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 18, 2005 **Arts Building A3074** **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. *(a)* Explain how you would approach analysing the security of systems? State how you would analyse vulnerabilities, select corresponding countermeasures, and (given that there is always limited time available to do security analysis), explain the criteria you would use in order to decide where to expend your analysis effort. (10)

(b) Name and briefly explain 3 significant vulnerabilities and corresponding countermeasures which commonly occur in real systems today. (5)

(c) Deploying a security countermeasure can introduce new vulnerabilities. Describe a realistic scenario in which a countermeasure causes a new vulnerability which is actually worse than the vulnerability that motivated deployment of the countermeasure. (5)

6. *(a)* Briefly explain each of the three main security properties which are desirable for hash functions.(5)

(b) State three examples of how hash functions are used in security protocols. (5)

(c) What are the effects of the recently discovered weaknesses in hash functions? (5)

(d) In a case where a hash algorithnm with a known weakness has to be used (e.g. for legacy support reasons) describe a way to mitigate those weaknesses. (5)

7. *(a)* Describe the workings of 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) How do scaling issues affect your chosen protocol in terms of the numbers of each of the folowing: clients, servers and "domains." For S/MIME or TLS a "domain" can be considered to be a given CA's public key infrastructure. For kerberos a "domain" is a kerberos realm (or a single KDC). (10)

8. You are a system designer who has been tasked to design a web-based insurance quotation system. The main functionality of the system is to allow users on the Internet to enter their details on a set of web forms, and to then get a number of quotations for insurance from a set of different insurance companies. If the user wishes to accept one of the quotations, then the system allows them to purchase the policy. The system is to be operated by a new company which will be owned by the set of insurance companies who are participating in the system, but this company has to be operated as a separate entity for regulatory reasons. The quotation engines (the sotware which maps from user information to an actual quote) are run on systems inside each insurance company. This is done to protect proprietary company information and also to allow each compamy the flexibility to tailor quotes, e.g. by making "special offers". Initially the system will only handle car insurance, but it may be extended later on to include home and health insurance (you need to decide the extent to which you include support for these potential extensions).

(a) Provide an overview of the system (including. e.g. a network diagram). (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) After the system has been operating for some time, a new insurance company enter this market, but do not take part in the web-based quotation system. This new insurance company hire some bad-guys to try to reduce the amount of buisness being done via our system. Describe how those bad-guys might attack the system. (5)