UNIVERSITY OF DUBLIN

4D4

TRINITY COLLEGE

Faculty of Engineering and Systems Sciences

Department of Computer Science

Senior Sophister Engineering **Hilary Term 2005**

CAD and Security 4D4

Friday May ??, 2006 **some location** **09.30–12.30**

Stephen Farrell

Attempt five questions, at least two from each section.

All questions carry equal marks (20)

Log tables are available from the invigilators, if required.

Non-programmable calculators are permitted for this examination—please indicate the make and model of your calculator on each answer book used.

You may not start this examination until you are instructed to do so by the Invigilator.

5. You are a developer working for a software product development company. They are starting work on a major new release of their main product which has been on sale for a number of years. The product is for running web-based communities, somewhat along the lines of flickr, i.e. the user's of the product are the administrators of such community sites. You are tasked with looking after security for this new release. (Note: for the purposes of this question, describing how you would carry out the security analysis matters much more than a description of the product.)

(a) Describe how you would approach analysing the existing security and privacy aspects of the product. (10)

(b) Name and briefly explain 3 significant vulnerabilities which would be likely to be present in recent versions of the product. Explain the countermeasures you would select to handle these. (10)

6. *(a)* What is the purpose of a public key infrastructure (PKI)? In other words, what security requirements does a PKI aim to meet? (5)

(b) Describe how the XML Key Management System (XKMS) supports the requirements you identified in part (a). (5)

(c) What are some of the advantages and/or disadvantages of using XKMS over a "pure" X.509 based PKI? (5)

(d) Give an example of when you might choose to use an XKMS bsaed PKI and say why. (5)

7. *(a)* Describe a practical key management scheme (e.g. the SSL/TLS handshake or Kerberos or S/MIME), noting the advantages/pitfalls of your chosen scheme. (10)

(b) Describe some of the issues that might arise when configuring clients or servers for your chosen scheme. (5)

(c) How might mis-configuration might cause security problems for this scheme? (5)

8. In the expectation that broadband bandwidth will increase sufficiently in the coming years, you decide to develop a startup company to support viewing movies over the Internet. Your initial target is to develop a system that supports near-video-on-demand, where some minutes may elapse between the time a movie is ordered and when the movie is ready for viewing (i.e. has been downloaded). Clearly, payments processing, security, privacy and rights management are important aspects of this system.

(a) Provide an overview of the system (including. e.g. a network diagram) focusing on the security components. (5)

(b) What do you consider to be the 3 most important vulnerabilities (in terms of probability of occurrence and impact) for this system, as described in the answer to part(a)? Specify a countermeasure aimed at each. (5)

(c) Assuming that the countermeasures you mentioned in part(b) are implemented, briefly describe the main operational security policies which the system adminstrators ought to follow, for example, if you included auditing as a countermeasure above, say how the audit trails/logs should be processed. (5)

(d) Given all of the above, how might an attacker still successfully abuse your system? (5)