Certified OS Hierarchies

Internal Roles

- Internal features: privileged mode, memory protection, file access permissions, etc.
- What do they accomplish?
- What is the real goal?

Whom do we protect

- Internal features protect the operating system against users
  - This necessary but not sufficient
- File permissions protect users (and the OS) against other users
  - Again, this is necessary but not sufficient

User Authentication

- File permissions are based on user identity, which is based on authentication
- How does an OS authenticate users?
  - Many methods: something you know, something you have, something you are

Something You Know

- Passwords
- Hashed Passwords
- Challenge/Response – Authentication

- HUMAN Element

Something You have

- Token – tamper proof device
-

Something You are

- Biometric

Attacks

- Trojan horses — “come and get it” attack
  - Trick someone into executing a program that does nasty things (Many viruses and worms spread that way)
  - How can the OS protect users?
  - Unix-type file permissions don’t help — the attack program can change permissions
  - Need mandatory access control (MAC)
- Login spoofing
- Buggy software — the big one

Sandboxes

- OS to provide sandboxes — an environment where the program can execute but can’t affect the rest of the machine
- Strong isolation is conceptually pretty easy — run the program on a separate machine, or under VMware or the like
- There are other, more elegant mechanisms that attempt to provide the same feature at lower cost; most are limited to root
- The trick — and it’s a very difficult one — is permitting limited interaction with the outside world while still protecting security

Race Conditions

- Consider a privileged program that checks if a file is readable and then tries to open it as root
- The attacker can pass it a symlink; in the interval between the two operations, the attacker removes the symlink and replaces it with a link to a protected file
- The OS must provide (and the application must use) atomic operations to open the file as that user

Fake LOGIN

login:

- Is that the real login prompt?
- A fake one could capture your login and password
- Many similar FAKES – CC readers, ATMs …

Trusted Path

- A trusted path is a user-initiated sequence that is guaranteed to get you to the real OS
- Example: cntl+alt+delete on Windows
- Well, it was supposed to be one. . . But — you have to train people not to log in unless they’ve initiated the sequence
- Must protect all password prompts that way

Viruses and Worms

- Viruses spread by themselves within a machine, but require human intervention to infect other machines
- Worms spread between machines, though they may require human assistance (i.e., opening an attachment) to infect another machine
- What can the OS do to stop these?

Access Controls Won’t Realize it

- One sometimes hears that “Windows is infested with these things because it has no (effective) file protection”
- File protection would prevent OS contamination, but worms can and do spread with user permissions
    - The IBM Christmas Card “Virus” (1987) relied on a Trojan Horse emailed shell script
    - The Morris Internet Worm (1988) was multi-exploit, multi-platform and didn’t violate any OS protections

Blocking Executables

- Operating systems can try to block suspicious content
- Very hard to do — lots of ways to sneak stuff in
- Windows XP SP2 “tags” downloaded files — anything that’s tagged is deemed non-executable
- But what about things like bug fixes, that you should permit to be downloaded?

Certified Systems

- In the early 1980s, the U.S. Defense Department created the so-called Orange Book (DoD Trusted Computer System Evaluation Criteria) and its companions
- The Orange Book described a set of secure system levels, from D (no security) to A1 (formally verified)
- Higher levels had more features; more importantly, they had higher assurance

Hierarchy (1)

- D – Minimal Protection: no security is required; the system did not qualify for any of the higher ratings.
- C1 – Discretionary Security Protection: the system must identify different users (or jobs) running inside the system, and provide mechanisms for user authentication and authorization to prevent unprivileged user programs from interfere each other (e.g., overwriting critical portions of the memory).
- C2 – Controlled Access Protection: the system meets additional security requirements than that of C1 that include access control at a per user granularity (access control for any subset of the user community); clearing of newly allocated disk space and memory; and ability of auditing (logging) for security relevant events such as authentication and object access, etc.

Hierarchy(2)

- B1 – Labeled Security Protection: the system must implement the Mandatory Access Control in which every subject and object of the system must maintain a security label, and every access to system resource (objects) by a subject must check for security labels and follow some defined rules. **RWFM**
- B2 – Structured Protection: few new security features are added beyond B1; rather the focus is on the structure (design) of the system to maintain greater levels of assurance so that the system behaves predictably and correctly (such as, a minimal security kernel, trusted path to user, and identified covert channels,etc

Hierarchy (3)

- B3 – Security Domains: more requirements to maintain greater assurance that the system will be small enough to be subjected to analysis and tests, and not to have bugs that might allow something to circumvent mandatory access controls, e.g., support of active audit, and secure crashing, etc.
- A1 – Verified Design: no additional features in an A1 system over a B3 system; rather there are formal procedures for the analysis of the design of the system and more rigorous controls on its implementation.
- Most existing commercial operating systems are with the ratings of C2 or below.

Challenge

- Certification + performance + usability

Assignment 2b

- 1. Construct RWFM model for BLP, Biba
- 2. Construct RWFM for RBAC
- 3. Construct RWFM Model for Chinese Wall Model

- SUBMISSION of Assignment 2: 10 April 2017