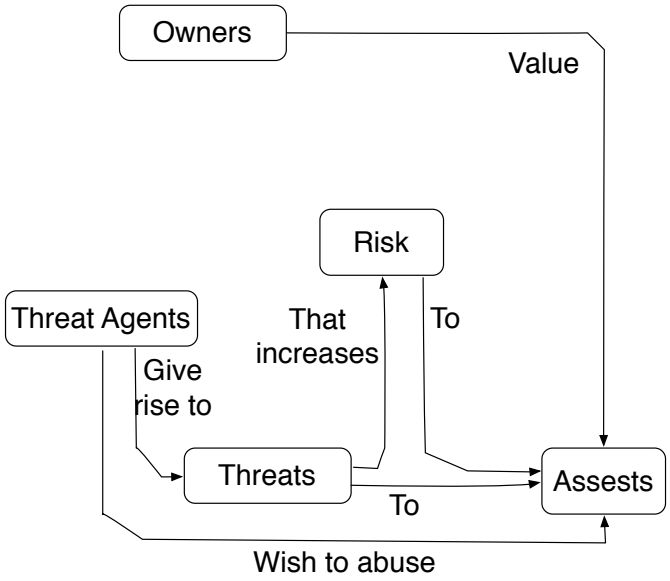


Figure 1.1 security Concepts and Relationship

1.22

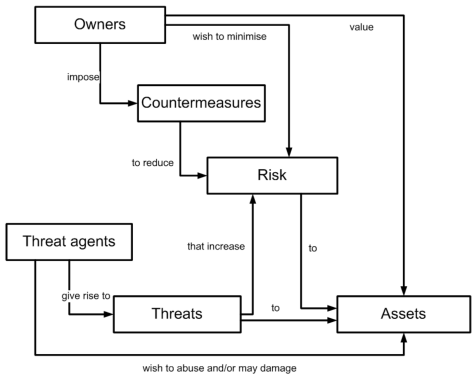


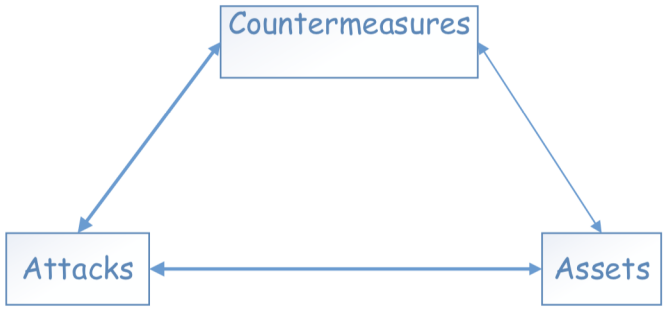
Figure 2 - Security concepts and relationships

From 'Common Criteria for Information Technology Security Evaluation', Part 1, April 2017, available at https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

1.23

2.2 Definitions

Assets



Q: What assets should be considered, and how do we assign values to them?

- Often it is hard to assign '*quantitive*' values ⇒ '*qualitative*

1.24

Assets

FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems

Based on "potential impact on organizations or individuals should there be a breach of security":

- Degradation of an organization mission capability
- Damage to organizational assets
- Financial loss
- Harm to individuals

Three (3) categories:

- **Low:** *limited*
- **Moderate:** *serious*
- **High:** *severe or catastrophic*

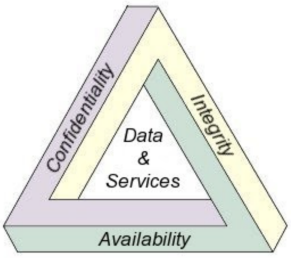
1.25

Definitions

Computer Security: (*classical definition*):"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications)."

SP 800-12: The NIST Handbook of Computer Security, page 5 (1995)
http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Also see FIPS 199: Standards for Security Categorization of Federal Information and Information Systems, page 6 (2004) http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf



Definitions

CIA Triad of Security

- Confidentiality
  - Data confidentiality
  - Privacy

  ← A loss of confidentiality is the unauthorized disclosure of information
- Integrity
  - Data integrity
  - System integrity

  ← A loss of integrity is the unauthorized modification or destruction of information
- Availability
  ← A loss of availability is the disruption of access to or use of information or an information system
- Note: There are more security services: Authentication, Accountability, etc.

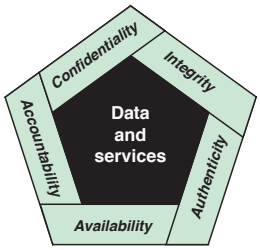


Figure 1.1 Essential Network and Computer Security Requirements

1.28

2.3 Model

A General Model for Computer Security

Assets:

- Hardware
- Software
- Data
- Communications facilities and networks

Vulnerabilities:

- Corruption
- Information leakage
- Unavailablitly
- ...

1.29

A General Model for Computer Security

Attacks : carrying out the exploitation

Categorized as

- Active (often easier to detect, but harder to protect)
- passive (often hard to detect, but easier to protect)

Or

- Inside
- Outside

(Or a combination of the two)

1.30

Countermeasures:

From FIPS 'Framework for Improving Critical Infrastructure Cybersecurity', Version 1.1 (April 16, 2018) available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

1.31

- "**Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

  The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy."

