Introduction to Computer Security
Midterm Exam
Spring 2009

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

1. Short Answer. [20 points]

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

   (a) Integrity

   (b) Confidentiality

   (c) Availability

   (d) Access Control Matrix

   (e) Originator controlled access control

   (f) Virtualization

   (g) Separation of duty

2. BLP [20 points]

   Summarize the Bell LaPadula security model. Describe the two conditions that define it. Paraphrase the security theorem that these conditions establish.

3. Information Warfare [20 points]

   In a March 29, 2009 article the New York Times reported on an information warfare initiative targeted against the Office of His Holiness the Dalai Lama (OHHDL). Ngaraja and Anderson wrote a technical report giving details of the incident.

   (a) What does the term information warfare mean? Why do Ngaraja and Anderson use that term to describe this incident?

   (b) How did OHHDL come to suspect that they had been infiltrated?

   (c) How do Ngaraja and Anderson conjecture the initial infiltration was accomplished?

   (d) Once a trusted machine was compromised, how did the attack proceed?

   (e) Are such attacks easily preventable? Are Nagaraja and Anderson optimistic or pessimistic about the ability of other organizations to resist such attacks?

4. BMA Model [20 points]

The British Medical Association model addresses mechanisms to keep medical records confidential. The model is distilled into nine principles, which are partially reproduced below

1 Access control: each identifiable clinical record shall be marked with an access control list . . . .

2 Record opening: a clinician may open a record with herself and the patient on the access control list. When a patient has been referred, she may open a record with herself, the patient and the referring clinician(s) on the access control list.

3 Control: One of the clinicians on the access control list must be marked as being responsible. . . .

4 Consent and notification: . . .

5 Persistence: no-one shall have the ability to delete clinical information until the appropriate time period has expired.

6 Attribution: all access to clinical records shall be marked on the record with the subject's name, as well as date and time. An audit trail must also be kept of all deletions.

7 Information flow: Information derived from record A may be appended to recrod B if and only if B's access contro list is contained in A's.

8 Aggregation control: . . .

9 Trusted computing base: . . .

The following questions explore the BMA model:

(a) What is pretexting? Give an example of a pretexting attack on a medical organization.

(b) How did Anderson propose medical records be automated? Specifically address the issue of a single centralized record vs. a set of distributed records? How is this decision reflected in the principles?

(c) How did the aggregation of National Health Service data across multiple practices change the significance of the insider threat for inappropriate disclosure of information?

(d) How did the BMA model address this significant threat? How do the principles prevent my dentist's recptionist from reading my therapist's notes about my mental health?

(e) How does the Information Flow principle (7) relate to Bell LaPadula?

(f) Why did Anderson reject just adapting military style confidentiality to the health domain? What went wrong with having AIDS-like information secret, normal patient records confidential, and prescription information sensitive?

5. Information-flow security [20 points]

Consider the four 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
```

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

(b) Which flows are explicit (direct); which are implicit (indirect)?

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