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 2024** **Year 1**

Security of Networks and Distributed Systems

CS7NS5/CSU44032

dd MMM 2024 *Location* *Time (2 hours)*

Dr. Stephen Farrell

Instructions to Candidates:

Attempt **three** questions. All questions carry equal marks (40 each).

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

2024 is a year with a lot of elections happening, in Ireland and elsewhere. A commercial Irish news organisation are planning to create a new web site for election related news that will have a mixture of their own locally generated articles and articles from other news organisations. The site will allow users to comment on articles, with moderation. They plan to use a new web content management system (CMS) for the new site, showing advertising for non-paid users but with the option for a paid subscription to use the service without advertising. Paid subscriptions are a new feature for the organisation. The organisation are concerned about the risks associated with moving to a new CMS, moving from purely advertising-driven web content to also supporting paid subscriptions, (a "paywall"), and also with the potential for abuse from user comments including possibly AI-generated comments. You are the employee tasked with carrying out a risk analysis of this system, both during the planning phase and as it goes "live."

(a) Describe the process you would use to carry out this task (note: this part of the question asks about process, not the specific risks associated with the new system).

[15 marks]

(b) Describe three significant risks affecting the planned system, including their potential impact and likelihood of occurrence, and outline countermeasures you would recommend that the news organisation ought apply.

[15 marks]

(c) What risks that potentially affect end users should be considered, and what actions would you recommend be taken to mitigate those risks?

[10 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. Describe how the cryptographic mechanisms used by your chosen protocol may affect server performance at scale.

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

[25 marks]

(b) Describe an application that can use your chosen protocol and that would be at risk in the face of a cryptographically relevant quantum computer? What application-layer mitigations and/or changes to your chosen protocol would you suggest to handle those risks in the short term (this year), and in the medium term, e.g., in five years' time?

[10 marks]

(c) What kinds of issues might arise should a server using your chosen protocol be deployed on a small device, such as a home controller running on a home network?

[5 marks]

Question 3

A regional transport authority (such as Transport for Ireland) provide a mobile application that allows users to see bus/train timetables and real-time information, and that is very widely used in the region. The application currently has a minimally invasive privacy policy, providing the option to access information without an account or without requests being easily identified as being from a particular device. Users do have the option to create an account, e.g. to get email notifications, but few users enable this option.

The local government and the transport authority now wish to enhance the mobile application to help them better plan changes to transport routes and to monitor pedestrian use of busier city-centre streets. This may require them to do some form of (possibly per-user) tracking, so they can accumulate information about, e.g., peaks and troughs in pedestrian use of streets, the numbers of people making specific bus/train transfers etc. However, adding such functionality clearly creates new potential privacy issues and may not be well-accepted by users.

You are tasked with designing a privacy-friendly enhancement to the mobile application and related back-end systems to achieve the goals above.

(a) Outline a design for the above enhancement (include diagrams as appropriate), and state the security and privacy requirements the resulting overall system should meet. Note that this part of your answer should only discuss security and privacy requirements and not describe specific mechanisms to meet those requirements.

[20 marks]

(b) Describe, in detail, the most important security and privacy mechanisms you would propose for the system to meet the requirements from part (a).

[15 marks]

(c) What are the best arguments you can provide for a) deploying the enhanced mobile application as described, and b) for not deploying an enhanced mobile application at all?

[5 marks]

Question 4

(a) Describe in detail how DNS query resolution for typical address records works, including, at each stage, potential attacks and mitigations. How might the new HTTPS resource record type affect browser performance if/when that is very widely deployed.

[15 marks]

(b) Describe the trust model and operation of DNSSEC, and the typical steps involved in validating DNSSEC-signed DNS responses. Explain why the number of domains for which DNSSEC is available is so small.

[15 marks]

(c) How do privacy issues arise in connection with the use of the DNS? How are those affected by the use of DNS-over-TLS (DoT) or DNS-over-HTTPS (DoH)? What default DNS privacy setup would you recommend for a current mobile operating system? Say why you consider that a reasonable default, and how it would affect those privacy issues.

[10 marks]