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

EXAM SOLUTION NOTES

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

Exam questions are in bold Calibiri, like this.

Solution notes are in Courier New, like this.

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]

The student should describe a process of identifying 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. 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 theory some other form of termination might be described. Any answer that captures most of this is fine.

In addition to the usual process above, students might include: building testbeds with mocked up new code (using guesses at new rules) to test ahead of time; surveys of existing deployments (esp to check what integration testing is needed); contacting customers to ask them what risks they see and agreeing roll-out (and roll-back) processes with customers.

(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]

The student should take proper account of the context – the existing web sites, the lack of time, the existence of ambiguity in rules as they affect particular products or services, possibly having to use contractors and lack of time to test. The main point is to describe a reasonable set of threats and mitigations that approximates what might really happen.

Risks should be described including estimates of impact and probability of occurrence and they ought concentrate on the more significant of those. Impact and probability can take any value without losing marks, but for something odd (e.g. if they considered lack of time to test low impact) more justification is needed. If the impact/probability are fairly obviously right, less needs to be said. Marking is out of 5 points for each good one and with 3 more for overall goodness. Possible risks would include:

- code quality/QA
- potential for coders (esp contractors) to add backdoors
- lack of time to test deployments, leaving sites with new vulnerabilities
- potential for web sites to try make chanegs themselves that conflict with the vendor’s s/w
- integration failures between new and existing code
- getting rules wrong for specific products/services and having to re-visit those
- errors if new geo-location is required and doesn’t work well
- payment processing changes

- changes to product delivery charges/rules being implemented badly
- changes to courier/tracking systems and costs causing breakage at integration time
- changes to reporting/accounting systems causing breakage at integration time or later

(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]

A flag day will likely put additional load in lots of places, so talking about that will be fine. For example, whatever s/w distribution scheme is used to get code to web sites could fail; some sites might get updated early, some late; some transactions could be in-play before the cutoff time; DDoS actors are more likely to choose to strike on the flag day; phishing attempts related to the flag day are to be expected etc.

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]

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 effects of APIs, e.g 0RTT early-data issues, private key mgmt/HSMs, even simple tings like threading.

(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]

They should refer to the NIST competition candidates, say that some of those can be used to do key exchanges that are mixed with (not replace) existing D-H key agreement; could be >1 PQ key exchange mixed in. They should say roughly how one might do such mixing, e.g. using TLS CH/SH extensions, or maybe key_shares. For impact, they should say there're still unknowns but key sizes are v. likely to change. Run-time performance may not be too badly affected but could be on some kinds of (smaller) device. If they propose use of hash-based sigs, then they need to note the stateful private keys. For today they should say to just monitor developments unless you have specific needs to keep application data secret for e.g. 20 years. For 5 years time more likely want to have some mixing of NIST candidates or winners usable and tested by then, so deployment can be done as needed.

(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]

Various possible points:

- different root stores vs. Web deployments

- can build own PKI easily and use mutual-auth, but still need some kind of mapping from x.509 subject names to application meaningful names

- no user to see warnings so need hard-fail and logging

- key storage needs to work across reboots on both sides

- key rotation needed (in case of breach)

- etc.

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]

They should probably outline how the lab is setup before and after, but definitely after. The "after" state can't really use any different h/w. Lab-for-exam setup should basically f/w off all machines from one another and from outside, but will still need some services running, esp student authentication.

Requirements likely include:

- special invigilator training (with sysadmin backup)

- ability to swtich-to-exam-mode and back without too much trouble

- strict workstation integrity - build needs to have everthing needed for exam but nothing else, e.g. no trojan code surviving switch-to-exam

- 3rd party audit of setup before and after exam

- authentication of students

- backup: saving state/work on the fly automatically

- student sign-off of final exam state

- archiving of exam-script equivalents for marking

- access controls for exam-script equivalents (course director, marker, admins etc with varying roles)

- alerting/audit of everything done during the exam time, esp student attempts to mess with systems:-)

- v. high reliability, against systems and power failure

- having a 2nd exam ready to go in the event of failures, either in the same or a different room, at the same or a later time

(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]

They should propose a way to meet each of the requirements stated. The more secure, sensible, practical and easy, the better. I'd expect this to mostly be built around some kind of VMs and re-flashing the boxes with some student authentication scheme and a later DB of scrip-equivalents accessible via the university intranet/web. There's scope for cleverness in handling student sign-off of final state, e.g. could be stuff gets sent to a specific printer that the inviligator can access and have the student physically sign the output might be easiest, anything fancier may be too hard.

(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]

The sneakier the better. Likely some backdoor triggered via a phone-in-pocket or smart-watch that allows student to get externally supplied solutions developed outside the exam environment e.g. 30 mins into exam. Delivery of solutions via covert channel, e.g if "gcc -o a.out prog.c" produces the goods for a few minutes around a known time if prog.c has the right innocuous-looking content. Delivery of that borked gcc into lab space via a late s/w update, but getting caught there isn’t hard.

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]

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 how changes are handled well, e.g. switching regisgtrar, DNSSEC re-signing, KSK roll-over, possibly automated via CDS/CDNSKEY.

(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]

5 marks for stuff about DNS privacy problem statement, 5 more for QNAME minimisation, DoT, DoH descriptions and 5 for calling out the good (better privacy, anti-censorship etc.) and bad effects: e.g. passive DNS disruption, enterprise DNS bypass via DoH, centralisation towards CF, quad-9 and google etc.

(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). Likely options include browser bulds with corp. setup that don't do DoH or only to in-house servers, 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.