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

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]

(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 to implement to mitigate those risks. [25 marks]

(c) Assume the company had instead gone ahead and designed the system without having done any risk analysis. Describe some mistakes (not covered in part b) they would be likely to 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. How would you test the security of a deployed application that uses that protocol? [20 marks]

(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]

(c) Describe two or three known attacks on implementations of your chosen protocol with an emphasis on explaining their significance for the Internet. [10 marks]

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]

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

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

Question 4.

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

(b) Why is DNSSEC hard to deploy? Suggest some changes to the protocol or overall DNS ecosystem that would make DNSSEC easier to deploy. [10 marks]

(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]