UNIVERSITY OF DUBLIN

TRINITY COLLEGE

FACULTY OF ENGINEERING, MATHEMATICS & SCIENCES

SCHOOL OF COMPUTER SCIENCE & STATISTICS

MSc in Computer Science Hilary Term 2013
CS7053

Security of Networks and Distributed Systems

EXAM SOLUTIONS

Date	**Location**	**Time**
XX April 2012	**XXXX**	**XX**

Dr. Stephen Farrell

Instructions to Candidates

Please attempt 3 questions.
All questions carry equal marks.

EXAM SOLUTIONS

EXAM SOLUTIONS

Question text is in italics below.
Answer outlines are like this.

Question 1. (33 marks)

A games company are planning to migrate their previously off-line single-person game to an on-line multi-player game, with the usual multi-player features (messaging, trading game items, player to player battles, non-player characters etc.). The company are planning to have game servers located in various data centres (co-location sites) around the world to provide lower latency access for their users. The game software has been developed and tested and the new version will be released soon, and the company have done internal work on security. As on-line multi-player gaming is new to this company they have hired you, as a security consultant, to help evaluate the security of their new game release and platform.

a) Describe the most relevant risks (at least 3) you see, including consideration of their impact and likelihood of occurrence, and outline the countermeasures you would expect that the company have implmented to mitigate those risks. (18 marks)

The student should take proper account of the context – gaming, a s/w dev company and the operational environment etc. The main point is to describe a reasonable set of threats and a review process that approximates what might really be used.

The main thing here is to describe risks with their impact and an estimate of probability of occurrence and to concentrate on the more significant of those. The impact and probability can be take any value without losing marks, but for something odd (e.g. if they considered DoS low impact) they will need more justification for saying that. If the impact/probability are fairly obviously right, less needs to be said. Marking is out of 3 points for each good one and with 3 more for overall goodness. Possible risks would include:

- Denial-of-Service attacks on the site
- Loss of logs and tracking information (accidental or not) needed because of the medical device aspect
- Leaking of customer personally identifying data especially medical or payment information
- Hackers breaking in to or defacing the site
- Abuse of customer support blogs, forums etc. for malware distribution or C&C
- Hosting site staff or other tenants abusing the web infrastructure from within
- Cloud-providers monitoring site traffic and data for their own benefit or for the benefit of competitors or foreign governments
- Staff from out-sourced providers (e.g. payments processors, customer service) hacking into the system
- Customer service staff working for competitors
- Manufacturers staff faking orders and hiding that

- Payment processors not reporting all payments, possible micropayments
- gamers cheating on one another or grouping together to cheat in the game
- whether or not goldmining is allowed, encouraged etc.
- etc. etc.

b) What questions would you ask about the company's internal development processes and the operational processes of the hosting data centres? (10 marks)

Marking is 5 for development stuff, 5 for OPS stuff. Should ask about processes incl., code reviews, tiger team testing, alpha/beta releases, what logs are generated, how those are analysed etc.

c) After you've finished this contract, another similar, competing company hires you to do a very similar piece of work. How might you expose confidential information related to the first company in carrying out this second contract? Describe steps you would take to avoid exposing such confidential information. (7 marks)

Marking is straight from 7 – key thing is to realise that there is confidential information, e.g. Locations, details of threats not well-mitigated, but also design choices made by the 1st company. Steps to avoid that would include, not keeping materials, if some are kept, to ensure that you don't cut'n'paste text etc. Asking the 1st company what they're happy with being re-used is good.

Question 2. (33 marks)

(a) For any real Internet key exchange protocol (e.g. TLS, S/MIME, IPsec, Kerberos) describe the key management and application data protection aspects of the protocol in detail, including a description of the impact of the exposure of relevant secret or private keys. (15)

Marks-from-10 for a good description of the scheme, with e.g. the TLS handshake and application layer properly described. 5 marks for properly describing a real use case such as IMAP/TLS. Key exposure part should e.g., cover that TLS with RSA ciphersuites doesn't offer perfect forward secrecy etc and how one might recover from server key compomise. Better marks if they conside CA key compromise or Kerberos TGT encrypting key compromise.

