CS 491/591 Security and Privacy Spring 2010 Midterm

Name:_____*Key*_____

Friday 12 March 2010, 1pm to 1:50pm. **You have 50 minutes.**

Closed book, closed notes, <u>closed everything.</u> And in particular, no calculators or other electronic devices.

Check right now to make sure you have all pages of the midterm.

1 (10 points). What is the difference between a mandatory access control (MAC) and a discretionary access control (DAC)?

A mandatory access control (MAC) is enforced by the system as part of the global policy, whereas a discretionary accesses control (DAC) can be modified by the owner of the object to grant or deny permissions to other subjects.

2 (20 points). Name four things, and describe each informally with a sentence, that we can do with asymmetric cryptography that we can't do with symmetric cryptography.

1. Public key encryption - possible to encrypt with a user's public key and then only they can decrypt it (using their private key).

2. Secret key exchange - can exchange a secret key over an insecure medium, which can then be subsequently used in, e.g., a symmetric encryption scheme.

3. Signatures - can sign something with your private key, which not only provides authentication (which symmetric schemes can do), but also non-repudiation so that it can be proved (based on some assumptions about computational difficulty) that only someone who has your private key could have produced the signature.

4. Identity-based encryption - possible for a trusted third party to confirm your identity and then provide you a private key for use with that identity as the public key.

3 (18 points). Explain how the Chinese Wall Model works, what kinds of settings it is suitable for, and why it models such settings well.

See the book for how it works, it's suitable for conflict-of-interest settings. It models these well both because of the time aspect (access control decisions are based on accesses that a subject has made in the past) and the fact that the COI classes and CDs capture the notion of a conflict-of interest.

4 (15 points). Compare and contrast Denning's lattice model approach to Fenton's data mark machine. Which is static and which is dynamic? What can each do that the other can't?

Denning is static, Fenton is dynamic. Denning's approach requires well-typed source code. Fenton's approach cannot have variable data marks for registers, meaning that it cannot handle implicit flows in a precise way without augmenting it with static analysis. This is because Fenton's approach only sees the code that is actually executed (the trace), whereas Denning's approach can reason about the code paths not taken.

Note that both use lattices, both ignore covert channels, and these are information flow control mechanisms, which is a very different thing from policies.

5 (15 points). When we use Kemmerer's matrix methodology, we calculate a transitive closure of the matrix. What does this transitive closure essentially mean in terms of information flow? What does it mean to add a new R to the matrix?

If a subject S1 can read object O1, but another subject S2 cannot, then there may still be a transitive way for S1 and S2 to collude for S2 to read O1 as follows. If there exists another object O2 that S1 can modify and S2 can read, then S1 can read O1 and write the data to O2 where S2 can read it. When we perform a transitive closure in Kemmerer's shared resource matrix methodology what we are fundamentally doing is finding all the possibilities for this type of collusion so that we can see the implicit read rights, too.

Note that Kemmerer's shared resource matrix methodology and the access control matrix model are two completely different things with different contexts (covert channels vs. the safety question). They are related in a fundamental way, I suppose, but don't get these two different things confused.

6 (20 points). Give one good example and one bad example of Saltzer and Schroeder's Principle of Least Privilege from the Windows XP access control model.

Good: The set of access controls for system services is rich enough that it's possible to give a particular group of users the ability to start and stop the service, but not reconfigure it.

Bad: In the first version of Windows XP that shipped, authenticated users were given all permissions over two services (UPnP and ssdp), which could be exploited for elevation of privilege to do arbitrary things. Authenticated users probably only needed to start and stop the service.

7 (2 points). Give a succinct, intuitive explanation of how Deutsch's quantum algorithm works.

When the function is evaluated a single time on the quantum superposition, Deutsch's algorithm causes the probability density for which quantum state will be measured to focus on different states based on whether the function is constant or not.