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 2023 Year 1

Security of Networks and Distributed Systems

CS7NS5/CSU44032

dd MMM 2023 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

Cost of living increases have been newsworthy in recent years. In Ireland the Central Statistics Office (CSO) calculate the Consumer Price Index (CPI) by monitoring price changes for a selected basket of goods. “Each month, approximately 80 price collectors collect approximately 50,000 price quotations directly from shops, department stores, supermarkets, petrol stations, etc. in 84 cities and towns throughout Ireland. Another 3,000 prices are collected centrally by the CSO on a monthly basis using postal, e-mail and telephone enquiries along with Internet price collection.”(*) Currently, price collectors submit paper reports to the CSO that are then processed centrally. The CSO are considering replacing this manual system with a system based around using a mobile phone app running on the collector’s own device. The app’s basic function is to allow entry of store and product pricing information and uploading of that to a CSO server for subsequent processing. The CSO however, are concerned about potential risks that might invalidate their CPI statistics and/or damage their reputation, so before going ahead with developing the app, they hire you as a consultant to carry out a risk analysis of the planned new system.

(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 CSO ought apply.

[15 marks]

(c) What risks that potentially affect collectors should the CSO consider, and what actions would you recommend they take to mitigate those risks?

[10 marks]

(*) The quote is from [1] (for anyone who’d like to check after the exam:-), but the mechanics of current and planned collection systems are invented for the purposes of the question.

[1] https://www.cso.ie/en/media/csoie/methods/consumerpriceindex/introductiontocpi16.pdf

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 an implementation of your chosen protocol could be vulnerable to timing attacks.

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

[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 automated pre-release (or continuous integration) testing would you suggest be put in place for developers of implementations of your chosen protocol?

[5 marks]

Question 3

A well-funded global human rights organisation plan to develop a new web-based system to allow small human rights defender groups to apply for funding for projects aiming to monitor possible rights violations. A typical project would involve less than US$50k in funding, would run for 3 to 6 months and might involve collating evidence of rights violations by state or commercial actors that can be confirmed later by others, e.g. mainstream media. (The ability to confirm evidence collected is an important requirement.) Other projects might involve training people to better use technology for evidence collection, in ways that don't put the collector at undue risk.

Application processing has to be fast, with a goal of providing funds for successful applications in a few weeks, in order to be able to react to events as they arise. As with any funding scheme, applications need to be reviewed by external technical, legal and ethics experts, and funding should be targeted towards applicants with good reputation. However, unlike many funding schemes, the application content and the identities of those working on funded projects can be highly sensitive - in some cases exposing application details could put lives at risk, so fine-grained confidentiality is required for the proposed system.

The funder will operate the web site that allows applicants to submit and track the progress of their applications, and that provides (some) access to outside experts who will evaluate relevant part(s) of the applications. Lastly, the funder also has to be accountable for the funds distributed, so needs to be able to provide information about the efficacy of funded projects, but again without creating risk for those executing funded projects.

(a) Outline a design for the overall system (include diagrams as appropriate), and state the security and privacy requirements the overall system must meet. Note that this part of your answer should only discuss security and privacy requirements and not describe how 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) If you were a bad actor working for an entity violating people's rights, describe how you might most effectively attack or abuse this system, after the requirements from part (a) have been satisfied?

[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 and privacy considerations relevant at each stage in the process.

[15 marks]

(b) The output from using the ``dig`` command to run a DNS query for the ‘jell.ie’ domain is shown below when DNSSEC validation is requested:

```
$ dig +dnssec jell.ie
; <<>> DiG 9.18.4-2ubuntu2.1-Ubuntu <<>> +dnssec jell.ie
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44569
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;jell.ie.               IN    A
;; ANSWER SECTION:
jell.ie.          3600  IN    A     213.108.105.239
jell.ie.          3600  IN    RRSIG A 8 2 3600 20230411141102
20230312131102 50256 jell.ie.
3JBP4mOqNNPGYZVtf2zUwjAuA30OgyCzXBQyK4LQqu+GUigGv3ns4kDn
0W778+KUXihgud5UTsRtCcC5gMReERgVK2hVA4+Uit/U3T53uIpmfXt7
ZYtDJZeAgzWmX+V3hfAPg6j28Sc7hLGohwCU+M2K+LoOiNzPb54dACjs OVQ=
;; Query time: 771 msec
;; SERVER: ::1#53(::1) (UDP)
;; WHEN: Tue Mar 14 01:00:46 GMT 2023
;; MSG SIZE  rcvd: 219
```

Describe the trust model and operation of DNSSEC, and the typical steps involved in producing the response shown above.

[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]