OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

SUMMER EXAMINATION 2014

CS4615: Computer Systems Security

Professor I. Gent,
Professor B. O'Sullivan,
Dr. S.N. Foley

Answer *all* questions
Maximum marks: 80

1.5 Hours
(Note 80 marks/90 minutes = 1.125 minutes per mark)

PLEASE DO NOT TURN THIS PAGE UNTIL INSTRUCTED TO DO SO

ENSURE THAT YOU HAVE THE CORRECT EXAM PAPER

1. a) Explain how a SYN-flood can result in a denial of service attack. *(6 marks)*

   b) Give an example of a C program that contains a stack smashing attack. Assuming that you have available a suitable input string that can generate this attack in your program, explain how it might be used to compromise a system. *(6 marks)*

   c) Alice includes the current directory "." in her shell path on the `cs1.ucc.ie` Unix server:

   ```
   PATH = .:/usr/local/bin:/usr/bin:/bin:/usr/X11R6/bin:/usr/lib/java/bin
   ```

   How might an attacker use this to compromise Alice's account? *(6 marks)*

   d) Give an example of an iptables firewall policy that contains a shadowing anomaly. Explain your answer. *(6 marks)*

   e) What is a *botnet*? Would a firewall prevent the operation of a botnet? Explain your answer. *(6 marks)*

   (30 Total marks)

---

2. When a client visits `http://stockbroker.com/SMgmt.jar`, a stock management application is downloaded and executes in the client's Java VM. This application uses (`RW` access) a local file `portfolio` on the client's workstation to store data on the client's stocks. The stockbroker provides a further Java application `Summary.jar` that returns stock summary detail based on the data it reads from the local client `portfolio` file.

   a) Write Java security policy rule(s) that permit the stockbroker's applications to have the necessary access to the portfolio file. *(5 marks)*

   b) A third party Java application `http://ragtag.com/Advice.jar` provides advice based on a stock portfolio summary. When executing in the client Java VM, it invokes `Summary.jar` (from stockbroker) and generates investment advice based on the summary data.

   Outline how the Java security manager can be used to ensure that this advice application may not have direct access to the `portfolio` file, but may still generate its advice by invoking `Summary.jar`. Your answer should include: a suitable Java security policy; an outline of how a new Java permission is declared and used by `Summary.jar`, and whether `Summary.jar` should be treated as a privileged operation. *(10 marks)*

   c) The stockbroker decides that it will no longer use mobile code and, instead, hosts client data and application execution on its own servers. `SMgmt` and `Summary` become network services to which clients and ragtag may direct their requests.

   Outline how a Trust Management system could be used to control client access to these services. You answer should include examples of suitable KeyNote credentials. *(10 marks)*

   (25 Total marks)

-I tcp -p 198.252.1.1 -j Dport 80 allow

3. The stockbroker in Question 2 moves to offer banking services in addition to stockbroking services. For simplicity, all client data records are managed in database table $R(id, client, data)$ whereby each record of (bank or stock) *data* has a unique identifier *id* (primary key). Strict separation (no information flow) between banking and stock data is required. A Chinese Wall policy is applied to banking and stockbroking divisions: an employee may only access banking data or stock data, but not both.

   a) Describe how multilevel security (MLS) can provide a high-degree of assurance for this system. Your answer should include a revised database table (with sample tuples), rules that govern table querying and insertion, and sample employee clearances. *(10 marks)*

   b) Give an example of a covert channel that permits a Trojan Horse to signal *two bits* of stock data to an employee in the banking division. Describe how the channel should be closed. *(5 marks)*

   c) A breach of the Chinese Wall/failure of the security mechanism in Question 3(a) would cost the stockbroker €500,000 in fines and loss of reputation. The stockbroker has a choice: either host both banking and stocks services on a single high-assurance MLS system (costing €5,000) following the design in Part (a), or host stocks on one conventional server and and banking on a separate conventional server (each costing €250). The probability of such an attack on the conventional systems configuration is 0.01; this is reduced to 0.001 if the MLS configuration is used instead. Use this information to carry out a *Risk Assessment* and advise the stockbroker on the best option.

   Suppose that insurance could be purchased for €500 per annum (regardless of system) that covered €200,000 in the event of a security failure. How would you revise your advice? *(10 marks)*

(25 Total marks)

PLEASE DO NOT TURN THIS PAGE UNTIL INSTRUCTED TO DO SO

THEN ENSURE THAT YOU HAVE THE CORRECT EXAM PAPER