# Introduction to Computer Security
## Midterm Exam
Fall 2007

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

1. Short Answer. [16 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
   (f) Virtualization
   (g) Sandboxing
   (h) Separation of duty

2. Crypto [14 points]

   Explain how public-key cryptography might be used to encrypt an email message between Alice and Bob.

3. Virtualization [15 points]

   Following Popek and Goldberg's 1974 article on virtualization, Bishop articulates two requirements for an architecture to be virtualizable:

   (a) All sensitive instructions cause traps when executed by processes at lower levels of privilege.
   (b) All references to sensitive data structures cause traps when executed by processes at lower levels of privilege.

   In the article "Intel Virtualization Technology," Uhlig, *et al.* write:

   > . . . the IA-32 and Itanium architectures both include instructions that access privileged state and do not fault when executed with insufficient privilege. For example, the IA-32 registers GDTR, IDTR, LDTR, and TR contain pointers to data structures that control CPU operation. Software can execute the instructions that write to, or *load*, these registers (LGDT, LIDT, LLDT, and LTR) at any privilege level. If the VMM maintains these registers with unexpected values, a guest OS using the latter instructions could determine that it does not have full control of the CPU.

   Three approaches to virtualizing IA-32 have been implemented: Vmware performs binary translation, Xen uses paravirtualization, and VT-x revises the architecture. Summarize each of the three approaches. Give strengths and shortcomings of each approach.

4. Information-flow security [18 points]

   Consider the six program fragments:

```
1   l := h

2   h := l

3   l := false; if h then l := true else skip

4   h := false; if l then h := true else skip

5   l := false;
    while h do l := true

6   l := false;
    while h do skip
```

   (a) Assume `h > l`. Explain informally which flows are desired and which flows should be prevented (undesired flows).

   (b) Which flows are explicit (direct in the study questions); which are implicit (indirect)?

   (c) Use the Sabelfeld and Myers type system to show that three of these programs are typable and three are not.

   (d) Volpano, Smith and Irvine define two properties, *simple security* and *confinement*. Simple security says that, when $\vdash e : \tau$, “only variables at level $\tau$ or lower in $e$ will have their contents read when $e$ is evaluated (no read up).” Confinement says that, when $[\tau] \vdash c$ “no variable below level $\tau$ is updated in $c$”.

   For each program fragment, discuss if it violates these properties.

   (e) Consider program fragments 5 and 6. Did the type system get the right answer? Discuss any anomalies concerning 5 and 6 in your answers above.

   (f) Bishop’s presentation gives a rule for while loops that requires that each loop terminates. This condition is omitted in the Sabelfeld and Myers system presented in class. Does Bishop’s requirement that all while loops terminate eliminate any anomalies? Discuss.

5. The Confinement Problem [12 points]

   In his October 1973 CACM article, Butler Lampson articulates the “confinement problem”. He articulates three kinds of channels: storage, intended, and covert.

   (a) Describe each kind of channel.

   (b) Give an example of each.

   (c) In a subsequent note Lipner comments on the confinement problem. Which of Lamport’s channels was Lipner not optimistic about closing? Why?

6. Basic Principles and Voting Machines [10 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?