CSE 543/Fall 2007 - Homework

Due: Thursday, Oct 25, 2007 — Professor Trent Jaeger

Please read the instructions and questions carefully. You will be graded for clarity and correctness. Write legibly and check your answers before handing it in. **Do your own work!**

1. (*10pts*) Answer the following questions regarding reference monitoring.

   (a) Define a *reference monitor* and the guarantees of a true reference monitor implementation.

   (b) How does the Multics reference monitor implementation satisfy these guarantees?

   (c) Does a sandbox, such as Janus, implement a reference monitor? Why or why not?

   answer:

   (a) A reference monitor processes authorization queries using the protection state. A true reference monitor provides tamper protection of itself, complete mediation of security-sensitive operations, and verifiability of its correct implementation and enforcement of security goals.

   (b) Multics mediates access to segments and all security-sensitive operations are on segments. Multics enables definition of mandatory access control policies for secrecy (Bell-LaPadula) and integrity (ring brackets) to define a protection state that enforces its protection goals. The reference monitor is implemented in a ring 0 kernel that is protected by the mandatory integrity policy. Hopefully, its implementation is correct, but there is no guarantee of that (consider the Multics vulnerabilities found by Karger and Schell).

   (c) Yes, a sandbox attempts to satisfy the reference monitor properties although it is limited in its ability – you might say it cannot because of these limitations as well. A sandbox tries to mediate

all security-sensitive operations (system calls are mediated by Janus), with a tamperproof module (although it runs in user-space), and a mandatory access control policy that hopefully enforces the desired security goals (although is usually used for least privilege).

2. (*8pts*) Consider a capability system. There are four major problems in building a secure capability system (meets reference monitor requirements). Name them. List one of the solutions for each.

   answer: Problems (solutions – more than one are possible): (1) Handing out capabilities to the correctly authentication parties (solution: grant initial set of caps based on authenticated identity using ACL, MLS policy, or authorized capability set); preventing forgery of capabilities (solns: in-kernel capability lists, crypto capability, hardware-supported capabilities, language enforced capabilities), ensuring confinement or *-property by limiting the rights of capabilities obtained from lower secrecy subjects (soln: by checking the legality of owning that capability in SCAP or weak capabilities in EROS), and ensuring revocation of capabilities should policies change (soln: revoker capabilities or capability chains).

3. (*10pts*) Answer the following questions about integrity models in your own words.

   (a) Define the Biba integrity model.

   (b) Define the Low-Water Mark (LOMAC) integrity model.

   (c) Define the Clark-Wilson integrity model (w/o audit or authentication).

   (d) What is the major difference between Biba and LOMAC?

(e) How does the integrity protection of guards in Biba differ from the protection of Transformation Procedures in Clark-Wilson?

answer:

(a) Lattice integrity model in which read-down and write-up is prohibited. Uses separate guard processes to upgrade the integrity of data.

(b) LOMAC is the same as Biba except it allows read-down or write-up, but the integrity of the process is lowered to the integrity level of the data. That is, the integrity of a process is the lowest (actual greatest lower bound of) integrity level of any data read (or executed) by a process.

(c) Clark-Wilson considers only high and low integrity data, and controls access of code to high-integrity data. High-integrity is verified at initialization by Integrity Verification Procedures. High integrity data is only processed by verified Transformation Procedures. TPs are trusted to protect themselves from low integrity inputs by immediately discarding or upgrading.

(d) LOMAC may change the integrity level of a subject if it reads lower integrity data. Biba rejects such an operation.

(e) Biba protects processes that operate on high integrity data via guard. CW requires that its high integrity data be processed by processes that are verified to both protect themselves and process the high integrity data correctly.

4. (*10pts*) Suppose that you are a Multics administrator (lucky you). You need to configure a web server to serve static and dynamic content. Suppose that the web server system consists of:

   - Web server executable file
   - Static content file
   - Database file
   - Script file
   - Admin shell process

   Suppose that the secrecy level of the static content file is *unclassified* and the database file may contain content at any secrecy level. Suppose that the script is a lower integrity codebase than the web server, and the admin shell is higher integrity than either file.

   The web server process is created by executing the web server executable from the admin shell process. The web server serves requests from either the static content or by using the script to compute a new web page from the database. However, the script cannot modify the database.

   Answer the following questions.

   (a) Select MLS secrecy levels for the files above (except the admin shell). Use the standard secrecy levels: unclassified, confidential, secret, top secret.

   (b) Select legal execution rings for the web server and dynamic content script processes (they are run in separate address spaces). Note: Kernel runs in ring 0 and admin shell in ring 2. Assume highest ring is 7.

(c) Select access brackets for the files above that protect the integrity of the files appropriately.

(d) Select call brackets for the web server and the script file that protect the integrity of the code appropriately.

(e) If an unclassified user updates the database, can she read the contents using the script as described above using the labels in (a-d)?

answer:

(a) Only the database has secrets, but they could be at the highest secrecy level.

- Web server executable file: unclassified
- Static content file: unclassified
- Database file: top secret
- Script file: unclassified

(b) Must be higher than the admin shell. Script must be higher than the web server.

- Web server executable file: 3
- Script file: ¿3

(c)

- Web server executable file: Admin can write, web server can read – (2, 3)
- Static content file: Admin can write, web server can read – (2, 3)
- Database file: Web server can write, script can read – (3, 4)
- Script file: Script level can write – (4, 4)

(d) Execute from their level or more privileged

- Web server executable file: cannot execute from below web server ring – (3, 3)
- Script file: Cannot execute below script ring – (4, 4)

(e) No.