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 2018**
Year 1

Security of Networks and Distributed Systems
CS7053/CS4474/...

XX April 2018 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.

EXAM question text is bold, like this.

Exam solution text is "Courier New," like this.

Materials Permitted for this examination:

N/A

Question 1.

An Irish medium-sized manufacturing company has about 1000 employees, a small number of overseas offices and some dozens of frequently travelling employees. The company want to replace their existing in-house email infrastructure and are considering how to do that, including deciding what to continue to host themselves and what to outsource. They ask you, as a security consultant, to do a risk analysis for them, considering the security and privacy implications of a new email system and of migration from the old to a new system.

The new system may involve updates for all email components: standard desktop, mobile and web user agents, mail submission servers, inbound and outbound mail transfer agents, message stores and security components such as anti-spam and anti-malware systems. Existing accounts and message store content will need to be migrated to the new system as that is incrementally deployed. A very small number of employees use PGP (mainly sysadmins) but most users do not use of PGP or S/MIME. Some users currently use third-party email systems, (such as gmail/hotmail), for work email, as there is no policy in place about the use of such third-party systems.

(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 email security.)

[10 marks]

The student should describe a method of identifying risks, (e.g. for different mail system components such as servers, MUAs etc perhaps also based on the corpus of existing mail and usage patterns etc.), 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.

(b) Describe the most relevant risks (at least 3) you see for the new system, including their potential impact and likelihood of occurrence, and outline the countermeasures you would recommend that the company and/or their chosen service providers (who provide out-sourced functions) ought to implement to mitigate those risks. Risks that could emerge during migration from the old to the new system are in scope here.

[25 marks]

The student should take proper account of the context – the existing email environment (with spam, phish etc), an SME without much expertise, the existence of various suppliers and 3rd party services, such as inbound filtering. The main point is to describe a reasonable set of threats and mitigations that approximates what might really be used.

The main thing here is to describe risks with their impact and an estimate of probability of occurrence and to concentrate on the more significant of those. The impact and probability can take any value without losing marks, but for something odd (e.g. if they considered phishing low impact) they will need more justification for saying that. 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:

- Spam, phishing, malware etc.
- Availability (lack therof) if all services handled in-house
- Lack of deliverability if servers badly configured (e.g. spf, dkim, dmarc)
- Abuse of content if 3rd parties used (e.g. malware scanners)
- MUAs that render active content
- Badly configured MUAs e.g. on phones, MUAs that re-direct to gmail

- Mail snooping via MX stealing or BGP
- Spear-phish aimed at local PGP users

(c) Assume the company had instead gone ahead and deployed a new system without having done any risk analysis. Describe some mistakes, not covered in part (b), that they might have made?

[5 marks]

Just marks-from-5 for a good answer. Obvious errors would include not setting up spf,dkim,dmarc or allowing MUAs to talk POP/IMAP in clear.

Question 2.

(a) For any real Internet key exchange protocol (e.g. TLS, S/MIME, IPsec, Kerberos) describe the key management and application data protection aspects of the protocol in detail. Include a description of how networking failures, (e.g. packet drops, re-ordering), might affect use of your chosen protocol.

Your answer may describe any widely used version of your chosen protocol, but you need to state which version you are describing. Choosing TLSv1.3 is allowed – you don't need to specify the exact Internet-draft version you've chosen in that case.

[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 network failures esp if reactions to those covered.

(b) Outline the ways in which the security of your chosen protocol depends on other infrastructure such as the Internet routing system, the domain name system or a key management infrastructure.

[10 marks]

Main thing here is PKI – for issuance, renewal and revocation status checking. CT is another. If TLS-stripping is possible with an application, then DNS or BGP attacks would work, but both DNS and BGP are depended-upon for correct operation. Noting man-on-the-side attacks would be a bonus. (That last only mentioned in class, not really covered.)

(c) State-level adversaries have different capabilities and interests when compared to potential industrial or commercial adversaries. Describe three ways in which the threat-model for an implementation or deployment of your chosen protocol would differ, when considering state-level versus industrial or commercial adversaries.

[10 marks]

Just simple bullets here would suffice, possible things would include:

- state-level attackers can see the network and record traffic from many vantage points, e.g. undersea fibre termination points; industrial attackers will tend to have to target specific nodes to try get at a target
- state-level attackers can bork implementations, e.g. like DUAL-EC attacking a system PRNG, or via physical implants into servers/routers; industrial attackers would need to breach each node
- industrial attackers can be assumed to be economically rational, whereas state-level attackers are not motivated to only go for the weakest link – threat models for the latter can be simpler as a result
- state-level attackers are more likely to want ongoing access (via APT or exfiltration of keys), whereas industrial attackers are more likely to want application layer data

If students don't talk about threat models, but only about specific threats, that's ok, but will be marked a bit less.

