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

EXAM SOLUTION NOTES

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

Exam questions are in **bold, like this.** Solution notes are in non-bold Courier New, like this.

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]

The student should describe a process of identifying assets and risks, classifying them in terms of impact and probability of occurrence, e.g. with High/Medium/Low scores for each, and assigning an overall (partial) order to the list. Normally, one then iterates, designing a mitigation for the most imporant item on the list, and then re-doing the analysis as necessary (since one mitigation may affect the probability of other risks or may introduce other risks). In practice, the process terminates when the available effort is expended. In this case, interviewing CSO staff to identify statistical risks would seem useful, as would identifying BYOD risks associated with collectors. Any answer that captures most of this is fine, as are descriptions of equally good alternative processes.

Up to 10 marks for describing a reasonable process, 5 more for overall goodness.

© Trinity College Dublin, The University of Dublin 2022

(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]

Up to 4 marks per risk, with 3 for overall goodness. Risks here are fairly standard for any BYOD/app/server setup, but examples include:

- DDoS against CSO server making CPI announcements late; mitigation: put server behind an anti-DDoS service

- Accidental bugginess in app, e.g. triggered by an OS update, causing lack of updates for many collectors and costly fallback to paper system; mitigation: testing/CI setup, measure used-device diversity, maybe have a set of backup devices ready to ship to collectors if needed

- Client/app authentication creds (as used to CSO server) could leak, e.g. if only API-key or long-lived JWT used to authenticate device connections; mitigation: periodic full re-authentication of client, perhaps requiring a montly code sent via SMS to collectors or similar

- CSO server DNS name or certificate expiry; mitigation: good processes in CSO, auto-renewal for names (via registrar) and certs (via acme)

- collector upload failures, e.g. lack of credit on device or failure of home WiFi; mitigation: ability to re-do uploads later, even possibly significantly later

- registrar-hack causing loss of control of DNS name; mitigation: registrar-locks or similar

- Badly coded app could enable pervasive collusion between collectors, stores or product makers if e.g. another on-device app can manipulate app data (possibly via rooted device); mitigation: pentesting/app hardening

- app could enable collectors to more easily fake doing actual price checks; mitigation: perhaps require a proof-of-life type picture periodically

(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]

© Trinity College Dublin, The University of Dublin 2022

If 2 risks identified, 3 marks for each and 4 for overall goodness.

- If app uses location, or regularly collects and uploads any other meta-data, collectors could be tracked by CSO; mitigation: don't do that, and make a DPIA available to collectrors

- Collectors could lose money if app/device malfunctions; mitigation: a good app and a regularly used fallback for collectors with malfunctioning devices (maybe shipping temp device to collector)

- Collectors could accidentally expose private information, esp if e.g. a proof-of-life photo were demanded, that could include other people such as a child; mitigation: minimise requirement for photo upload, delete such data asap, train collectors about the risk

(*) 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

© Trinity College Dublin, The University of Dublin 2022

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]

Marks-from-15 for a good description of the scheme, with e.g. the TLS handshake and application layer properly described. 5 marks for describing possibly timing issues (Bleichenbacher etc.) and 5 for additional goodness (e.g. covering TLS extensions/tickets etc).

(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]

5 marks for describing an application that suffers today's PQ problem properly (ciphertext collection) and other PQ issues (e.g. immaturity of algs, IPR on Kyber, ...); Example could be anything processing genomic or health data. 5 marks for covering hybrid proposals and justifying short/medium term answers (which can vary depending on application).

(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]

2 marks for covering typical CI tests e.g. triggered by every commit to a PR or similar, 3 more for security relevant things, e.g. fuzzing, tests with bad integrity, wrong keys etc.

© Trinity College Dublin, The University of Dublin 2022

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]

8 marks for overall design, e.g. diagram showing roles; 8 marks for more obvious requirements identified 4 more for overall goodness. Basically an obvious web-based system but with strong authentication, and likely managed pseudonyms for applicants, also with strong separation of roles linked to access to parts of application content. Roles: admin, applicant, evaluator (tech, legal, ethics), auditor (finance/real identities). Likely selective field confidentiality for different parts of applications.

© Trinity College Dublin, The University of Dublin 2022

Including incident-handling plans is good. Notification system (e.g. result available) should also preserve confidentiality and not expose applicant e.g. if email monitored.

As usual some students will mix up requirements & implementation/mechanisms (i.e. parts (a) & (b)) but I'll be lenient on that.

(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]

Marks from 10 for hitting the obvious points, with 5 more for inclusion of less obvious things. Obvious things:

- User authentication with 2FA for all roles
- Good list of roles
- General server goodness: pentesting; no external JS/CSS dependencies, modern TLS setup etc.
- Arguments could be made for self-hosting server but care needed wrt IP address tracking, so one could argue using an AWS/Azure instance better
- separating application into different parts, differently visible to different roles
- encrypting application content at rest using selective field confid with access to keys tied to roles
- minimal notifications

Less obvious (perhaps):

- Provide a Tor .onion server for applicants to use
- If/when ECH becomes widely available, move server to CDN that supports ECH
- Separate applicant pseudonyms vs. real identities but with persistent pseudonyms (for reputation)
- Training for applicants wrt what to put in what parts of application so as to preserve pseudonymity; how to use a public recursive etc.
- Require auditors to flag some project(s) before they see real identities
- Create an innocuous fake project that real projects can pretend to have been doing if their funding becomes known

© Trinity College Dublin, The University of Dublin 2022

(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]

Straight marks from 5, with more marks for sneakier attacks. Possibles:

- Obvious: DDoS server, get govt. to block server IPs/DNS names, leverage OSINT to identify funded people
- sybil attacks using ChatGPT generated applications to overwhelm process
- get a spy inside the funder as an employee, or inside mainstream media who've confirmed evidence
- try identify project participants via staged actions or traitor-tracing

© Trinity College Dublin, The University of Dublin 2022

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]

Marks-from-8 for a good description of the life-cycle with all players and basic DNSSEC included and potential security issues (e.g. hack registrar) mentioned. The other 7 for describing security/privacy issues well, e.g. whois data, rgistrar a/c hijack, registrar hacks, lookalike domains etc.

(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]

5 marks for a good description of basic DNS recursion; 7 marks for describing DNSSEC well and 3 more for overall goodness, e.g. if they included CDS/CDNSKEY or similar or discuss non-obvious specifics of the DNS query shown (e.g. flags, server is on localhost, EDNS).

© Trinity College Dublin, The University of Dublin 2022

(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]

The students will need to figure this out themselves as we'll only briefly have mentioned it in class (and today, nobody knows for sure what'll actually happen). We won't have covered ADD in class. Likely options include browser builds with corp. setup that don't do DoH or only to in-house revursives, doing nothing and saying that enterprises should get rid of split-horizon and just put it all out there, browser detecting some local config enterprise can set e.g. in their own recursives or in-house authoratitives that control how DoH is done (possibly with some form of authentication required). Most of those could be defended, 7 marks for describing something sensible that could work, 3 for how well they justify it as reasonable.

© Trinity College Dublin, The University of Dublin 2022