Unit OS7: Security

7.1. The Security Problem

Copyright Notice

Roadmap for Section 7.1

- The Security Problem - a Definition
- Program & System Threats
- Security Ratings

The Security Problem

- System is secure if its resources are utilized and access is as intended under all circumstances
- Security violations:
  - Unauthorized reading of data (theft of information)
  - Unauthorized modification of data
  - Unauthorized destruction of data
- Security measures:
  - Physical
  - User authorization
- Weakness at high-level security may circumvent low-level (operating system) measures

Solving the Security Problem

- Access to a system (1) vs.
  access to resources on a system (2)
- (1) is solved through
  - Authentication
  - Local or networked database of users
- (2) is solved through
  - Permissions
  - Mandatory vs. discretionary access control
  - Capabilities vs. access control lists

Authentication

- Username/password, biometric ID, smartcards
  - Special case of keys/capabilities
  - System generated vs. User generated passwords (hard to remember/easy to guess)
  - Paired passwords: system selects one/user responds appropriately
- How to store passwords securely
  - one-way functions executed on passwords
    - easy to calculate but hard to invert
  - Shadow passwords
    - restricted access to password files

Security Ratings & Windows NT

- Windows NT was designed to be secure from the start, which meant aiming at achieving a security rating from a recognized rating system

- In 1981 the National Computer Security Center (NCSC www.radium.nsc.mil/tpep) was established as part of the US DoD’s NSA to help government, corporations and home users protect proprietary, confidential information

- Part of the goal was to create security ratings, also known as the “Orange Book”, which were defined in 1983

Security Ratings

A1	Verified Design
B3	Security Domains
B2	Structured Protection (Trusted XENIX)
B1	Labeled Security Protection (HP-UX, Trusted IRIX, Tru64 UNIX)
C2	Controlled Access Protection (highest level considered practical for general purpose OS)
C1	Discretionary Access Protection (obsolete)
D	Minimal Protection (e.g. DOS)

Windows Security Support

- Microsoft's goal was to achieve C2, which requires:
  - Secure Logon: NT provides this by requiring user name and password
  - Discretionary Access Control: fine grained protection over resources by user/group
  - Security Auditing: ability to save a trail of important security events, such as access or attempted access of a resource
  - Object reuse protection: must initialize physical resources that are reused e.g. memory, files

Windows Certification

- Certifications achieved:
  - Windows NT 3.5 (workstation and server) with SP3 earned C2 in July 1995
  - In March 1999 Windows NT 4 with SP3 earned e3 rating from UK's Information Technology Security (ITSEC) – equivalent to C2
  - In November 1999 NT4 with SP6a earned C2 in stand-alone and networked environments
- Windows meets two B-level requirements:
  - Trusted Path Functionality: way to prevent trojan horses with "secure attention sequence" (SAS) - Ctrl-Alt-Del
  - Trusted Facility Management: ability to assign different roles to different accounts
    - Windows does this through account privileges

Common Criteria

- New standard, called Common Criteria (CC), is the new standard for software and OS ratings
  - Consortium of US, UK, Germany, France, Canada, and the Netherlands in 1996
  - Became ISO standard 15408 in 1999
  - For more information, see http://www.commoncriteriaportal.org/ and http://csrc.nist.gov/cc
- CC is more flexible than TCSEC trust ratings, and includes concept of Protection Profile to collect security requirements into easily specified and compared sets, and the concept of Security Target (ST) that contains a set of security requirements that can be made by reference to a PP
- Windows 2000 was certified as compliant with the CC Controlled Access Protection Profile (CAPP) in October 2002
  - Windows XP and Server 2003 are undergoing evaluation

A Note About Physical Security

- Windows is definitely *not* secure if someone has physical access:
  - At the minimum they can destroy data
  - They can easily gain access to FAT/FAT32 files (by booting DOS)
  - They can gain access to NTFS files with NTFSDOS or ERD Commander (or free Linux-based tools)
- Encryption (like EFS) is the only way to secure data on systems that can have compromised physical security (like laptops)
  - On Windows 2000, must encrypt with domain credentials
  - On Windows XP & higher, the local administrator account is no longer a recovery agent
  - Since credentials are cached and can be cracked, must remove SAM's encryption key from system (use syskey level 1 or 2)

Further Reading

- Mark E. Russinovich and David A. Solomon, Microsoft Windows Internals,
  - 4th Edition, Microsoft Press, 2004.
  - Security (from pp. 485)

- Ken Thompson, Reflections on Trusting Trust, Communication of the ACM, Vol. 27, No. 8, August 1984, pp. 761-763.