SOLUTIONS AND QUESTIONS FOR CS7053 SECURITY EXAM 2010

Dr. Stephen Farrell

Questions are in normal *font, answers/marking scheme text is italicised.*

1. You are an independent security expert hired by a startup web services company that has just won a significant new contract with a major customer. The startup offer both installable/deployable products but can (they say!) also host deployments on behalf of their customers. The major customer is a mature business with a very structured way of handling information security. The startup are a startup and while they have thought about security for their products and service deployments, that has been done informally. Your task is to help the startup meet the requirements of the major customer. If it helps, you can use any reasonable startup/mature business scenario in your answer, e.g. a web merchant and a bank, a new social networking technology/site and a large ISP, etc.

The main thing here is that their answers attempt to be reasonable, regardless of the specific situation, a startup cannot be expected to fully

(a) Describe what you consider are most likely to be the three most important generic security issues that you would expect to face in general in a situation like this? Note that the question here is not asking for a description of three specific technical vulnerabilities, but rather for the important process/company-level security issues that are likely to arise. (5 marks)

Possible issues (in my rough order of most likely/important) include:

- *startup has insufficient in-house security knowledge to be able to meet major customer's security requirements (or even to properly analyse them)*
- *lack of security processes in the startup (e.g. for incident handling, vulnerability reporting, security review of code/deployments)*
- *cost of ISO 27001 compliance (or similar) for a startup is too high, so if major customer requires (something like) that one needs to figure out an intermediate approach (e.g. startup internally does 27001-like work, and major customer gets to audit)*
- *startup's products/services were designed with no serious consideration of higher-security modes of operation – designers made assumptions that "medium/low" level security measures would be most appropriate*

- *startup has insufficient resources for really independent review of its internal code/processes – when all you have are two eyes, four-eyes testing just isn't possible!*

Any equivalent level issues can be ok, so long as they're reasonable. Marking is one per reasonable issue, with 2 more for overall. If a student misinterprets the question and the answer relates to specific technical vulnerabilities, the they'll be marked from 2.5 for this (i.e. 50% down) – there is a note in the question saying not to do this!

(b) Describe how you would determine the actual situation, (i.e. say how you would find out if and to what extent the particular issue applies), how you would set about mitigating each of the issues identified abouve assuming there is work to be done, and how you would determine that the issue has been sufficiently addressed. (15 marks)

In each case, the starting point would be to meet with the startup, to describe the issue so that they understand it, then to drill down with them to find out if the issue is relevant for them. (1-2 marks) For some issues, one might have to interact with the customer to determine the state of play (1 bonus point).

Marks from 4 for each issue for addressing the other parts of the question. To take the last example above, one could ask what development processes are used and how those address security, one could ask to see bug/security-issue reports that have previously been filed, etc. If (as one would expect) the startup does not handle securit y in their development processes, one could suggest that they nominate one or more developers, professional services and/or operations staff and give them some security training; they could then be involved in security reviews at relevant parts of the startup's development cycle (when exactly depends on the type of model used, agile, waterfall...). If the startup has very few staff, then consider hiring in a (cheap?) security professional for part of e.g. system test. To check if something's been done about this one, best might be to revisit the startup after a major release and just ask to see the bug reports/tickets that were generated as a result of security review. The quantity and quality of those will reflect the level of review.

(c) How would you, as a security professional, handle the situation where you suspect that the startup intends to lie to their major customer about some significant security issue? (5 marks)

Straight marks-from-5 for this. The main answer is "carefully!" First the answer should reflect that the situation is not certain ("suspect"). I'd say that as a contractor for the startup your first duty is to do a good job for them and to be clear that the onus to act correctly is on the startup and not on you as their contractor. However, one should make it clear to the startup that hiding

security issues is, in the end, counteproductive. How to do that would depend on who it is that's likely to fib. The contractor should be sure to document the issue for the startup in some form. Its possible that a good answer might take a very different position from me, the main thing is that it be insightful.

2.

(a) For any real Internet key exchange scheme (e.g. TLS, IKE, S/MIME), describe the protocol, specifically highlighing the main security features of the protocol and explaining why the designers chose these specific features. (For example, if a particular key derivation function is used, why is it done that way?) (10 marks)

Marks from 6 for the basic answer. Take TLS as an example. The answer should cover the handshake and APDU protocols, negotiation/finished messages, the use of RSA key transport, the pre-master secret and KDFs for other secrets (and that the default KDF uses two hash functions for robustness) etc etc.

2 more marks for explaining optional/less-used aspects of the protocol, e.g. compression, the possibility for D-H or Kerberos ciphersuites, how client certificate handling involves re-negotiation etc.

2 further marks for covering implementation and/or design vulnerabilities that have affected the protocol, e.g. bleichenbacher, the TLS re-nego bug, bad PRNG issues etc.

