SOLUTIONS AND QUESTIONS FOR CS7012 SECURITY EXAM 2009

Dr. Stephen Farell/ Prof Vinny Wade

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

1. You are an internal IT security analyst for a consumer bank, which, like many banks these days, is facing market challenges. The bank's management wish to ensure that no further damage to the bank's reputation occurs and so have requested you to o a security review of their current consumer Internet banking offering.

a) Describe a current consumer Internet banking operation, emphasising the security measures deployed, in both the customer-facing and internal parts of the system. (Note: you may use any real, or invented but realistic, consumer Internet banking operation with which you are familiar as the model when answering this question. It is not required however, that your description be exhaustive with respect to bank-internal systems; demonstrating an understanding of the server-side security issues in generic web applications is sufficient.)

(10 marks)

The description here should include user facing security measures, in pareticular some way to authenticate users that might be acceptable to a bank. Mechansms that reassure the user that they have contacted their bank (e.g. displaying the time the user last logged in, after entry of partial user information, but before entry of the user's secret), could be included. Server-side security must be described in some level of detail, e.g. Specifying termination points for TLS sessions (at application servers or load balancers), mechanisms to secure databases against theft, handling of log files etc.

Marking scheme is marks-from-2 for the overall descritpion of user side security and marks-from-4 for the server side. Each specific, reasonablly accurate descriiption of a realistic countermeasure will attract an additional point.

b) Given that management's goal is to reduce the risk of reputational damage to the organisation at this highly-sensitive sensisitve time, describe how you would approach carrying out a security analysis of the Internet banking operation you described above. (Your answer should cover both generic and system-specific aspects of risk analysis.)

(10 marks)

Marks-from-6 for how well they descibe generic risk analysis 2 marks for overall goodness of the answer and 2 marks specifically for noticing that (and *properly describing the handling of) the fact that the risk analysis is being carried out is itself sensitive.*

c) Banks are of course attractive targets for phishing attacks. How would you monitor general Internet activitiy so that you would have early warning that your bank is a current target of a phishing campaign? How should the bank react to that, when it occurs?

(5 marks)

Almost straight marks from 5 for this. The answer should be that the bank themselves, or more realistically, a contractor of theirs, sets up a honey net of some sort and reacts to relevant phishing attacks with increased security surveillance of the site. The wrinkle here is that the bank must not send out e-mail telling their customers that a phishing attack is ongoing – to do so, would simply add to user's spam and is ineffective in any case.

2. (a) For any real Internet key exchange mechanism (e.g. TLS, S/MIME, Kerberos), describe how that mechanism is used in some real application from the user interface down. For example, for HTTP/TLS your description might start with "The user clicks an https:// link." and would go on to detail that TLS handshake and application data protocols.

(10 marks)

Marks-from-6 for the usual description of the key exchange mechanism (e.g. the TLS handshake). Additional marks-from-2 for each/any of:

- *correct description of the UI issues, possibly including setup (e.g. root certificate managers)*
- *describing how the mechanism is triggered, e.,g. STARTTLS in IMAP/TLS; connecting to 443 in HTTP/TLS*
- *covering how application data is protected and not just the handshake stage*
- *covering server-side implementation aspects, e.g. load balancing*
- *covering revocation and other error cases in the description, regardless of the next part*

(b) For the application you chose above, say how five errors can occur in the cryptographic mechanism that affect the user interface of the application? For each error considered, say how you think it *should* (as opposed to is currently) be presented to the user.

10 marks)

*Marks-from-2 for each, possible candidates include: expired or not yet valid public key certs; unknown CA; self-certified keys; weak ciphersuite; short public key in certificate; known bad key pair (e.g. as in SSH vulnerability); domain name (or mail address for S/MIME) mismatch between site and certificate; cannot contact OCSP responder; revoked cert; bad EV cert; etc. In each case, a proper description of the error is worth one mark, and a good description of how it **should** be presented to a user is worth one. The main thing with the latter is the avoidance of technical jargon and saying what actions the user can take (which may include "ignore," possibly via a few clicks as is done by Firefox 3).*

(c) User testing indicates that many security error handling user interfaces merely triain users to click "ok" without thinking. Why is that and what would you do about it?

(5 marks)

Straight marks-from-2 for noticing that the errors presented mean nothing to users and often include an “ok” button on the first dialog. Marks-from-3 for suggesting sensible things to do, e.g. cleverer use of browser history to know when to annoy the user.

3. You are asked to design an Internet survey system (e.g. like surveymonkey.com), but in this case only for use by law enforcement officials. The main function of the system is to allow users to setup and run simple surveys among targetted groups.

(a) What do you consider the 5 most important security requirements that the system must be designed to meet? (In each case, justify your selection.)

(10 marks)

2 marks each, 1 for a reasonable requirement, the other for a good explanation of why its important. Possible requirements include:

- *Only authorized LE users can use the system to create surveys and read results –justification: that's the point of the system! But this assumes some infrastructure for authent/authz is setup.*
- *Survey invitees MUST also be authorized LE personnel; justification: if you allow non LE to be invited, then you leak information (its also reasonable for a student to state the opposite requirement, i.e., that non LE folks can fill in surveys).*
- *Survey fillers MUST be authorized LE personnel; justification: these could, but hopefully aren't, different from the invitees, but good to distinguish. (As above, an opposite requirement could be ok here too.)*
- *Results DB MUST be strongly protected against theft (probably encrypted); justification: the DB is probably the most sensitive part of the system*
- *All connections to system MUST run over TLS or a VPN; running in clear could allow leaks*
- *Survey results MUST be integrity protected, at least by the system; if someone might act on the results then they better not have been modified.*
- *The system MUST audit/log events; justification: otherwise no way to detect possible abuses.*
- *The DB must be behind a f/w and not accessible directly from the Internet; justification: good way to design border systems.*
- *Anonymity for respondents, where required.*

(b) Describe your design for the overall system, specuifically calling out the aspects of the design that satisfy the requirements you stated above..

(10 marks)

Marks from 6 for overall; plus 1 each (up to 4) for the specific points below that are called out. Designs may vary but they should all be reasonable, with e.g. the following featurres:

- *Use of an IPsec VPN or TLS more or less everywhere, no need for cleartext here since traffic levels won't require that*
- *Separate application server and DB, with DB inside and application server in DMZ.*
- *User authentication and authorization system, maybe with speedy user revocation*
- *DB integrity and confidentiality*
- *Restrictions on viewing results (can be done various ways)*
- *Probably not enough to have received the invite mail to fill in a survey, typically, user authentication would also be needed which is different from a more open system.*
- *Maybe a clever anonymising solution.*

(c) How might law enforcement officials abuse this system? How might you detect and react to such abuse?

(5 marks)

Abuses might involve collusion (audit); use of the system as a covert channel (audit); leaking results (audit; maybe traitor tracing). Straight marks from 5 with a bonus for inventive badness.