

Security in Computing

Chapter 1

Is There a Security Problem in Computing?

Outline

- 1.1 What Does “Secure” Mean?
- 1.2 Attacks
- 1.3 The Meaning of Computer Security
- 1.4 Computer Criminals
- 1.5 Methods of Defense
- 1.6 What’s Next
- 1.7 Summary

Outline

- 1.1 What Does “Secure” Mean?
- 1.2 Attacks
- 1.3 The Meaning of Computer Security
- 1.4 Computer Criminals
- 1.5 Methods of Defense
- 1.6 What’s Next
- 1.7 Summary

1.1 What Does Secure Mean? Wild West vs. Today

- *then* not so hard to rob bank, big payoff
- *now* pretty hard. payoff?
 - today we use checks, credit cards
- why the difference?
 - bank, large institution security well-studied
 - they have more secure:
 - procedures
 - infrastructure
 - lots of practice
- today’s computers, nets like wild west

Protecting Money vs. Information

	Money	Information
size (portability)	<i>at large sites</i> - guards, alarms, vaults, thick walls	laptop, ipods, thumb drives, etc. large capacity
avoid contact?	tough for thief to steal money without touching	easy
value	high	depends

Need for Security?

- often overlooked
 - computer crime underreported
 - not taken seriously. just pranks
 - law is behind the times
 - few lawmakers understand the technology

Automobile Example

- modern cars have many computer systems
- do they need security?
- false assumptions:
 - the code is too complex for troublemakers
 - the more complex, the more difficult to make secure
 - why would anyone want to hack them?
 - disable alarms, unlock doors, tracking
 - just because they can

Goals of the Book, Course

- understand the basic principles and problems of computer security
 - examine security risks
 - consider *countermeasures* or *controls*
 - think about uncovered vulnerabilities
 - identify areas where more work is needed

What's Valuable?

- important to protect what's valuable
- bank example:
 - protect money well
 - forget to protect the customer information

Principle of Easiest Penetration

- intruder will use *any* means of penetration.
- site or method of penetration
 - may not be most obvious
 - not necessarily where the strongest defenses are
- *e.g.*, don't install strong lock but not hinge

Outline

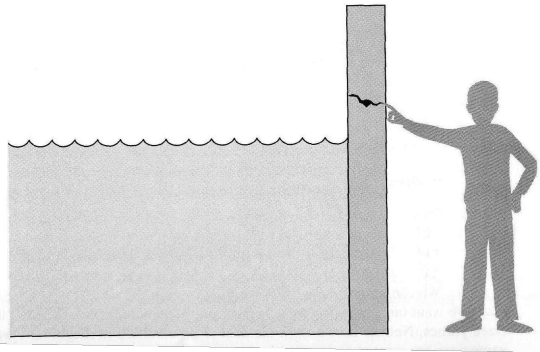
- 1.1 What Does "Secure" Mean?
- 1.2 Attacks
- 1.3 The Meaning of Computer Security
- 1.4 Computer Criminals
- 1.5 Methods of Defense
- 1.6 What's Next
- 1.7 Summary

Valuable Components

- computer "valuable components"
 - hardware
 - software
 - data
- any can be targeted

Threat vs. Vulnerability

- Water is the threat
- Crack is vulnerability
- Threats can be:
 - human initiated
 - computer initiated
- Threats can be:
 - attacks
 - mistake
 - failure



Controls

- A **control** is a protective measure
- “A **threat** is blocked by a **control** of a **vulnerability**”

Kinds of Threats

- **interception**
- **interruption**
- **modification**
- **fabrication**

MOM

- for a successful attack, attacker must have:
 - **method** skills, knowledge, tools to pull off the attack
 - **opportunity** time and access
 - **motive**

Universities Are Prime Targets

What the Text Says

- universities often:
 - run systems with vulnerabilities
 - have little monitoring
 - have little management
- universities promote free exchange of ideas
 - wide access
- student population frequently changes
 - old accounts stay around
 - often student workers (little training)
- many departments
 - one dept. doesn't always know what the other is doing

Pfleeger Security in Computing, Chapter 1

17

Universities Are Prime Targets

What the Book Doesn't Say

- they usually have plentiful resources
 - fast machines
 - fast networks (*Temple OC-3*)
 - large hard drives (*file repo Penn research site*)
- information
 - student, employee financial info
 - research groups work with govt., industry
 - possibly easier to crack University machines than gov't/industry partner

Pfleeger Security in Computing, Chapter 1

18

Outline

- 1.1 What Does “Secure” Mean?
- 1.2 Attacks
- 1.3 The Meaning of Computer Security
- 1.4 Computer Criminals
- 1.5 Methods of Defense
- 1.6 What's Next
- 1.7 Summary

Pfleeger Security in Computing, Chapter 1

19

1.3 Meaning of Computer Security

security should provide:

- confidentiality
- integrity
- availability (implies *timely availability*)

Pfleeger Security in Computing, Chapter 1

20

Vulnerabilities

- consider three types:
 - hardware
 - software
 - data

Hardware Vulnerabilities

- often easiest to defend against
- examples:
 - adding/removing/changing devices
 - pull the plug
 - spill soda
 - reboot with boot disk to use machine for attack, mount HDs, *etc.*

Software Vulnerabilities

- breaking software
- modify to do something different
 - *e.g.* bank software **salami attack**, or send duplicate of all transactions to attacker
- delete software
- software theft
- can use **configuration mgmt.** to avoid software modification attacks.