(b) Discuss, in detail, the performance implications of your chosen protocol, both for clients and servers (or senders and recipients) covering a range of platforms and a range of scaling factors. (10 marks)

Marks from 5 for basic description of protocol performance issues, e.g. using TLS again, that the client usually does an RSA public operation whereas the server has to do private key ops, (and why those differ); that the APDU protocol adds an acceptable bit of overhead to packet sizes; that the symmetric crypto is very quick.

Marks from 2 for covering a range of platform issues: mobile clients (and servers!), TLS accellerator hardware boxes, ability to do TLS on most any system. Good to mention that TLS can be used for more than HTTP here, e.g. IMAP/TLS.

Marks from 2 for covering a range of scaling issues: e.g. busy hour, v. Large scale systems (e.g. gmail sized and bigger); possible use of mixed content or TLS only for "login" operations and cookies thereafter (and pros and cons).

(c) Describe a way to modify the protocol, without seriously compromising security, that would result in improved performance in one of the situations you described in part (b) above. (5 marks)

Straight marks from 5, mainly based on the credibility and novelty of their proposal. If their proposal exists (e.g. a TLS session resume equivalent) they loose marks (esp. If they don't indicate that they know their proposal isn't novel!). If their proposal is novel but just doesn't work then they loose marks.

An example for TLS might be the ability to (securely, maybe protected via EKE) export a pre-master secret from one instance of an application layer client to another that belongs to the same user (while telling the server) so as to reduce the frequency of full handshakes on the server when clients login from different devices regularly. There could even be a standard format and standard interfaces for that so you could export from Thunderbird and import into your iPhone or "bind" those two so that they would rendezvous via some untrusted server on the Internet.

3. The regulation of the financial industry has been in the news of late. You are asked to design the security aspects of a new system to be developed for a country's financial regulator that will be installed in each financial institution ("FI") and will interface to that FI's internal systems, so as to give the regulator an online and immediate view of the FI's current activities.

Note: You can pick any country you like - if you happen to know some details of financial regulation in some country then its ok to use that country. The overall system is intended to report on the full range of FI activities (consumer and business banking, stock trading, interbank deals, insurance etc.) but for the purposes of answering the question you can limit the system as you see fit, for example, its ok if your answer only covers one of the above such as consumer banking. You should preface your answer with any assumptions along these lines that you wish to make.

Each part is straight marks from 5.

(a) List and justify the 5 most important high-level security requirements that you would expect the system to meet. (5 marks)

*There are many from which to choose here, 1 mark for each good one. They should however be "high-level" as are the examples below, and not e.g. "files should be encrypted on disks". The justification just needs to explain why this gets onto the list and should basically be related to risk (impact * probability). Examples:*

- *All details submitted by FI's must be authenticated as being from that FI (risk: bad guy fakes FI's data)*
- *Only registered FI's can use the system (as above)*
- *Components deployed in FI's must be highly tamper resistent or tamper evident (FI's have a reason to mess about)*

- *Regulator staff access to FI data must be controlled and audited at a very fine-grained level (shouldn't be too easy for these staff to tell one FI what another's doing)*
- *FI's must supply all agreed data that must be validated against the FI's audited accounts at year-end (FI's have lots of motive to keep things "off books" from this system)*
- *Etc. Etc. There are loads really*

(b) Provide an overview of the system, highlighting the security aspects of your design. Include diagrams as appropriate. (5 marks)

There are many options as to how to do this. One would be to provide a web based interface (RESTful API) on a tamper resistent device within the FI that sets up secure connnections to the regulator. (That device probably needs some local storage). Within the regulator there is a need for secure storage (and lotsof it) which would be a challenge. The regulator needs to be able to data mine etc (and so generates results frmo that that also need to be stored) but it should not be easy to get bulk data out of the system. There needs to be a backup solution. There needs to be a user management solution. Devices sent to FI's also have a life-cycle and must be manufactured, provisioned deployed and end-of-lifed securely.

(c) How would you ensure that the deployed and running system meets the security requirements imposed at design time? (5 marks)

Audit mainly – of systems, code and data. Also tiger team testing. Setup a fake FI and let the tiger team attack it every few months.

(d) How would you convince a third party (say a local parliament or Government committee) that the outputs from the system are trustworthy? (5 marks)

Use digital signatures on application layer but that requires a good/complex PKI so that the evidence generated (signatures) is strong. Could be done in this case, better if the private keys are within the tamper-resistant devices but that affects how you deploy new devices.

(e) It turns out you are dishonest and after the system has been runnning for a few years, you are paid a large sum of money by one FI so they can avoid or subvert the system. How would you set about doing this for them? (5 marks)

Better marks for sneakiness here, but the answer should not be a "Hole" deliberately left in the system in previous parts of the answer! One possibilitiy is simply to threaten the credibility of the system by getting a 2nd FI to pay someone else for the same thing and then leaking that story to the media.