1.32

- "**Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.

  The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology."

1.33

- "**Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

  The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes."

1.34

A General Model for Computer Security Countermeasures

- "**Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

  The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements."

1.35

A General Model for Computer Security Countermeasures

- "**Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

  The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications."

Worth nothing that countermeasures used may result in

- may result in new vulnerabilities
- will have residual vulnerability
- goal is to minimize risk given constraints

1.36

Computer Security Challenges

This should be easy, right?

1. Easy/ simple to describe, but often difficult/ complex to implement
2. A designer has to consider all (possible?) attacks, where an attacker only has to find one vulnerability
3. Best location to place security is not always obvious
4. Typically require 'security' keys ← difficulties with key generation and distribution
5. Security is often afterthought, and valued "only" after an attack!
6. It can make systems less 'user friendly'.

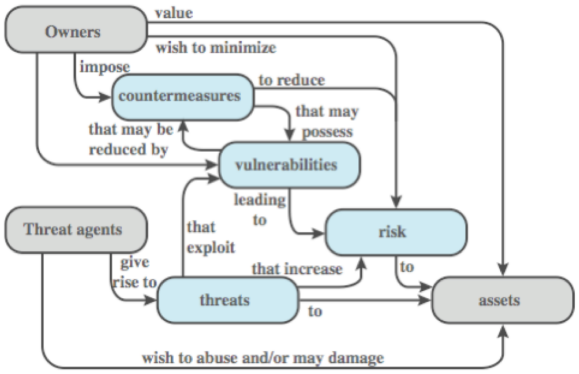
1.37

2.4 Examples

Example

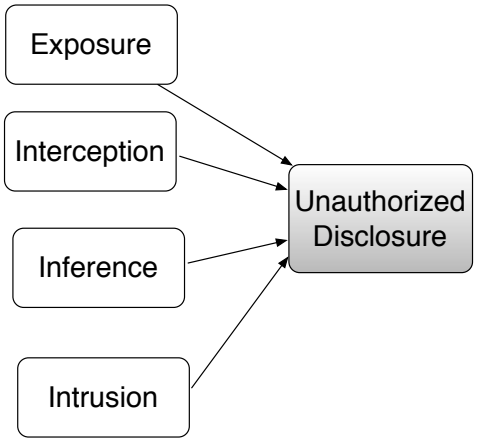
RFC 4949: *Internet Security Glossary* (March 2013), available at `https://datatracker.ietf.org/doc/rfc4949/`:

- "information for the Internet community" only
- It focuses on CIA triade.



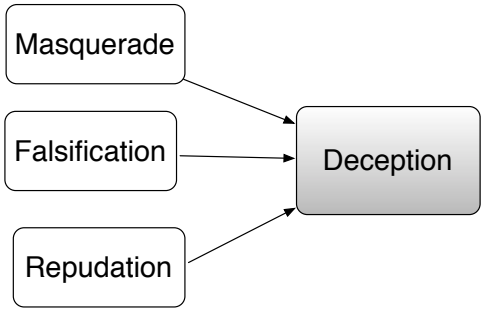
1.38

Threats and Attacks



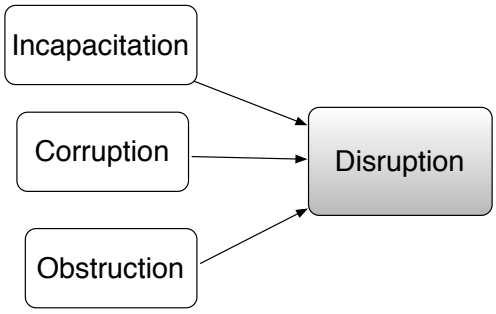
1.39

Threats and Attacks



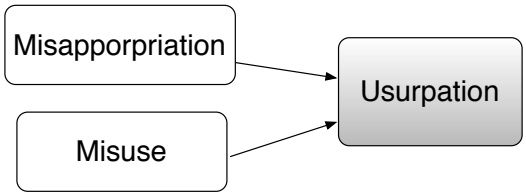
1.40

Threats and Attacks



1.41

Threats and Attacks



1.42

Threats and Assets

	Availability	**Confidentiality**	**Integrity**
Hardware	Stolen/disabled equipments	An unencrypted drive/DVD	
Software	Deleted programs	Unauthorized copy	Malware
Data	Deleted files	Unauthorized read, Inference	Modification of existing files
Comm. Lines	Messages deleted	Message read, traffic analysis	Messages deleted, modified, duplicated or fabricated

Examples of threats to computer and network assets

1.43

3 Security Functional Requirements

3.1 FIPS 200

FIPS 200

FIPS 200 : Minimum Security Requirements for Federal Information and Information Systems (2006) available at `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf`

• Includes 17 security-related area dealing with CIA in two general categories of countermeasures:

- Technical measures
  - Identification and authentication
  - Access control

  - System and communication protection
  - System and information integrity
- Management and policy measure
  - awareness and training
  - audit and accountability
  - Certification
  - ...

