## SE-4920: Lecture 2 Security Principles

- Today's Outcomes...
  - Discuss the 12 generally accepted principles of information security
  - Discuss the 8 generally accepted principles underlying security mechanisms

1

## Definitions

- Information security
  - The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use [McDaniel 94]
- Security policy
  - The rules and laws in place to ensure a certain level of security for people, devices, and networks
- Security mechanism
  - A physical or software device or algorithm that enforces a security policy

2

## IS Principle 1: There is no such thing as absolute security

- Consider combination safe locks
  - With increased cost, they can be made very tamper resistant, tamper evident, etc.
  - But, an attacker with sufficient resources will be able to break through
- Safe lock approach
  - Testers get a certain amount of time and tools, then a rating is assigned
- Moral
  - Match the security investment to the value of the asset (see also IS principle 7)

3

## IS Principle 2: The three security goals are "CIA"...

- Confidentiality
  - Only disclose to authorized parties (*cf.*, "least privilege")
- Integrity
  - Ensure that data are not tampered with
- Availability
  - Ensure that authorized users are guaranteed access despite equipment (or personnel) failures, sabotage, and attacks
- Choose 1, 2, or all 3 depending upon application
- We will see that cryptography primarily addresses C and/or I
  - Can also address A in limited situations

4

## IS Principle 3: Defense in depth as strategy

- Must pierce one layer before reaching the next
- Views
  - Redundancy (multiple mechanisms – several/all must fail for security to fail)
    - *E.g.*, guard, keycard access, motion detector
    - *E.g.*, multiple hashes for integrity
  - Provide prevention, detection, and response by separate mechanisms

5

## IS Principle 4: When left on their own, ...

- people tend to make the worst security decisions
- Example:
  - Organizers of the 2003 InfoSecurity Europe conference asked commuters (who were office workers) at a mass transit station what their passwords were, offering a free pen.
  - 75% responded immediately, 90% after some prodding
- Example: many people fall for email banking scams, information "phishing", etc. every day
- Solutions?
  - Education
  - Multifactor authentication (chapters 9 and 10)
  - Make security easy/transparent (more later – design principle 8)
  - ...

6

## IS Principle 5: Computer security depends on...

- two types of requirements:
  - Functional
    - What the system should do
  - Assurance
    - Process for implementing and testing
- Also: Validation and verification
- Common pitfall
  - assure/verify certain attributes
  - while missing other key ones (lack of proper functional requirements / validation)
- A solution: checklists and best practices

7

## IS Principle 6: Security through obscurity is not an answer

- Compare with the "Fundamental Tenet of Cryptography" [Kaufman 02, p. 41]:
  - "If lots of smart people have failed to solve a problem, then it probably won't be solved (soon)."
- One approach: keep the algorithm secret... But people can still probe and disassemble
- A commonly accepted, better approach: make it public, challenge the smart people to break it

8

## IS Principle 7: Security = risk management

- Balance value of asset with cost of security
- Risk management seeks to identify and understand two key aspects of each risk: consequences (cost) and likelihood
- Understand the "attacker" as the link between "vulnerability" and "exploit"
  - Need to identify attackers and vulnerabilities
- Outcomes:
  - Risk mitigated / countered
  - Insurance against loss
  - Accept risk, manage consequences

9

## IS Principle 8: The three types of security controls are…

- preventative,
- detective,
- and responsive

10

## IS Principles 9-12

- 9: Complexity is the enemy of security
- 10: Fear, uncertainty, and doubt do *not* work in selling security
- 11: People, process, and technology are *all* needed to adequately secure a system or facility
- 12: Open disclosure of vulnerabilities is good for security

11

## 8 Security Mechanism Design Principles

- Lower level principles to be applied when designing a cryptographic algorithm, a new software security mechanism, etc.
- Focus on two things
  - Simplicity – ease analysis
  - Restriction – limit damage

12

## Design Principle 1: Least Privilege

- Only grant a principal (user, system) the privileges *necessary* for task completion
- Reason: limit potential for intentional/unintentional misuse
- Limitations
  - Granularity of permissions (time / whole directory)
  - Tasks change over time (a solution: roles?)

13

## Design Principles 2-3

- Fail-safe defaults
  - If a subject lacks explicit access to a needed resource, access should be denied by system
- Economy of mechanism
  - Security mechanisms should be as simple as possible
  - Guard against unexpected interactions across the network or software modules; avoid assumptions about security
    - *E.g.*, avoid need to store password in a file
    - Instead, use a simple, well-understood key-based authentication mechanism – more later

14

## Design Principles 4-5

- Complete mediation
  - Check all object accesses for proper permission (*e.g.*, caching ability to read may be dangerous)
- Open design
  - Like IS principle 6 / fundamental tenet

15

## Design principle 6: Separation of privilege

- Avoid granting rights based on a single condition (*e.g.*, username)
- *E.g.*, add the need for a key, group membership, etc., to guard important resources
- *E.g.*, Two company officers must sign checks for greater than $N.

16

## Design principle 7: Least common mechanism

- Mechanisms for accessing different resources should not be shared.
- Example mechanisms: web interface, network connections, shared memory
- Problems with sharing
  - A user prevents another user from accessing
  - The mechanism conveys unintended state information
- Examples
  - Flooding a server with meaningless requests might prevent it from responding to legitimate work
    - Solution: efficiently separate valid requests at the protocol level (stateless cookies [text sec. 16.5])
  - State stored in shared libraries allows one application to learn what others are doing

17

## Design principle 8: Psychological acceptability

- The security mechanism should not make the system harder to use
- A tall order!
- In practice:
  - Meaningful, informative error messages
  - Public key authentication (Chapter 6)
- Potential pitfall: error messages should not impart unnecessary information, *e.g....*
  - whether account exists
  - what version of software is running

18

## General References

- *Information Security: Principles and Practices*, by Mark Merkow and Jim Breithaupt, ISBN 0131547291, Prentice Hall, 2006. (Chapter 2)
- *Computer Security: Art and Science*, by Matt Bishop, ISBN 0201440997, Addison Wesley, 2002. (Chapter 13)

19

## Specific References

- IS1: Safecracking for the computer scientist by Matt Blaze
  - http://www.crypto.com/papers/safelocks.pdf
- IS4: Office workers give away passwords for a cheap pen by John Leyden
  - http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/

20

## Bibliography


- [McDaniel 94] *IBM Dictionary of Computing.* George McDaniel, ed. McGraw-Hill, 1994.
- [Kaufman 02] *Network Security*, 2 ed., Charlie Kaufman, Radia Perlman, and Mike Speciner, Prentice Hall, 2002.
  - Course textbook


21