Introduction to Computer Security
Midterm Exam
Winter 2007

This is a closed-book, closed-notes exam.

1. Short Answer. [15 points]

   Please give a **short** description of each of the following:

   (a) Access Control Matrix

   (b) Originator controlled access control

   (c) Classic (secret key) cryptography

   (d) Public key cryptography

   (e) Message digests

2. Key Management [15 points]

   Define the terms *session key* and *interchange key*. Describe a protocol that uses session and interchange keys. Discuss why it is important to distinguish these two kinds of keys.

3. Basic Principles and Voting Machines [15 points]

   (a) In English, state the security policy for a voting system. Identify which requirements address confidentiality, integrity, and availability concerns.

   (b) Summarize the vote stealing attack presented in the Feldman, Halderman, and Felten paper.

   (c) What aspects of the security policy does the vote stealing attack violate?

   (d) Feldman, Halderman, and Felten also sketch denial of service attacks; describe a denial of service attack on the Diebold voting machine.

   (e) What aspects of the security policy does the denial of service attack violate?

4. Integrity Model applied to Voting Machine [55 points]

   This question explores how the Clark-Wilson model can be applied to the voting machine described in the paper by Feldman, Halderman, and Felten (FHF).

   The Clark-Wilson model has several components. These include identifying constrained data items (CDI), integrity constraints, integrity verification procedures (IVP), transaction processes (TP), and the allows and certifies relations. **A synopsis of the Clark-Wilson certification and enforcement rules is provided following the question.**

   Assume the following set of Constrained Data Items:

   (a) Boot loader
   (b) Operating System and Trusted Applications
   (c) Voting Application
   (d) Ballot Definition
   (e) Vote Tally
   (f) Completed Ballot

   A partial set of integrity constraints includes:

   (a) New images of the boot loader, OS, Trusted Applications, and Voting Applications must include a certificate of origin signed by a trusted party. The certificate must include a message digest of the image.
   (b) The OS, Trusted Applications, and Voting Applications must pass an integrity check based on their certificate of origin before being executed.
   (c) The Ballot Definition must be signed digitally by an election official distinct from the official operating the voting machine.

   The transaction processes (TPs) are:

   (a) Update Boot Loader
   (b) Update OS and Trusted Applications
   (c) Update Voting Application
   (d) Define Ballot
   (e) Start Election
   (f) End Election
   (g) Vote

Problems

(a) Complete the model by listing additional integrity constraints. Every CDI should appear in at least one integrity constraint. [5 points]

(b) Sketch the *certifies* relation. (The certifies relation assocates a set of CDIs with a particular TP.) [5 points]

(c) Sketch the *allowed* relation. Specifically call out any separation of duty concerns. (The allowed relation defines a set of triples to capture the associate of users, TPs, and (sets of) CDIs.) [5 points]

(d) Discuss the tension between the Clark-Wilson model and the secret ballot requirement. [5 points]

(e) Given a system conforming to this model, discuss the feasibility of (1) FHF's vote stealing attack, (2) FHF's denial of service attack, and (3) FHF's mechanism for propagation of malware. Identify which (if any) integrity constraints would be violated by these attacks. Be specific about how mechanisms implementing the Clark-Wilson rules would prevent these violations. [10 points]

(f) Given a system conforming to this model, discuss the feasibility of (1) updating the voting software, (2) defining a ballot, and (3) voting. Be specific about which CDIs are modified, which integrity constraints are maintained, which relationships are verified, and which rules require which actions. [10 points]

(g) If the requirement for a secret ballot is eliminated and all aspects of the Clark-Wilson model you describe above are implemented is the resulting system robust against external threats? Is it robust against internal (insider) threats? [10 points]

(h) Several researchers have recommended the use of a Voter Verified Paper Audit Trail (VVPAT) inserted into a conventional ballot box. If this mechanism were used would it be possible to have a secret ballot without compromising the integrity properties provided by the Clark-Wilson model? Discuss. [5 points]

Synopsis of Clark-Wilson:

CR1 When any IVP is run, it must ensure that all CDIs are in a valid state.

CR2 For some associated set of CDIs, a TP must transform those CDIs in a valid state into a (possibly different) valid state.

ER1 The system must maintain the certified relations, and must ensure that only TPs certified to run on a CDI manipulate that CDI.

ER2 The system must associate a user with each TP and set of CDIs. The TP may access those CDIs on behalf of the associated user. If the user is not associated with a particular TP and CDI, then the TP cannot access that CDI on behalf of that user.

This defines a set of triples (user, TP, CDI set) to capture the association of users, TPs and CDIs. This is called the *allowed* relation.

CR3 The allowed relations must meet the requirements imposed by the principle of separation of duty.

ER3 The system must authenticate each user attempting to execute a TP.

CR4 All TPs must append enough information to reconstruct the operation to an append-only CDI.

CR5 Any TP that takes as input a UDI may perform only valid transformations, or no transformations, for all possible values of the UDI. The transformation either rejects the UDI or transforms it into a CDI.

EF4 Only the certifier of a TP may change the list of entities associated with that TP. No certifier of a TP, or of any entity associated with that TP, may ever have execute permission with respect to that entity.