UNIVERSITY OF LONDON

BSc EXAMINATION 2017

For Internal Students of
Royal Holloway

DO NOT TURN OVER UNTIL TOLD TO BEGIN

IY2840: Computer and Network Security

Time Allowed: **TWO hours**

Answer ALL questions
Calculators are not permitted

1. In 1946 von Neumann published a new architecture for computer design.

   (a) What was novel about the von Neumann architecture? Explain why this was helpful to programmers, and explain why this also introduced security problems. [6 marks]

   (b) What vulnerability in modern systems, often exploited by hackers, is a consequence of the above? [2 marks]

   (c) What mechanism did the IBM 360 computer and OS/360 introduce to mitigate this problem, and how is this mechanism used in modern CPUs such as the Intel x86? [6 marks]

   (d) To formalise the security requirements that emerged during the early development of computer systems, Anderson proposed the concept of a Reference Monitor. Describe 3 properties that a reference monitor must have. [6 marks]

   (e) Disruptive technologies, such as von Neumann, often give rise to security problems. Give one example of what you consider to be a modern disruptive technology.

   Are there any security issues with this technology? Explain your answer. [5 marks]

2. The Reference Monitor is an abstract idea that is used to model access control based on Principals, Subjects, and Objects.

   (a) State three places in a computer system where you might find a Reference Monitor, and give an example of each. [6 marks]

   (b) In Unix what are the Principals, Subjects, and Objects? [6 marks]

   (c) Johnny Hacker gains user level access to an old Unix system. He notices that there are no salts used with the passwords and is pleased to see this. How does 'salting' passwords work? Explain 2 benefits of this. [6 marks]

   (d) Johnny now wishes to elevate his privileges. He notices that the host is running `/usr/lib/preserve` to make backups if the `vi` editor crashes.

   He knows that this program runs as SUID root, and he knows that this program, in the event of a crash, will send an email to the user by making a `system()` call to `/bin/mail`.

      i. What environment variable could Johnny change in order to get the system call to run his own program, and what would he change it to? [2 marks]

      ii. Explain why doing this would get the `system()` call to run the attacker's program? [4 marks]

      iii. What will the Effective UID of the attacker's program have when run? Explain why this is the case. [3 marks]

3. Johnny Hacker has gained root access to an old Unix system. He now wishes to access other systems on the network and thinks about poisoning the local name server's DNS cache.

   (a) To do this, Johnny needs to understand how DNS works. Explain the steps involved when a client uses DNS to find the IP address of a particular domain. You may use a diagram if this helps. [10 marks]

   (b) How does a DNS resolver authenticate replies from authoritative name servers, and how does this help Johnny with his attack? [4 marks]

   (c) Assuming the local name server has a short TTL for local cache entries, how might Johnny poison its DNS cache to set the IP address of a local server to one of his choosing? [12 marks]

4. HTTP is a stateless protocol. But sometimes Web Applications need to maintain state.

   (a) List 3 reasons why some Web Applications might need state information. [3 marks]

   (b) Cookies are often used to store state information. Explain how the cookie mechanism works, and what policies are used to secure access to cookies. [6 marks]

   (c) Session cookies are used to maintain state.

      i. Explain how session cookies and session IDs are used by client and server to maintain state. [6 marks]

      ii. An attacker may try to steal or modify a session cookie.
      Briefly describe 3 things that could be done with the cookie to defeat such an attack. [3 marks]

   (d) Johnny Hacker is trying to gain access to a web server. He knows it is running a SQL database.
   What SQL queries could Johnny try to get the SQL server to run in order to identify the table names in the database, and the column names in the tables? Give an example of each. [4 marks]

END