No calculator permitted

UNIVERSITY OF BIRMINGHAM

School of Computer Science

MSc Cyber Security

06 28214

Designing Secure Systems

Summer May/June Examinations 2017

Time allowed: 1 hour 30 minutes

[Answer ALL Questions]

1. Defence in depth.

(a) Explain what is meant by defence in depth. [6%]

A bank allows customers to login to the bank website using their username and password. The bank’s objective is to prevent unauthorised logins. A security consultant advises the bank to introduce additional security mechanisms in order to achieve this objective with greater defence in depth. Which of the following measures introduce defence in depth, and which do not? Explain your answers.

(b) Customers will be required to pre-register a telephone number. When the customer tries to log into the bank and types their user name and password into the browser, an automated service will call the number and announce an access code. To gain access, the customer is required to type the access code into the browser. [7%]

(c) Instead of asking the customer to type their password on the computer keyboard, a "soft" keyboard will be displayed with the keys in random order. Customers will have to click on the keys corresponding to their password. The idea is to try to defeat keyboard loggers and mouse event loggers.

[7%]

(d) The bank will introduce certificate transparency, to provide better authentication of the bank to web browsers. Customers using web browsers that don't support certificate transparency will not be able to use internet banking. [7%]

(e) The bank will blacklist certain IP ranges. Attempts to login from IP addresses in those ranges will be denied. [7%]

2. Cloud computing.

(a) Explain the terms "confidentiality" and "availability" as applied to data security. [9%]

(b) Explain the difference between following two of the top twelve cloud computing issues (2016) identified by the Cloud Security Alliance (CSA):

1. data breaches
8. data loss

The numbers 1 and 8 are the numbers given by the CSA. [9%]

"Confidentiality from the cloud provider" is a design goal in cloud computing. It means that the cloud should not be able to derive any information about the data being processed. Suppose you have commissioned a cloud service which, through means of encryption and obfuscation of data requests, guarantees confidentiality from the cloud provider.

(c) Explain whether such a service addresses the issues of data loss and data breaches. [8%]

Suppose your cloud computing application requires strong assurances of data availability.

(d) Briefly explain a design approach that would be appropriate. [8%]

3. Certificate transparency.

(a) Explain what is "certificate transparency". [6%]

Which of the following problems does certificate transparency address? Explain your answers.

(b) A rogue employee of a certificate authority is bribed by criminals and issues fraudulent certificates for a bank website to them. [7%]

(c) Due to a fault on the bank's website, users are directed to a login page which does not use TLS. [7%]

(d) When Alice logs into her bank account, she ignores warnings about the certificate (for example, warnings about its validity dates). [7%]

A startup company is developing a new end-to-end encrypted person-to-person messaging mobile phone app. They decide to use certificate transparency to authenticate users' public keys. As their implementation is not required to interoperate with any other, the programmer suggests to use hash chains as the basic data structure in the log, rather than Merkle trees.

(e) Explain why this suggestion by the programmer is likely to cause problems. [7%]