Michael Lee

Problem Set 3

1. Digital signature
   a. A digital signature is a way to validate the authenticity and integrity of a message as something signed with your private key could only come from you assuming the pk hasn't been broken.
   b. The digital signature can add to the length of a message because they need to add their signature to the message. MAC is the message hashed and encrypted with a shared key, so it must be appended to the message as a tag. They need to transmit extra information along with the message, and so the sent message that is transmitted is longer.
   c. Alice chooses two prime numbers p,q. n is p*q and we choose e such that it is prime to (p-1)(q-1) and d such that ed mod 0(n) = 1. Then the message is sent like this **m^p mod n = s(m)** where s(m) is the signed message. Alice can decrypt this with here private key d using **s(m)^d mod n = m.**
   d. The hash function does not need to be keyed, but if the same signing message is being hashed over and over, it would be wise to use the hashed function to provide potential leakage.
   e. You would want to sign and then encrypt message m to hide what you're doing from outside eyes. This allows the recipient to decrypt the message and then see your signature.
   f. A digital certificate is a certificate attached that verifies the user is who they claim to be granted to them by a certificate authority. The certificate chain is a chain of certificates where each is signed by the next certificate up until the certificate authority.
2. Time-Variant Parameters
   a. R1 and R2 are random messages that are send back and forth between the parties to confirm that they are who they say they are.R1 is send out in the first message and received back in the second message and it shows that whoever is sending the response received the first message.
   b. R2 is encrypted by the session key and is used to confirm that the Alice is who she says she is as she replies with R2-1. Only she knows R2-1 in theory and a would be attacker can't reply with a correct message as they won't know the session key.
   c. Time stamps are not random, but they are much easier to implement than a random number.
3. Trusted Computing
   a. Measure what program is loading, reading that measurement, how to get only authorized programs to execute, and who gets to authorize programs.
   b. Each process extends the PCR with a hash of the old PCR value along with other values, an attacker cannot change these values without being detected.
   c. A manifest is a type of certificate chain that is signed by the program's manufacturer and it is used to prove that the subject was released by them intentionally.

   d. TCB is integrated into the hardware of a machine which is critical to security, and so we can't trust a machine that is physically open because it could be tampered with.
   e. As long as the hardware is not tampered with we can continuously prove that the software was loaded by a TCB but not necessarily the intended machine.
   f. Measured boot allows the program to execute regardless if it is authorized and it may not have a manifest. Secure boot always requires a manifest and the program to be white listed.
   g. Sealed storage is where the TCB hardware seals a program's parameters generated by the program with a symmetric key pair derived from the PCR value at the time.
   h. Taking ownership and ownership transfer are the two models. Currently, take ownership is implemented because ownership transfer requires more machinery.

4. Long lived and session keys
   a. Pseudo random numbers are simulated cryptographically random numbers generated by an algorithm. They are used because we need random numbers to generate good keys, but it's difficult to generate good random numbers.
   b. Interchange keys are long lived and aren't used in general communication only to establish, while session keys expire and are used to encrypt a bulk of messages. Session keys are needed, because we don't want to keep encrypting messages with the same key it could lead to information leakage. Yes, we need symmetric keys because we want to preserve the confidentiality of our system and the integrity as a whole. Even when using symmetric keys, we want to send a temporary symmetric session key over.
   c. A trusted third party is desirable because they can't always guarantee that there's a secured channel to send and its more practical to use a trusted third party with symmetric keys. With asymmetric keys it's desirable but not needed as each sender can sign with their private keys providing security.

5. Access Control Concepts
   a. Authentication, authorization, audit.
   b. In DAC regular users can adjust the system's policy while in MAC regular users can't adjust the policy.
   c. Open means you can access anything that isn't explicitly limited. Closed means you can't access anything that's not explicitly stated.
   d. RBAC is where access is defined per roles rather than individuals, but UNIX groups just bunch up users together as an easier way to manage security. Roles are more focused on permissions during roles, while groups focus on the user and doesn't change.
   e. RBAC again uses only roles, but ABAC takes much more into account such as the user, the resource they need, environment and context to determine access.

6. Access Control Matrix

a. Develop code = dc, test code = tc, develop exec = de, test exec = te, test report = tr, production code = pc, production excec = pe, read = r, write = w, exec = x, delete = d, change = c.

b.

	dc	de	tc	te	tr	pc	pe
Eve (Manager)		rx			r	rx	rx
Alice (Programmer)	rwxdc	rwxd			r	rx	rx
Bob (Programmer)	rwxdc	rwxd			r	rx	rx
Carol (Tester)			rwxdc	rwxd	rw	rx	rx
Dave (Tester)			rwxdc	rwxd	rw	rx	rx

c. Develop exec: { (read,[Eve, Alice, Bob]), (write,[Alice, Bob]), (execute,[Eve, Alice, Bob]), (delete,[Alice, Bob]) }

d. Alice: { (read, [DC, DE, TR, PC, PE]), (write, [DC, DE]), (execute, [DC, DE, PC, PE]), (delete, [DC, DE]), {changeAccess, [DC]) }

7. UNIX Permissions

a. The file can be edited, deleted, or overwritten but it can't be seen.

11. Changing Access Control

a. Allowed, Subject C is owned by subject A and thus A can have subject C's read ability to file 2

b. Allowed, subject A has ownership over subject C and thus can remove their permissions.

12. Mutual authentication means that multiple people have to authenticate say two keys to nuclear weapons while multifactor authentication means that one user has to authenticate multiple times

13. P1 = 4, p2 = (4+5) mod 7 = 2, p3 = (2+5) mod 7 = 0

11. The * property means that users can write to a higher security level, but they can't write to a lower security level. This allows say employees to report to managers and managers to respond, but providing confidentiality between employees.

12. a. No, because MAC policy blocks users from changing the policy and they have no access.

b. Yes, because while the user doesn't have access to the file, because it's DAC they can change the policy to gain access.

13.

a.

Subject	Object	Rights
Alice	XRay	Read
Bob	Zebra	Read
Carol	Yoyo	Append
Carol	Zebra	Read

b.

Subject	Object	Rights
Alice	XRay	Read
Bob	Zebra	Append
Carol	Yoyo	Append
Carol	Zebra	Read