UNIVERSITY OF DUBLIN

TRINITY COLLEGE

FACULTY OF ENGINEERING, MATHEMATICS & SCIENCES

SCHOOL OF COMPUTER SCIENCE & STATISTICS

MSc in Computer Science Hilary Term **2016**

CS7053

Security of Networks and Distributed Systems

CS7053-1

Date	**Location**	**Time**
TBD	**TBD**	**TBD**

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 well-established mainstreet department-store are setting up a new web site to sell their usual array of physical goods (clothes, household goods, electronics) and a limted set of digital goods. There are some thousands of products in their overall catalog sourced from a number (about 100) of Irish and foreign manufacturers, which change from time to time. The set of products changes frequently, while the set of suppliers changes more slowly. As they are very concerned with both their real-world and online reputation, the company want to follow best security and privacy practices for all of their web site development and operations, online and telephone support, onine marketing, billing and payments functions. They would also like to out-source as many of these functions as possible, for example, using a company such as Paypal or similar for payment processing.The company don't however have internal secuirty or privacy expertise and ask you to consult with them to ensure that they end up with a sufficiently secure web site.

Answer outlines are like this.

a) Describe the most relevant risks (at least 3) you see for the new system, including consideration of their impact and likelihood of occurrence, and outline the countermeasures you would expect that the company and/or their chosen service provider s (who provide out-sourced functions) would need to impelment to mitigate those risks. (18 marks)

The student should take proper account of the context – a department store, many suppliers and 3rd party cloudy out-sourced serviecs. The main point is to describe a reasonable set of threats and mitigations 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 date leakage 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 5 points for each good one and with 3 more for overall goodness. Possible risks would include:

- Top requirements is availability, e.g. DdoS resilience
- They need out-sourcers to do as well or better at security and privacy
- Hackers breaking in to or defacing their site or outsourcer sites

- 3rd party staff or other tenants abusing the infrastructure from within
- Sales or customer service staff working for competitors
- etc. etc.

b) What other questions would you suggest the company ask about the out-sourced service provider's systems and operational processes? (10 marks)

As above basically in terms of marking scheme. This could be more or less focused on security, which is fine, OPS issues are good to ask about too. Possible questions could include:

- Describe your operations security model
- Have you done tiger-team testing
- Describe your risk analysis model
- What SLAs (five-9's etc) do you offer
- What other tennants use this and how to you separate them/us
- How do you report security issues found to your customers (i.e. us)
- etc etc

c) What functions would you recommend that the company should not out-source and why? (5 marks)

A fine answer is “none,” if justified, e.g. by arguing that all of the service providers are specialised and hence are going to be better at their job than the site owner. Another would be to argue that since they need to be able to replace service providers, the site owner actually needs to do their own web site operations.

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. How would you test a library implementation of the protocol before using it in some appllication. (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 how one might test the library e.g. fuzzing as well as nominal operation, performance, and for known side-channels timing etc.

(b) What are the main barriers to deployment that are likely to be experienced with applications using your chosen protocol? (8)

So much from which to choose! :-(2 marks for each good point made + 2 for overall goodness (expecting 3-4 different points), possibles:

- admin/opex costs
- ignorance
- lack of browser hardfail
- http -> https content transitions hard sometimes
- CPU (not really)
- middleboxes
- ...

(c) Desribe some known attacks that have been seen with implementations of your chosen protocol and briefly outline their actual significance on the Internet. (10)

A couple or three are sufficient, depending on the level of detail. Fewer marks for just naming attacks, more for saying why they are interesting.

Attacks (on TLS): Bad PRNG, Bleichenbacher, etc a reasonable list is at https://en.wikipedia.org/wiki/Transport_Layer_Security#Attacks_against_TLS.2FSSL

Question 3. (33 marks)

You work for a large multinational corporation in the software business that has operations in about 40 countries. You are asked to design a system for internal whistleblowers (or "reporters") to report misbehaviour. The system should allow employees and contractors to enter new reports without being identified. Only a special team (the "ombudsman" team) should be able to read and process reports and associated information. Processing reports will require annotating content and possibly adding additional information as incidents are investigated by the ombudsman team. There should be some way in which the ombudsman can attempt to contact reporters, if (and only if) the reporter has opted-in to being contactable. While the typical report is expected to be about pesonnel matters (e.g. manager X is treating person Y badly, or person W is harassing person Z), it is also possible (though far less likely) that much more sensitive reports could be entered (e.g. our company has spent millions of Euros on bribes in the last decade). Note that the company has many personnel (e.g. devlop staff) who are capable of, but unlikely to, attack a system that has any obvious or documented weakness. Your goal in designing the system is to balance usabllity and the cost of developing and operating the system against the level of confidence that reporters can have that they will not be identified if they use the system and their confidence that reports will result in real and fair investigations and subsequent action.

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

> This should be a fairly straightforward web-like distributed system. But they need to pay attention to confidentiality that is robust against significant insider attack.

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

> Given a good set of requirements (marking will be lenient in terms of allocating marks to this part for text in the answer to (a)) this is pretty straightforward too, basically use good mechanisms for confid. Maybe outsource parts. Audit should be part of the solution too though. And ideally (extra marks) some way of demonstrating accountability without exposing reporter information (easliy done if reporter works in a small office).

c) Describe a non-obvious way in which an employee or contractor might use the system to their benefit. (8)

> Obvious is easy here (diss a colleague) but gets fewer marks, maybe 3. Non-obvious is better. An example might be to work for a competitor by (arranging the) filing of

reports that will damage the competing product/service. That'd be medium. If one can breach the confid of the system them one might find someone one can blackmail, not for cash, but for promotion or other in-company favours, and even perhaps with the latter not enabling identification of the attacker (e.g. “unless you close group-X and enlarge group-Y, I'll leak that you reported on the CEO to the ombudsman”).

Question 4. (33 marks)

a) Describe the architecture and key management hierarchy of DNSSEC. (15)

5 for arch; 5 for key hierarchy and 5 for overall goodness. This is a straightforward “do they know it” part of the question; they should cover all the basics as taught in class

b) Describe issues that can make DNSSEC harder to deploy, compared to DKIM?

- DS from child to parent issue
- Registrars, registries, and registrants all need to do stuff and often don't have GUIs for that – all entities need to support before benefits start to be seen
- DNS resolvers (e.g. in ISPs/access-points) might not support DNSSEC Rrs
- DKIM signers can just fire ahead (but do need write access to DNS)
- DKIM doesn't hard-fail (DNSSEC does) but is still useful
- DKIM doesn't break as easily “h=” and c14n allows for some expected mods to email
- ...

c) Describe ways in which the DNS can leak private information and how one might mitigate that with changes to DNS protocols, implementations and deployments. (10)

They should note that DNS data being public is not the same as the act of accessing to that data being public. 3 for covering lack of confid; 3 for covering QNAME minimisation; 4 for overall goodness; -1 if they mix up DNSSEC with this. Bonus is they get the diff between stub and recursive resolver and authoritative server and how that that affects all this and/or things like Google's public DNS servers hoovering up access info.