Protection and Security

- Reading: OS Concepts, Ch. 19 – Security
- Protection
  - Of objects (memory, devices, files, etc.)
  - Normal mechanism used is an access matrix
  - Normally just done for files
- Security
  - External Protection…

The Problem

- Requirements
  - Secrecy: _____
  - Integrity:_____
  - Availability: _____
- Must protect against both accidental and malicious misuse
- Protection is needed at 4 levels
  - Physical: _____
  - Human: _____
  - Network: _____
  - OS: _____

User Authentication

- Basis for user authentication is typically one of
  - Possession of some physical object
    - E.g. _____
  - Knowledge of something
    - E.g. _____
  - Attribute of the user
    - _____
    - _____
    - _____
    - _____
    - _____
  - A combination works best…

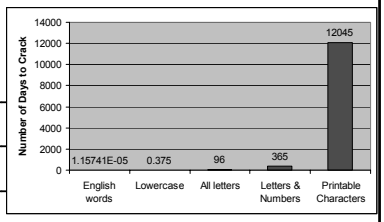



Obtaining Passwords

- Collect and use information about users
- Brute Force: _____
  _____
- Shoulder surfing: _____
- Sniffing: _____
- Exposure: _____
- Help from a friend: _____
  _____
- Defaults: _____
  _____

Protecting Passwords

- Use System generated passwords?
  - Problems: _____
    _____
- No guessable passwords:
  - _____
    _____
    _____



- Aging: _____
- Invalid attempts: _____
- Paired passwords: _____

Storing Passwords

- Passwords must be stored securely
- To do this we need an encryption function as follows:
  - f(x) = y _____
  - Security: _____
  - Store y: _____
  - To validate users: _____
    _____
  - Risks: _____
    _____

Intrusion Detection

- What is an intrusion? How can we detect it?
- _____
  _____
- Signature detection: _____
  _____
  - E.g. _____
    _____
- Statistical anomaly detection
  - _____
  - _____
  - Need to maximize P(I | A) and P(¬I | ¬A)
    _____

Auditing & Logging Example

- Need the OS to log all security related events in order to form an audit trail
- In UNIX
  - Default: _____
  - _____
    _____
  - syslog: _____
    - _____
  - swatch: _____
    - e.g. _____
    - Too simple: _____

Anomaly Example

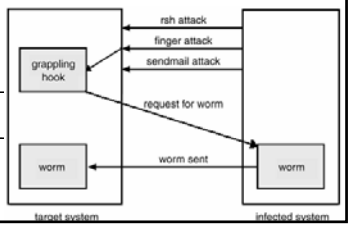
- File System Integrity: Monitoring changes to SOME files in the file system
  - _____
  - _____
  - _____
- Tripwire is a file system integrity check tool
  - Monitors specified i–node attributes: e.g. _____
    _____
  - _____
  - Problems: _____
    _____

Program Threats

- Trojan Horse: _____
  _____
  _____
- Trap Door: _____
  _____
  - e.g. _____
- Stack & Buffer Overflow: _____
  _____
- Logic Bomb: _____
  _____
  _____

System Threats – Worms

- Worms
  - Use some mechanism to replicate themselves
  - Standalone programs: _____
  - e.g. Internet Worm (1988)
    - Grappling Hook: _____
    - Worm: _____
      - Attack using rsh
      - Attack using finger
      - Attack using Sendmail
    - Effects _____
    - Sentence _____



System Threats – Viruses

- Example Mechanism
  - Modifications: _____
    _____
  - Payload: _____
- Types
  - Parasitic: _____
  - Memory-resident: _____
  - Boot sector: _____
  - Stealth: _____
  - Polymorphic: _____

System Threats – Denial of Service

- _____
  _____
- _____
  _____

Threat defence

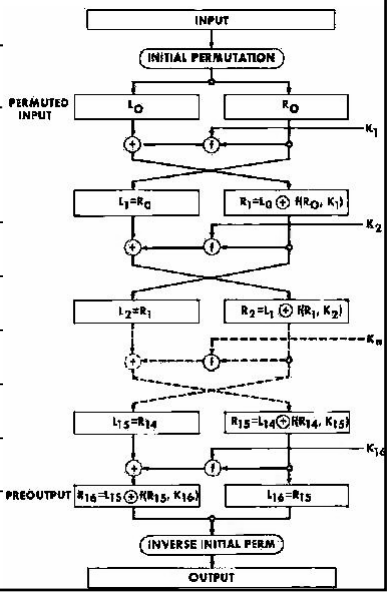
- To defend against all these threats…
  - _____
  - _____
    _____
  - Practice Safe computing
    - _____
    - _____
  - _____

Cryptography

- Authentication: _____
- Encryption: _____
  - E(k)(m) = c _____
  - D(k)(c) = m _____
- Symmetric Encryption: _____
  _____
  - Uses: _____
- Asymmetric Encryption: _____
  _____
  _____
  - Uses: _____

Cryptography – DES

- Key size _____
- Possibilities _____
- Computation
  - _____
  - _____
  - _____
  - _____
  - _____
  - _____



Cryptography – AES

- DES Cracker: _____
- Triple DES: _____
- AES: _____
  - Uses the "Rijndael algorithm"
  - Key size: _____
  - Possibilities: _____
  - Computation: an iterative application of
    - SubBytes() _____
    - ShiftRows() _____
    - MixColumns() _____
    - AddRoundKey() _____

Cryptography – SSL

- SSL: _____
- https: _____
- Server & Client authentication
  - _____
  - _____
- Mechanism for SSL requires
  - _____
  - _____
  - _____
  - Use of the encrypted SSL connection
- Ciphers: _____