CS 380S - 0x1A Great Papers in Computer Security
Fall 2012

Homework #3

Due: 2pm CST (in class), November 20, 2012

NO LATE SUBMISSIONS WILL BE ACCEPTED

YOUR NAME: ______________________________

Collaboration policy

No collaboration is permitted on this assignment. Any cheating (*e.g.*, submitting another person's work as your own, or permitting your work to be copied) will automatically result in a failing grade. The Computer Sciences department code of conduct can be found at `http://www.cs.utexas.edu/academics/conduct/`.

Homework #3 (30 points)

Problem 1

In this problem, we will use information flow to express privacy policies. Consider a customer relationship management (CRM) program. Some of its variables contain `private` values (*e.g.*, information about the customer's income); others contain `public` values (*e.g.*, customer's ID).

Problem 1a (3 points)

Give a snippet of pseudo-code that outputs only the values of `public` variables, yet leaks information about the value of some `private` variable.

Problem 1b (2 points)

Can you think of a way to use Jif type labels to prevent the leak in Problem 1a?

Problem 1c (3 points)

Give a snippet of pseudo-code that leaks some `private` information even if the Jif type system is used.

Problem 2 (3 points)

Write a program in pseudo-code that (i) will pass verification in the Myers-Liskov model for decentralized information flow control (as described in their SOSP 1997 paper), yet (ii) contains an information channel which leaks the value of some secret variable. Show the labels associated with variables at each point of your program.

Problem 3 (12 points)

In this problem, we consider authentication in distributed systems. Suppose Alice and Bob are logged into the same workstation. The workstation shares a secret symmetric key with a mail server that stores Alice's and Bob's email. Bob wants to retrieve his email from the server and read it on the workstation.

- Which principal speaks for Alice?

- How does Alice delegate her authority to this principal?

- Which principal speaks for Bob?

- Which principal submits the mail retrieval request to the mail server?

- Who does this principal speak for?

- How is authority delegated to this principal?

Problem 4 (4 points)

Consider extending the technique for detecting SQL injection vulnerabilities described in the PLDI 2007 paper by Wassermann and Su ("Sound and Precise Analysis of Web Applications for Injection Vulnerabilities") to detect cross-site scripting vulnerabilities.

What do you think would be the main difficulties?

Problem 5 (3 points)

Consider an e-commerce server that needs to protect customers' data even when running on an untrusted operating system. The server consists of two programs: NewUser and SellGoods. The NewUser program receives credit card numbers, addresses, etc. from users and stores this information in files. The SellGoods program allows users to purchase goods using previously stored credit cards.

Would you use Overshadow to protect such a server? Explain.