Paper Code

Coláiste na Tríonóide, Baile Átha Cliath
Trinity College Dublin
Ollscoil Átha Cliath | The University of Dublin

Faculty of Engineering, Mathematics and Science

School of Computer Science & Statistics

MSc in Computer Science **Hilary Term 2017**
Year 1

Security of Networks and Distributed Systems
CS7053/CS7453/CS7074

20 April 2017 LOCATION **09.30 – 11.30**

Dr. Stephen Farrell

Question text is in italics below.

`Answer outlines are like this.`

Instructions to Candidates:

Attempt **three** questions. All questions carry equal marks.

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

Materials Permitted for this examination:

N/A

Question 1.

A small Irish company are just setting up as a distributor for a range of imported electronics goods that will be sold online. To do this they need to set up a web site as cost effectively as possible, for example through the use of open-source technologies and out-sourcing. The company have no specialist security or networking expertise. The company do however realise that a significant breach of their web platform could put them out of business, so before making any significant technology decisions, they hire you to advise them on what security and privacy risks to consider and what countermeasures to deploy to mitigate those risks.

(a) Describe the risk analysis process you would follow in order to assist the company. [10 marks]

The student should describe a method of identifying risks, classifying them in terms of impact and probability of occurrence, e.g. with High/Medium/Low scores for each, and assigning an overall (partial) order to the list. One then iterates, designing a mitigation for the most imporant item on the list, and then re-doing the analysis as necessary (since one mitigation may affect the probability of other risks or may introduce other risks). In practive, the process terminates when the available effort is expended. In theory some other form of termination might be described. Any answer that captures most of this is fine.

(b) Describe the most relevant risks (at least 3) you see for the new system, considering their potential impact and likelihood of occurrence, and outline the countermeasures you would recommend that the company and/or their chosen service providers (who provide out-sourced functions) ought implement to mitigate those risks. [25 marks]

The student should take proper account of the context – an online store, many suppliers and 3rd party cloudy out-sourced services. 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 data 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 risk is leak of the customer database

Also needed: 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.

(c) Assume the company had instead gone ahead and designed the system without having done any risk analysis, describe some mistakes they would be likely to have made? [5 marks]

They might have a username/pwd DB with crappy salting, or breach PCI requirements, or have SQL injection vulns, or XSS, or non-updated technology (e.g. outdated Wordpress blog).

Question 2.

(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 the security of a deployed application that uses that protocol? [20 marks]

Marks-from-15 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 do the test e.g. testing with bad-certs, fuzzing, use of standard hacking tools etc.

(b) What are the main barriers to upgrading your chosen protocol? For example, if your chosen protocol is TLS, you might describe barriers to deployment of TLS1.3. [10 marks]

Generally the issues are slow updates of s/w, middleboxes (e.g. TLS accelerators, snooping devices) and similar. Lack of update of other infrastructure can be an issue (e.g. RSA-PSS not in h/w, CA’s not updating to handle new cert extensions, ...)

(c) Describe two or three known attacks on implementations of your chosen protocol and briefly outline their significance on the Internet. [10 marks]

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.

Human rights defenders and other Non-Governmental Organisations (NGOs) in various parts of the world face many challenges, often from authorities in their own countries, whether those authorities are the de-facto government or a terrorist organisation or a set of "freedom-fighters." Technology can help NGO employees, especially in terms of information access and sharing at home and abroad, but can also provide their adversaries with opportunities to track and spy on individuals and on the organisation as a whole. Some NGOs are well-resourced but many are not and need to minimise costs and complexity. You are tasked with designing a system to be replicated in different NGOs worldwide to allow employees to communicate with their colleagues, and with chosen non-employees, in as secure and privacy-friendly a manner as possible. Bear in mind that NGO employees will tend to be local activists and cannot be expected to have much computer or networking training, though they can be trained to use the system you design.

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

This should be a fairly straightforward interpersonal messaging system, could be email or IM e.g. Telegram/signal-like. But they need to pay attention to confidentiality that is robust against significantly resourced attack. One non-obvious and hard-to-meet requirement they should note is to not leave traces that the staffer is even using the system.

(b) Describe, in detail, the security solution you would propose to meet those requirements. [20 marks]

Say it's email, then SMTP/STARTLS everywhere, with PGP or S/MIME etc. Probably needs message-in-message encapsulation to be really ok. Not clear what cover traffic might work. Likely better if IM based (OTR/Signal/whatever) running on e.g. Tor sometimes and HTTPS or XMPP/TLS all the time. It's ok for the students to describe their solution as if those technologies (e.g. signal) didn't exist and the student is just inventing 'em as we didn't cover the detail of these protocols in class. But the concepts should be there, confid, origin auth, some level of deniability, cover traffic.

(c) Describe a non-obvious way in which an adversary might attempt to breach the system to their benefit. [10 marks]

Traffic analysis (TA) of various forms, compromise source code of applications or OS modules to directly leak or to make TA easier, forcing traffic to clear (like SSLstrip), bribing staff or system designers. Etc. Etc. Sneakier is better here.

Question 4.

(a) Describe the architecture and key management hierarchy of DNSSEC. [20 marks]

8 for arch; 8 for key hierarchy and 4 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) Why is DNSSEC hard to deploy? Suggest some changes that would make DNSSEC easier to deploy. [10 marks]

- 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
- Applications don’t see benefits they can measure

Improvements:

- Automation of DS handling
- Better OSS tools for registrars/registries
- Other improvements aren’t easy, e.g. some opportunistic mode, if they get more then maybe bonus points

(c) Give some examples of how the DNS leaks private information? How can we mitigate that via changes to policies, protocols, implementations and deployments? [10 marks]

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.