CMSC 426
Principles of Computer Security

Standards, Requirements, and Principles

Last Class We Covered

- Course Information and Syllabus
  - Grading Scheme
  - Academic Integrity
- Security Objectives
  - CIA Triad
- Avenues of Attack

Any Questions from Last Time?

Today's Topics

- Security Standards
  - Standards Bodies
- Security Principles
- Security Strategy

Security Standard

- There is no one, single security standard
  - Also no one, single standards board/creator

- The more well-known standards boards (for security) include
  - ISO (International Organization for Standards)
  - IETF (Internet Engineering Task Force)
  - NIST (National Institute of Standards and Technology)

Importance of Standards

- Interoperability
- Compliant equipment and software
- Assures market share for vendors of technology

- Good security is…
  - Difficult
  - Tricky
  - Sophisticated
  - Not for newbs

ISO (International Organization for Standards)

- Worldwide organization of national standards bodies
  - "ISO" isn't an acronym – it's Greek for "equal"
- ISO has committees and standards on many different topics
  - 27000-series: information technology (security techniques)
  - 676: spices, 2074: plywood, 3029: photography, 6009: hypo needles
- Access to most of these standards is behind a pay wall

IETF (Internet Engineering Task Force)

- Part of “The Internet Society” along with the IAB and IESG (Architecture Board and Engineering Steering Group)

- Global professional membership organization
- Charters working groups to develop (voluntary) standards
  - Drafts of standards are called RFCs (Requests for Comment)
- IETF drafts RFCs, which the IESG can approve into standards
- IETF is split into working groups that focus on specific topics

NIST (National Institute of Standards and Technology)

- Part of the US Commerce Department
  - Applies to US government departments and agencies
  - Many standards are still used widely in international industry

- Standards are FIPS (Federal Information Processing Standards) and SP (Special Publications), and include things like
  - FIPS 197: Advanced Encryption Standard
  - SP 800-78-4: Cryptographic Algorithms and Key Sizes for Personal Identity Verification
  - SP 800-9C: Recommendation for Random Bit Generator Constructions

Security Principles

Fundamental Security Design Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Psychological acceptability
- Modularity
- Layering

Information taken from Computer Security (Stallings & Brown)

Economy of Mechanism

- Design of security measures is as simple and small as possible

- Easier to test
- Easier to verify
- Less opportunities for weaknesses and exploits
- Simplifies configuration and management

- KISS

Information taken from Computer Security (Stallings & Brown)

Fail-safe Defaults

- Default situation is a lack of access
- Security identifies when access is permitted
- Why is this an important distinction?
  - In the case of error, access is not available to authorized users

Information taken from Computer Security (Stallings & Brown)

Complete Mediation

- Every access is checked against the mechanism
- Nothing is cached, nothing is assumed

- Requires considering how updates to access rights are propagated and stored throughout the system

- Hardly ever done completely
  - Once a user has opened a file, they're assumed to have access for near-future writes and reads

Information taken from Computer Security (Stallings & Brown)

Open Design

- Opposite of “security by obscurity”
- Design of a security mechanism should be open

- Passwords are secret, but how they’re entered and used is not
- Encryption keys are secret, but encryption algorithms are not

- Allows experts (and everyone else) to examine them for flaws
- Leads to higher confidence when using them

Information taken from Computer Security (Stallings & Brown)

Separation of Privilege

- Multiple privilege attributes are required for access
- Commonly used in two different ways:
  - Multi-factor authentication (password and ID card/biometrics/etc.)
  - Program divided into parts, each with specific privileges to perform specific tasks
- Prevents attacks from causing widespread damage

Information taken from Computer Security (Stallings & Brown)

Least Privilege

- Processes and users operate with the lowest set of permissions necessary to perform a task

- For example: reading, writing, and executing are separate permissions in many role-based access control systems
- “Run as administrator” is not default

Information taken from Computer Security (Stallings & Brown)

Psychological Acceptability

- Security mechanisms should:
  - NOT interfere with users
  - Meet the needs of authorizers
  - “Make sense”

- Mechanisms should be transparent and minimally obstructive

Information taken from Computer Security (Stallings & Brown)

Modularity

- Security functions are developed separately from other modules
- Security functions can be “plugged in” to other applications
  - Including replacing one security function with another in future

- No need to have hundreds of people individually re-invent the wheel
  - Especially when the “wheel” is complex and finely-tuned

Information taken from Computer Security (Stallings & Brown)

Layering

- Use multiple, overlapping approaches to ensure security
- If one layer is breached or circumvented, another can pick up the slack
- Multiple layers means requiring multiple means of attack to gain access to protected information and systems

Information taken from Computer Security (Stallings & Brown)

Security Strategy

Security Strategy

- Security is only as good as the people/systems using it
- If the system is too inconvenient, then it won't be used properly
  - Examples?
  - Passwords must change monthly → "pass1" "pass2" "pass3" "Pass3"
  - System requires key to unlock → make copy, leave in keyhole
  - Users must have expensive ID card → let multiple people use same one
- These considerations must be balanced when making decisions

Security Tradeoffs

- Ease of use VS. security
  - Passwords must be remembered/typed in
  - Firewalls might reduce transmission capacity or slow response time

- Cost of security VS. cost of failure and recovery
  - Monetary cost of implementing and maintaining security
  - Monetary cost of needing to recover (data or public face)

Information taken from Computer Security (Stallings & Brown)

Daily Security Tidbit

- June 1903, a demonstration of Morse code transmitted wirelessly was done at London's Royal Institution
- Message was to be sent from Cornwall (300 miles away)
  - From Guglielmo Marconi, who invented technique, to Ambrose Fleming, running a receiving apparatus in the theater
  - Before it could begin, messages of "Rats" and "There was a young fellow of Italy, who diddled the public quite prettily" were received
    - This message was sent by Nevil Maskelyne, who was frustrated by Marconi's wide patents on the technology
    - Fleming called the attack "scientific hooliganism"

Information taken from https://www.newscientist.com/article/mg21228440-700

Announcements

- None today!