1.44

4 Security Design Principles

4.1 NCAE

NCAE

National Centers of Academic Excellence in Information Assurance/Cyber Defense. NCAE IA/CD Knowledge Units, June 2013: Fundamental Security Design Principles (a good set slides on this can be found at `https://sites.cs.ucsb.edu/~kemm/courses/cs177/principles.pdf`)

- *Economy of mechanism:* keep the design as simple as small as possible
- *Fail-safe defaults:* access decision based on permission rather than exclusion
- *Complete Mediation:* check every time every file
- *Open design:* keep the design public rather than Secret
- *Separation of privileges:* limit specific privileges to a specific task to be undertaken
- *Least privilege:* give the least amount of privileges needed to undertake the task
- *Least common mechanism:* minimize when possible the functions shared within different users application or Hardware

1.45

NCAE

- *Psychological acceptability:* match security need of the system with that of comfort level and understanding of users
- *Isolation:*
  - Isolate public part of the system from the sensitive ones
  - Isolate file and process of users from one another
  - Isolate and protect the security mechanisms
- *Encapsulation:* this is isolation based on object-oriented functionality
- *Modularity:*
  - develop security module
  - use a modular architecture for design and implementation
- *Layering:* use multiple overlapping protection
- *Least astonishment:* Ensure mechanism are transparent enough to users.

1.46

4.2 Surfaces and Trees

Attack Surfaces

More on attacks/attackers: two concepts useful in evaluating and classifying treats

Attack Surface: reachable and exploitable vulnerabilities in a system

- Network attack surface: the way we connect
- Software attack surface: applications we use
- Human attack surface: people!

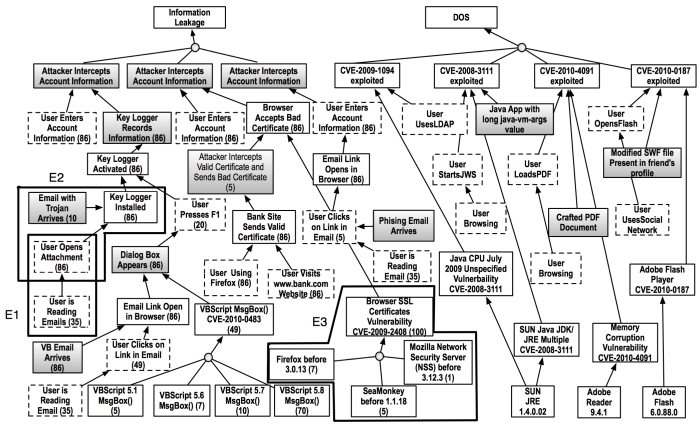
Why they are important?

- useful technique for assessing the scale and the severity of the threats
- can help with testing
- may result in solutions or modifications in services/applications to reduce attack surfaces

1.47

Attack Trees

Attack tree: a branching, hierarchal data structure representing a *set* of potential techniques for exploiting security vulnerabilities.



Accepting the Inevitable: Factoring the User into Home Computer Security,CODASPY'13

1.48

Attack Trees Example

an Internet banking authentication ⟵ *compromising a user's account*

Q. What are (some of) possible attacks that can achieve the attacker's objective?

1.49

Attack Trees Example

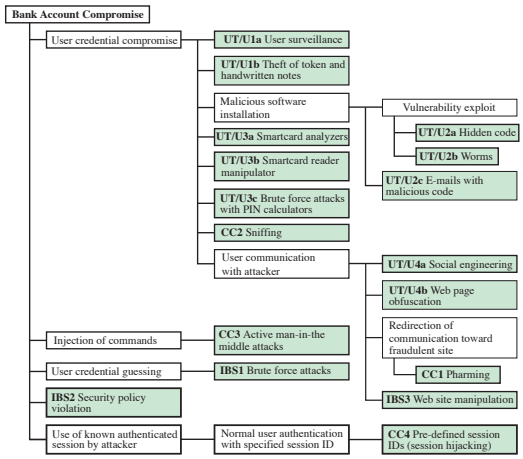


Figure 1.5 An Attack Tree for Internet Banking Authentication

1.50

5 Security Strategies

5.1 Policies

Security Policies

For a comprehensive security strategy need to consider

- **Specification and policy** - what is it supposed to do.

Security policy is an informal or formal description of desired system behaviour or formal statement of rules and practices governing the security of system.

Things to consider:

- Value of assets
- System vulnerabilities
- Potential threats and the likelihood of attacks
- **Ease of use versus security**
- **Cost of security versus cost of failure and recovery**

1.51

5.2 Implementations

Security Implementation

- **Implementation/mechanisms** - how to do it → NIST suggested countermeasures (see earlier slides).

1.52

5.3 Assurance

Security Assurance

- **Correctness and Assurance** - does it really work?

- Test to see if the system meets its design requirement
- Examine system/product with respect to certain criteria on regular intervals.

1.53