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 2019 Year 1

Security of Networks and Distributed Systems

CS7NS5/CS4407

XX April 2019 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.

You are hired to do a risk analysis by a web development company who write generic shopping-cart software for web sites. Most of the company's customers are in Ireland or the UK. Given that the UK may be leaving the EU, the company's customers will require updates to the shopping-cart software, e.g. to calculate changes to taxes or tariffs should those be introduced when (or if!) the UK leaves the EU. At the time when you are hired, the specific changes that will be needed remain unknown, but it is considered highly likely that some changes will be needed, and that the details of those changes will only become known at the last minute. So your job is not to evaluate the risk related to those functional changes, but rather to help the company and their customers evaluate the risks associated with making and deploying last-minute changes to the shopping-cart code.

(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 web-site security.)

[10 marks]

(b) Describe the most relevant risks (at least 3) you see for handling such changes, including their potential impact and likelihood of occurrence, and outline the countermeasures you would recommend that the company, their customers and/or related service providers ought implement or deploy ahead of time to mitigate those risks.

[25 marks]

(c) If the changes end up being required to be deployed on many web sites all at the same time (a "flag day"), what specific risks not already mentioned would apply in that case and how would you suggest mitigating them?

[5 marks]

Question 2.

(a) For any real Internet key exchange protocol (e.g. TLS, IPsec, or Kerberos) describe the key management and application data protection aspects of the protocol in detail. How might the application programming interface (API) offered by an implementation of your chosen protocol affect application layer security?

Your answer may describe any widely used version of your chosen protocol, but you need to explicitly state which version you are describing.

[20 marks]

(b) How might your chosen protocol be strengthened against the possibility of attacks if a sufficiently powerful quantum computer were available to an adversary? What impact might such changes have on performance and interoperability? If someone using your chosen protocol was very concerned about the possibility of such an attack being feasible in 2029, what would you recommend they do today and in 5 years time?

[15 marks]

(c) Describe three security-relevant differences that arise when your chosen protocol is used in server-to-server deployments versus when deployed a client-server environment. (If you have chosen IPsec then describe three differences between transport mode and tunnel mode deployments.)

[5 marks]

Question 3.

A university computer science department teach an introductory ‘C’ programming module. To date, the examination for that module has been a hand-written exam (like this one:-). The university want to allow students to take the programming exam in a computer lab with standard desktop computers provided. Students will be given a number of programming tasks and must complete those during the 90 minutes of the exam. All students take the same exam at the same time in the same room. Students are not allowed to make use of the Internet whilst doing the exam. You are tasked with making an existing computer lab suitable for use for such an exam.

(a) Outline your overall design for such a system (include a network diagram), and state the security requirements the system must meet. Note that this part of your answer should only discuss security requirements and not describe how to meet those requirements.

[15 marks]

(b) Describe, in detail, the security solutions you would propose to meet those requirements, specifically including how you would prevent or otherwise mitigate potential abuses of the system.

[20 marks]

(c) A student wants to cheat and is willing to pay you to help do that. Given that you will not have seen the exam questions ahead of time, how would you assist that student in cheating without either of you being caught?

[5 marks]

Question 4.

(a) Describe the life-cycle of a typical second-level DNS name in a typical top level domain (e.g. .com or .ie), from initial registration to eventual retirement, including the steps required of all of the entities involved. Include a description of the security considerations relevant at each stage in the process. What additional steps are required to secure the zone for that name using DNSSEC?

[15 marks]

(b) What are the current and likely future privacy issues related to the overall DNS system? Describe mechanisms that have been proposed to improve privacy and the positive and negative consequences of those mechanisms.

[15 marks]

(c) An enterprise has been using split-horizon DNS for many years and use many names that are only resolvable internally. How would you suggest that enterprise handle split-horizon DNS in the event that browsers commonly use the DNS-over-HTTPS (DoH) protocol? In your opinion, what should browser-makers who support DoH do (or not do) to avoid having a negative impact on such enterprise networks? Justify your opinion.

[10 marks]