CSE543/Fall 2010 - Midterm

Tuesday, October 19, 2010 — Professor Trent Jaeger

Please read the instructions and questions carefully. You will be graded for clarity and correctness. You have 75 minutes to complete this exam, so focus on those questions whose subject matter you know well. Write legibly and check your answers before handing it in.

Short Answer - some will be one or two words – no more than 3 sentences

1. (*4pts*) What is the difference between *protection* and *security*?

   answer: A system that provides security ensures the protection of its data (i.e., enforcement of its security goals) even when a user may run code that has malicious intent. Systems that provide protection enforce the specified policy only if the user runs trusted code.

2. (*3pts*) Define *protection state*.

   answer: The permissions available to every system principal at a particular time – a snapshot of the system's access matrix.

3. (*3pts*) How can you configure a file's access control list in Windows to permit every subject but one to access that file?

   answer: Add a negative ACE at the beginning of the file's ACL, give everyone access in next ACE.

4. (*4pts*) What is the purpose of a *public key infrastructure*? Why is there a risk for "who is using my key?"

   answer: Bind a public key to an identity securely on internet scale. System cannot protect private key from compromise.

5. (*4pts*) How would a server procedure be designed for a Hydra system to avoid the *confused deputy problem*?

   answer: Use capability templates to instantiate input capabilities for the server procedure from the client and use only those capabilities to avoid using unauthorized rights.

6. (*4pts*) What mechanisms does Multics use to protect the *secrecy* of objects?

   answer: Multics authorizes access to segments which represent memory and I/O (files). There are a variety of policies. Protection rings provide the mediation points for enforcing integrity. The access and call bracket policies describe the integrity policy of a Multics system. MLS and ACLs too.

7. (*3pts*) Why does a hash chain value (e.g., $h^i(t)$) serve as an *authenticator*?

   answer: The receiver of the hash chain value can use that value to authenticate that a particular principal holds the secret t.

8. (*3pts*) What impact does the *birthday paradox* have on the security of a 140-bit hash function?

   answer: Due to the *birthday paradox*, the probability of finding a collision in a 90 bit hash is only one in 2^{70}.

9. (*3pts*) Why is *discretionary access control* incompatible with the *reference monitor concept*?

   answer: tamperproofing.

10. (*3pts*) Why security purpose does the timestamp serve in the Kerberos protocol?

    answer: used as a nonce.

11. (*3pts*) Why is using the function $h(K + m)$ insufficient as a secure *message authentication code*?

    answer: Attacker can forge the MAC of m' where it is an extension to m.

Long Answer - no more than 3 paragraphs

12. (*7pts*) Why is an access matrix representation of a mandatory access control (MAC) policy fixed when a new subject or object is added to the system? What does the reference monitor need to do when a new object is created to control access to it correctly in a MAC system? In a MAC system, how would a `setuid` mechanism be implemented (e.g., to enable a user process to invoke a privileged `passwd` process)? In what ways would MAC improve the security of such a mechanism?

    answer: access matrix representation of a mac policy uses labels, so they are not changed by the addition of subjects or objects. Need to assign label to object. Need to associate process label with the labels it could change to when executing a file. Would limit setuid to system administration (which is similar to UNIX) and could limit the label transitions possible.

13. (*7pts*) What is the difference between LOMAC (low-water mark) integrity and Biba (strict) integrity? Show why LOMAC and Biba authorize the same set of operations on a system. What operations does ring integrity allow that Biba does not? What operations does Clark-Wilson integrity authorize that Biba does not?

    answer: LOMAC changes the integrity levels of subjects based on their inputs. In Biba, labels are fixed. ... Ring allows read-down. Clark-Wilson allows high integrity processes to read low if their a certified to discard or upgrade.

14. (*7pts*) How does the Linux Security Modules framework design aim to achieve the reference monitor guarantees? Which guarantees do you think have been achieved and why?

    answer: LSM defines a reference monitor interface aiming for complete mediation. The LSM itself must define a MAC policy that provides tamperproofing of the reference monitor. The simple enough to verify is not really attempted. None are verifiably achieved, as complete mediation is not validated and tamperproofing depends on the policy and the integrity of the trusted processes.

15. (*7pts*) What purpose does the *ticket* in a Kerberos message serve? Why isn't it necessary for the ticket include an HMAC to ensure authenticity and integrity? Why can't a malicious service, Mallory, spoof Alice to Bob by using ticket Alice provides to Mallory, $\{Alice, K, timestamp\}$, to create a ticket for Bob?

    answer: A ticket provides a session key to Bob encrypted in the TGS's key shared with the service. This way the service knows that the ticket is from the TGS.

    HMAC is not necessary because you know the format of the message.

    Since the ticket is encrypted by the TGS-Mallory key to be valid, a ticket presented to Mallory will not be of any use.

Word Problems - take your time and answer clearly and completely.