Question 3.

TCD decide to plan for the increasingly common situation where the campus must temporarily close due to a "red" weather alert. The overall plan is to be able to switch into a "remote-access" mode of operation where administrators, academic staff and students can still do some work, even if they cannot operate entirely normally. In "remote-access" mode, (some) lectures will continue via the Internet, and coursework assignments can be set, completed and marked. Clearly, real-time exceptions will need to be handled, e.g., due to network problems. More fundamentally, new timetables/schedules and modes for student/staff interaction will be needed to handle lecture timetabling and assignments without over-burdening staff and students who will at the same time be dealing with the physical disruption caused by the inclement weather.

The university are at the early planning stages for this system, and ask you to provide a design for a prototype system to be trialled in the School of Computer Science and Statistics. The prototype system will be tested via a planned exercise that will only be announced a few days ahead of time. That is, students, academic and support staff, will only have 2-3 days notice that they are to switch into "remote-access" mode for one week, that they must not attend campus during that week (relevant buildings will be locked), and that they need to use the new system to do as much "normal" work as possible. Before the exercise, students will not have used the system before, but they will have undergone some training and HOWTOs and other guides will be available online. You can assume staff have had more training but are still quite unfamiliar with the system.

(a) Outline your overall design for such a system (include a network diagram and describe how scheduling is handled), and state the security and privacy requirements the system must meet.

[15 marks]

This should be a fairly straightforward multimedia web system, with feedback and assignment handling, but will need some consideration of flexible schedules and e.g.

instant messaging sessions. Giving students and staff new credentials for this system is optional, but good to note the possible issue.

For S&P requirements:

- authentication, maybe with some detection of impersonation (e.g. track multiple devices being used)
- confidentiality and authorization, student interactions must only be visible to authorized entities (if materials are publicly visible, that's ok but different)
- staff access is clearly different
- scheduling system has separate authorization issues
- DoS risk from students who'd prefer to do nothing
- etc.

(b) Describe, in detail, the security solution you would propose to meet those requirements.

[20 marks]

Could be a fairly simple use of Oauth with some MOOC or similar (it's ok if they go for a home-grown system and not some MOOC/CMS) with the various roles defined. Should really do everything over TLS, e.g. use WebRTC (ok that's DTLS-SRTP but whatever:-).

Credential handling could fill pages here if they choose.

(c) How would you handle evaluating the security and privacy aspects of the system, before, during and after the planned exercise?

[5 marks]

Before: (Pen-)Testing, then more of that:-) Do a dry-run if possible for one course and try attack that whilst the test is in progress. Usage monitoring and audit.

Question 4.

(a) Describe three significant security and privacy differences between real-world end-to-end and hop-by-hop security mechanisms as used for interpersonal messaging, in email and/or instant messaging systems.

[15 marks]

Take mail:

- e2e gives message body security but not headers; hbh covers headers but allows servers to see content; traffic analysis remains possible but differs in each case
- e2e typically makes malware detectection harder
- e2e is harder to deploy
- hbh is vulnerable to e.g. DNS attacks (MX stealing)
- etc.

(b) Describe three significant barriers to the deployment of Internet-scale end-to-end email security mechanisms such as S/MIME or PGP. In each case, describe realistic actions you would recommend that aim to at least partially overcome those barriers.

[15 marks]

- users don’t know the difference and aren’t motivated to figure it out
- getting a cert for SMIME is too hard
- finding public keys for peers is too hard (signed messages and PGP keystores don’t work so well)
- e2e typically makes malware detectection harder
- SMIME and PGP were designed in a one-MUA per person world, which is not today’s (private key mgmt is hard and needs new infrastructure)
- SMIME and PGP clients both tend to fail with complex messages (many attachments, forwarded messages)
- Large mail services (gmail etc) aren’t motivated to want to all deploy the same solution and are needed

- etc.

(c) If end-to-end email confidentiality became the norm, so that most email messages were encrypted between sender and recipient(s), what problems would that cause for email system administrators, and how would you recommend they address those issues?

[10 marks]

- e2e typically makes malware detectection harder; would need to move that to endpoints (MUAs) which costs (but is needed in any case for other reasons, e.g. malware arriving via https)
- some admins like outbound mail scanning for good (malware spread) or bogus (IPR leak) reasons – can ensure MUAs bcc some admin a/c that can do all the scanning needed
- spammers would use public key info to generate target lists – some novel form of access control would be needed (e.g. you can see a pulic key if you've previously interacted) but that's a hard hard problem to solve while keeping mail deliverability