(b) What are the main issues that arise with very large scale deployments of your chosen protocol ? (10)

Assuming they choose TLS:

- Load balancing and how to handle that
- Provisioning of keys and servers and interacting with the public PKI.

- Dealing with all the various browsers
- Dealing with old protocol versions of TLS
- Dealing with high levels of traffic and bursty traffic

(c) Describe any side-channel (e.g. timing, power) attacks might be attempted against a naïve implementation of your chosen protocol? (8)

Timing attacks and side-channels like Bleichenbacher based on formatting and oracles are what's called for here. Straight marks from 8 for this. Extra bonus if someone knows about cache-misses.

Question 3. (33 marks)

You are asked to (re-)design a national application system for students to use when applying for third-level grants. The system should allow the applicants (and/or their parents or guardians) to enter contact, educational and financial information relating to family income, and to track the process of their grant application. Staff are responsible for validating the information entered against exam results, university applications and tax systems and for approving or denying applications. Payments for successful applicants are to be transferred to the correct bank accounts in a timely fashion. Auditors are special users who can randomly check the processing of applications and who also produce anonymised statistics as to the operation of the system. There are also system administration users who have privileges to manage the system but who should not have access to personal information about applicants. The system is expecteed to handle high peak loads and is considered likely to be attacked.

(a) Outline the overall design for such a system (include a network diagram) and describe the security requirements you would propose the system must meet (10).

> This should be a fairly straightforward web-like distributed system with user registration, access controls for staff etc. Protection of personal information is the stand-out requirement. Marks from 6 for the description and out of 4 for a good diagram that explains stuff well.

(b) Describe, in detail, the security solution you would propose to meet those requirements. (15)

> This needs to cover authentication; access control for staff and with all links over some form of protected tunnel (TLS). Audit should be mentioned. The registration subsystem would probably be web-based and there would need to be some sysadmins who can set that up. The solution should cover strong protection of personal information and secure links to external systems (e.g. Banking, tax). Marks from 5 for each of authentication and authorization description and 5 for overall goodness.

(c) Having designed the system, you are then fired and decide to launch a denial-of-service attack that prevents the system working, but so that you could not be traced as the bad-actor. How would you go about doing this? (8 marks)

> Straight marks from 8 for sneakiness.

Question 4. (33 marks)

a) Describe the concept of a de-militarized zone (DMZ) and how that is used in typical enterprise networks. Desribe three security technologies that one can reasonably place in a DMZ? For each, describe some threats that that technology mitigates and how that is achieved. (18 marks)

> *Pick from firewalls, IDSes, anti-spam filters, split-DNS, TLS accelerators, application servers (with DB on internal n/w). Threats for these are fairly obvious, e.g. Firewalls (if configured properly) can ensure only DMZ hosts that are expected to listen for incoming traffic are allowed to see that traffic; split-DNS ensures that internal hosts and other DNS entries aren't visible to the Internet; TLS accelerators can provide higher assurance storage and handling of server private keys even whilst running in the DMZ. (5 marks for each technology, plus 3 for overall goodness)*

b) Describe a realistic network that uses the technogies, described in part A and say what kinds of penetration testing you would attempt in order to determine if the network is sufficiently secure. (The meaning of "sufficiently secure" will depend on the kind of network you describe.) (10 marks)

> *Main idea is that the student picks some sensible n/w and commenmsurate level of penetration testing and a reasonable set of tools for that e.g., metasploit. 4 for describing the n/w and 6 for desribing the testing.*

c) Describe common mis-configurations of one of the technologies that you described in part A and the kinds of expoit that such mis-configuration enables. (7 marks)

> *Straight marks from 7. Firewall mis-config is the most common thing here, where e.g., old settings remain after they're no longer needed, un-patched servers in the DMZ would be too obvious.*