System Security

Passwords and Password Cracking

Authentication vs. Authorization

- Authentication
  - Proving you are who you say you are
  - Tools: passwords, biometrics
- Authorization
  - Given who you say you are, do you have privilege to do a particular action / affect a particular object?
  - Tools: access control lists, privileges

Password Security/Policy Issues

- Length
- Required Characters (Letters, Letters plus Digits, Letters plus Digits plus Special Chars, etc.
- Prohibited Constructs (e.g. Dictionary Words)
- User Changeability (Require/Prevent User From Changing)
  - How often?
- How password remembered (memory, written, on system, etc.)

Classic Techniques

- Try all possible passwords
  - Difficult, as most systems disconnect after small number of attempts, lock out after more
- Break the encryption scheme
  - Difficult with current one-way encryption methods
- Find password file and compare encrypted passwords
  - Linux - /etc/passwd, world-readable, but passwords encrypted
  - Line from unshadowed /etc/passwd:
    - wagnerpj:3#aVu5O1:2510:10::/home/pjw:/bin/tcsh
  - Linux (better) – use shadow password file /etc/shadow, with only system access (content as on line above)
  - Line from shadowed /etc/passwd:
    - wagnerpj:x:2510:10::/home/pjw:/bin/tcsh
  - Run password cracker program, compare encrypted versions of possible passwords from sample file with actual encrypted passwords in file
  - Another technique: search for certain patterns (e.g. NULL in the password field of /etc/passwd => no password set)

Possible Password Sources

- Regular dictionary
- Special cracker dictionary
  - Common phrases, names, bands, slang, expletives, etc.
- Combinations of relevant numbers and constructs from above sources
- Knowledge about user

Comparison re: Length/Content

- 6 chars, Letters (52 upper and lower)
  - 52^6 = 19.7 billion possibilities
  - Easier to crack
- 8 chars, Letters plus Digits plus Special (approximately 82 characters)
  - 82^8 = 2 quadrillion possibilities
  - 100,000 times harder (longer) to crack

Enforcing Password Policies - Linux

- System utilities
  - passwd
  - npasswd (replacement for passwd)
  - File: /etc/login.defs

Enforcing Password Policies - Windows

- Windows System – Group Policy Editor
  - Start/Run: gpedit.msc
    - Computer Configuration
    - Windows Settings
    - Security Settings
    - Account Policies
    - Password Policy
  - Items to control: keep password history, min and max age, min and max length, complexity requirement, encryption

Defensive Issues

- Weakest Link Theory
  - One weak password on system jeopardizes other users, system
  - Security officer should check all passwords periodically to make sure there aren't potential problems
    - What to do if find problems?
      - Notify users
      - Lock out accounts

Password Encryption Techniques and Tools - Linux

- Crypt – tool for encrypting many passwords under Unix/Linux
  - Based on Data Encryption Standard (DES)
- PAM – Pluggable Authentication Modules
  - Supports dynamic configuration of authentication for multiple applications

Password Encryption Techniques and Tools - Windows

- Passwords stored in protected part of registry (SAM file)
- rdisk command – can back up SAM
- Password crackers can analyze this backup file
- Other tools can extract the password information directly
  - E.g. SAMInside

Password Cracking Tools

- Linux
  - John the Ripper (http://www.openwall.com/john/)
  - crack (http://www.crypticide.org/users/alecm/)
- Windows
  - L0phtCrack (http://www.evadenet.com/downloads/lophtcrack.shtml)
  - John the Ripper (see above)
  - SamInside (http://www.insidepro.com)
- Functionality
  - Check word lists against password files
  - Increasing support for cracking other types of passwords; e.g. mySQL (database management system), LDAP (network directory)

Account Management

- Related issue
- Need to monitor accounts
  - If no longer needed, remove them
  - Periodically check for unused accounts, remove them
- Need policy for abuse of accounts (e.g. not maintaining password secrecy)