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 2018**
Year 1

Security of Networks and Distributed Systems
CS7053/CS4474/...

XX April 2018 LOCATION **09.30 – 11.30**

Dr. Stephen Farrell

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.

An Irish medium-sized manufacturing company has about 1000 employees, a small number of overseas offices and some dozens of frequently travelling employees. The company want to replace their existing in-house email infrastructure and are considering how to do that, including deciding what to continue to host themselves and what to outsource. They ask you, as a security consultant, to do a risk analysis for them, considering the security and privacy implications of a new email system and of migration from the old to a new system.

The new system may involve updates for all email components: standard desktop, mobile and web user agents, mail submission servers, inbound and outbound mail transfer agents, message stores and security components such as anti-spam and anti-malware systems. Existing accounts and message store content will need to be migrated to the new system as that is incrementally deployed. A very small number of employees use PGP (mainly sysadmins) but most users do not use of PGP or S/MIME. Some users currently use third-party email systems, (such as gmail/hotmail), for work email, as there is no policy in place about the use of such third-party systems.

(a) Describe the risk analysis process you would follow in order to assist the company. (Note – this part of the answer is about *process*, not the details of technical mechanisms for email security.)

[10 marks]

(b) Describe the most relevant risks (at least 3) you see for the new system, including 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 to implement to mitigate those risks. Risks that could emerge during migration from the old to the new system are in scope here.

[25 marks]

(c) Assume the company had instead gone ahead and deployed a new system without having done any risk analysis. Describe some mistakes, not covered in part (b), that they might have made?

[5 marks]

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. Include a description of how networking failures, (e.g. packet drops, re-ordering), might affect use of your chosen protocol.

Your answer may describe any widely used version of your chosen protocol, but you need to state which version you are describing. Choosing TLSv1.3 is allowed – you don't need to specify the exact Internet-draft version you've chosen in that case.

[20 marks]

(b) Outline the ways in which the security of your chosen protocol depends on other infrastructure such as the Internet routing system, the domain name system or a key management infrastructure.

[10 marks]

(c) State-level adversaries have different capabilities and interests when compared to potential industrial or commercial adversaries. Describe three ways in which the threat-model for an implementation or deployment of your chosen protocol would differ, when considering state-level versus industrial or commercial adversaries.

[10 marks]

Question 3.

TCD decide to plan for the increasingly common situation where the campus must temporarily close due to a “red” weather alert. The overall plan is to be able to switch into a “remote-access” mode of operation where administrators, academic staff and students can still do some work, even if they cannot operate entirely normally. In “remote-access” mode, (some) lectures will continue via the Internet, and coursework assignments can be set, completed and marked. Clearly, real-time exceptions will need to be handled, e.g., due to network problems. More fundamentally, new timetables/schedules and modes for student/staff interaction will be needed to handle lecture timetabling and assignments without over-burdening staff and students who will at the same time be dealing with the physical disruption caused by the inclement weather.

The university are at the early planning stages for this system, and ask you to provide a design for a prototype system to be trialled in the School of Computer Science and Statistics. The prototype system will be tested via a planned exercise that will only be announced a few days ahead of time. That is, students, academic and support staff, will only have 2-3 days notice that they are to switch into “remote-access” mode for one week, that they must not attend campus during that week (relevant buildings will be locked), and that they need to use the new system to do as much “normal” work as possible. Before the exercise, students will not have used the system before, but they will have undergone some training and HOWTOs and other guides will be available online. You can assume staff have had more training but are still quite unfamiliar with the system.

(a) Outline your overall design for such a system (include a network diagram and describe how scheduling is handled), and state the security and privacy requirements the system must meet.

[15 marks]

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

[20 marks]

(c) How would you handle evaluating the security and privacy aspects of the system, before, during and after the planned exercise?

[5 marks]

Question 4.

(a) Describe three significant security and privacy differences between real-world end-to-end and hop-by-hop security mechanisms as used for interpersonal messaging, in email and/or instant messaging systems.

[15 marks]

(b) Describe three significant barriers to the deployment of Internet-scale end-to-end email security mechanisms such as S/MIME or PGP. In each case, describe realistic actions you would recommend that aim to at least partially overcome those barriers.

[15 marks]

(c) If end-to-end email confidentiality became the norm, so that most email messages were encrypted between sender and recipient(s), what problems would that cause for email system administrators, and how would you recommend they address those issues?

[10 marks]