Types of Software Modification

- Logic bombs
- Trojan horses
- Viruses
- Trapdoors
- Information leaks

Data Vulnerabilities

- Data can be understood by lay people
 - *e.g.* SSN, address, name ...
 - don't need:
 - physical access (as in HW vulnerabilities)
 - computer skills (as in SW vulnerabilities)
- Can be very valuable
 - *e.g.* private company info.
- Can be damaging if modified
 - *e.g.* air traffic control, patient drug allergies

How Long Are Data Valuable?

- Might only be valuable for short time
 - *e.g.* Oscar winners, movie *Trading Spaces*
- Principle of Adequate Protection
 - Items must be protected only until they lose value
 - Must be protected to degree consistent with value

Data Confidentiality

- Data can be compromised by:
 - wiretaps
 - bugs in output devices
 - bugs in input devices *e.g.* keystroke loggers
 - monitoring electromagnetic radiation
 - inferring one data point from other
 - just asking

Data Integrity

- concerned about data modification
- change often more effort than reading
- some sophisticated examples:
 - salami attacks
 - replay

Top Methods for Attack

- Information Week Survey (2001)
 - survey of security professionals
- Attacks:
 - 33% OS vulnerabilities
 - 27% unknown application vulnerabilities
 - 22% passwords
 - 17% abuse of valid accounts & permissions
 - 12% internal denial of service
- **Note** - 80% done by **insiders**

Outline

- 1.1 What Does “Secure” Mean?
- 1.2 Attacks
- 1.3 The Meaning of Computer Security
- 1.4 Computer Criminals
- 1.5 Methods of Defense
- 1.6 What’s Next
- 1.7 Summary

1.4 Computer Criminals

book identifies:

- amateurs
 - average user who stumbles upon vulnerability
- crackers
 - hack for the challenge
- career criminals
 - hack for personal profit

other distinction:

- script kiddies
 - download tools
 - don’t understand them
- users with skills
 - design, implement tools

Outline

- 1.1 What Does “Secure” Mean?
- 1.2 Attacks
- 1.3 The Meaning of Computer Security
- 1.4 Computer Criminals
- 1.5 Methods of Defense
- 1.6 What’s Next
- 1.7 Summary

Methods of Defense

- **prevent** - close vulnerability
- **deter** - make attack more difficult
- **deflect** - make another target attractive
- **detect** - know when attack occurs
- **recover** - mitigate attack's effects

Controls in a Castle

- strong gate
- heavy walls
- moat
- arrow slits
- drawbridge

Controls in Computer Security

- encryption
- software controls
- hardware controls
- policies and procedures
- physical controls

Controls: Encryption

- important part of security
- but many more things in the picture
 - Bellovin survey of CERT vulnerabilities
- much more about encryption later

Controls: Software

- internal program ctrls
 - part of program
 - enforces sec. restrictions
 - *e.g.*, access ctrl in DBMS
- OS, net controls
 - same for OS, nets
 - protect OS, net from users
 - protect users from each other
- ind. control programs
 - *e.g.*, passwd checkers, IDS, antivirus
- development controls
 - quality standards
 - used during:
 - design
 - coding
 - testing
 - maintenance

Controls: Hardware

- Examples
 - smart cards
 - locks, cables
 - user identification devices
 - firewalls
 - IDS
 - circuit boards that control access to storage media

Controls: Policies & Procedures

- *i.e.*, “*human*” policies and procedures
- very important, often overlooked
- examples:
 - proper use of passwords
 - what not to write in email
 - what not to say over the phone
 - what not to say to strangers (or let overheard)
 - probes for stock insider info, HIPAA, etc.
 - documents to shred or not

Controls: Physical

- Examples:
 - guards
 - locks
 - backups (including off site)
 - etc.

Effectiveness of Controls

- controls don't help if not used
 - can do the opposite - false sense of security
- making sure they're used:
 - make users aware of necessity
 - simplicity of use
 - overlapping controls, *i.e.*, a *layered defense*

Principle of Effectiveness

- controls must be used and used properly to be effective
- they must be:
 - efficient
 - easy to use
 - appropriate

Principle of Weakest Link

- Security is no stronger than the weakest link
- weakest link can be:
 - firewall's power supply
 - OS that a security app runs over
 - human who:
 - plans
 - implements or
 - administers controls

Outline

- 1.1 What Does "Secure" Mean?
- 1.2 Attacks
- 1.3 The Meaning of Computer Security
- 1.4 Computer Criminals
- 1.5 Methods of Defense
- 1.6 What's Next
- 1.7 Summary

1.6 What's Next

- Encryption (ch. 2, 10)
- Hardware, software controls
 - program security (ch. 3)
 - OS (ch. 4)
 - trusted OS (ch. 5)
 - database security (ch. 6)
 - network security (ch. 7)
- Human controls
 - security planning, etc. (ch. 8)
 - law and ethics (ch. 9)

Outline

- 1.1 What Does “Secure” Mean?
- 1.2 Attacks
- 1.3 The Meaning of Computer Security
- 1.4 Computer Criminals
- 1.5 Methods of Defense
- 1.6 What's Next
- 1.7 Summary

1.7 Summary

- Security may provide:
 - confidentiality
 - integrity
 - availability (to authorized users)
- Attacks can be against:
 - hardware
 - software
 - data
 - communications of above
- Attacks:
 - interception
 - interruption
 - modification
 - fabrication
- Important principles:
 - easiest penetration
 - timeliness
 - effectiveness
 - weakest link
- Controls:
 - program
 - system/net
 - physical
 - human