16. (*13pts*) Suppose that Alice uses a cloud computing system administered by Bob. That is, Alice sends her computations to Bob, Bob runs them on one of his available compute nodes, and Bob returns the results to Alice.

    Answer the following questions related to secure communication of the inputs (from Alice to Bob), secure computation of the results (by Bob's system), and secure communication of the results (from Bob to Alice).

    NOTE: In the questions below, when symmetric key cryptography is to be used assume that Alice and Bob share a symmetric key K and when public key cryptography is used assume that Alice and Bob have securely obtained each other's public keys, K_A^+ and K_B^+, respectively.

(a) (2pts) Using the symmetric key cryptography, write a message that Alice would use to send the inputs Inp to Bob, such that Bob can verify that they are from Alice.

(b) (2pts) Using the public key cryptography, write a message that Alice would use to send the inputs Inp to Bob, such that Bob can verify that they are from Alice.

(c) (3pts) Suppose that Bob provides compute nodes that are secure from physical threats (only trusted insiders can access the physical hardware), how would Bob use mandatory access control to prove to Alice that her computation was executed securely (can ignore network access, since we haven't done that yet – just consider subjects (processes) and objects (files) on Bob's compute node)?

(d) (2pts) Using the symmetric key cryptography, write a message that Bob would use to send the results Res and MAC policy P (say from a Linux Security Module) to Alice *secretly*, such that Alice can verify that they are from Bob.

(e) (2pts) Using the public key cryptography, write a message that Bob would use to send the results Res and MAC policy P to Alice *secretly*, such that Alice can verify that they are from Bob.

(f) (2pts) Would you trust your most security-sensitive (secret) data to such a service providing the evidence in (c)? List one key reason why or why not.

answer:

Suppose base capability is $C = \{obj, rw\}$.

(a) $Inp + HMAC(K, Inp)$
(b) $Inp + S(K_A^-, Inp)$
(c) Show that the only processes that can access Alice's data are Alice's processes in MAC policy
(d) $E(K, Res + P) + HMAC(K, Res + P)$
(e) $E(K_A^+, Res + P) + S(K_B^-, Res + P)$
(f) No. The OS is not fully trusted

17. (*10pts*) Answer the questions below regarding Diffie-Hellman key exchange and RSA key generation.

```
int DHgen(int key, int n, addr dest)
{
    int p = 3, g = 4;
    int x = n;
    int y, y';
```

```
    int z;

    y = ???; // (see part a)

    send(y, dest);
    recv(y', dest);

    z = ???; // (see part a)
    key = z;
    return 0;
}
```

(a) (2pts) Write the Diffie-Hellman equations to compute y and z in the code above.

(b) (2pts) Suppose n is 3 and y' is 5. What is your shared DH key?

(c) (2pts) Consider RSA key generation (not shown). Assume the primes are q=7 and p=5. What is $phi(n)$?

(d) (2pts) If we choose e=5, what is the smallest value of d that: (1) is a legitimate private key value and (2) not equal to e?

(e) (2pts) Why is e=21 not a valid public key value for this n?

answer: (a) $y = g^x modp$ and $z = y'^x modp$
(b) 2
(c) 24
(d) 29 (for 145, which is one more than 144)
(e) GCD(24,21) = 3 /= 1

18. (*12pts*) Suppose that you are a Multics administrator. You need to configure a password program to enable users to modify their passwords. To change password data, we execute a *password procedure* from a *user's shell process* to modify a shadow file. A summary of the key objects is below.

    - Password procedure
    - Password process
    - Shadow file: has password hashes

- User's shell process

Suppose there are two secrecy levels: (1) system secret and (2) public. The former is more secret than the latter and used to protect data that is secret to the system.

Answer the following questions.

(a) (2pts) Select secrecy levels for the files and processes above.

(b) (2pts) Suppose the user's shell process runs in ring 4. Define a call bracket for the password procedure that enables it to be run in a password process in ring 2.

(c) (2pts) Suppose that the password procedure must not be modifiable by the password process. Define the access bracket for the password procedure and adjust the call bracket, if necessary.

(d) (2pts) Define an access bracket for the shadow file that enables the password to be changed (shadow file to be modified) by the password process, but not the user shell and prevent the user shell from reading the passwords (shadow file).

(e) (2pts) If the password process was made a Multics *master mode* process, what ring would it be run withing when invoked by the user shell described in (b)?

(f) (2pts) What security guarantees would have been considered before executing the password program in *master mode* in that ring?

answer:

(a) Only the shadow file has secrets

- Password procedure: public
- Password process: secret
- Shadow file: system secret
- User shell process: public

(b) (3, 5) would work

(c) (1, 3) would work with above; a1 ¡ 2 (prevent write); a2 ¿= 2 (enable execute)

(d) (2, 3) a1 ¿= 2 (so can be modified at 2); a2 ¡ 4

(e) ring 4 - same as shell

(f) reference monitor guarantees