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 2016**
Year 1

Security of Networks and Distributed Systems

CS7053/CS7453

21 April 2016 Goldsmith Hall **09.30 – 11.30**

Dr. Stephen Farrell

Instructions to Candidates:

Attempt **three** questions. All questions carry 33 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 well-established main street department-store are setting up a new web site to sell their usual array of physical goods (clothes, household goods, electronics) and a limited set of digital goods. There are some thousands of products in their overall catalogue 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 their web site development and operations, online and telephone support, online 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 security or privacy expertise and ask you to consult with them to ensure that they end up with a sufficiently secure web site.

(a) Describe the most relevant risks (at least 3) you see for the new system, considering their impact and likelihood of occurrence, and outline the countermeasures you would expect that the company and/or their chosen service providers (who provide out-sourced functions) ought implement to mitigate those risks. [18 marks]

(b) What questions should the company ask the out-sourced service providers about their systems and operational practices? [10 marks]

(c) What functions would you recommend that the company should not out-source and why? [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 a library implementation of the protocol before using it in some application. [15 marks]

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

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

Question 3.

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 whistle-blowers (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 personnel 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. DevOps 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 usability 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 marks]

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

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

Question 4.

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

(b) Why is DNSSEC less likely to be deployed, compared to DKIM? [8 marks]

(c) How does the DNS leak private information? How can one mitigate that via changes to protocols, implementations and deployments? [10 marks]