UNIVERSITY OF DUBLIN

TRINITY COLLEGE

FACULTY OF ENGINEERING & SYSTEM SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

M.Sc. in Computer Science Hilary Term 2007

Code & Name of Exam

Date of Exam Location Time of Exam

Name of Lecturer (Lecturers)

Attempt * questions
(all questions carry equal marks)

Question 1:

You have been hired by a software development company in order to setup a new code quality and security review team.

a) **Describe how you would set out to analyse the security of an existing product of theirs? (10)**

The main thing here is to be reasonable – you cannot revolutionise an entire company just to improve their security processes, so an evolutionary/stepwise approach is needed. Marks from 4 for the overall approach embodied in their answer.

Otherwise they get a mark for a reasonable mention of each of the following or equivalents:

- Start with a status review
- Establish a team including some of the older hands
- Setup some training for other staff
- Review sources of vulnerabilities for problems with current product (e.g. CVDB/CERT etc.)
- Setup some scheme for filtering external bug/vulnerability reports and making them easier to use in-house
- Setup an internal/external tiger-team test
- Talk to current users/administrators
- Pay a bounty for bug/vulnerability reports
- Setup an old code review scheme
- Spot-check existing documentation/test-reports

b) **Describe how you would setup processes so that future projects would result in fewer security problems. (10)**

Again up to 4 marks an overall reasonable approach. Otherwise specific marks for:

- There are obvious analogs to the above bullets here all of which can count
- After the 1st product is done - build from the results achieved
- Get management buy-in for inclusion of security reviews in development processes
- Include both early and late-stage security reviews
- Setup an internal CERT with accreditation
- Join industry/local security for a
- Encourage/argue-for the use of tools (e.g. static code analysis, leak checkers etc)
- Pair-programming
- Move towards development environments less prone to buffer overruns (e.g. maybe to Java)
- Educate employees

c) **The company are considering acquiring an embedded systems development company; what questions would you ask of their staff in order to evaluate the potential acquisition? (5)**

Main thing here is to realise that practically time would be of the essence so you'd have to ask some penetrating questions and wouldn't have a chance to fully verify the answers. Getting that fully right adds two marks. Otherwise ½ mark for each/any of:

- Describe your security processes?
- Show me some/all developer CVs
- How have you tested for vulnerabilities?
- How many security reports did you process last year? What happened to N of those?
- Show me the security part of the design documents for your main product?
- How do you generate random numbers/store keys?
- Who has access to your source code backups?
- How do you ensure source code integrity?

Question 2:

a) **Give an overview of the current situation with spam, including describing the reasons why spam is possible; the problems caused; currently deployed countermeasures and some of the methods spammers use to avoid those countermeasures. (15)**

3 marks for overall "goodness" of the answer, then marks from 3 for each of the point (why possible, problems caused, deployed counters, spammers actions). If they focus more on deployed counters that's ok, up to 6 marks with the others being marked from 2).

I'll just give specifics for the first one (why possible) where they should cover things like:

- Lack of authentication in SMTP opens the door
- Requirement for any-to-any messaging means we can't close the door fully
- Scaling of mail as an application means that no single fix can easily work everywhere
- The spammers have found financial incentives

b) **How might a digital signature like DKIM scheme provide an additional anti-spam countermeasure? What pitfalls might such a scheme bring with it? (5)**

Simple marks from 4 for describing DKIM & its pitfalls correctly/well with a bonus mark for saying being clear that DKIM is mainly useful for MTA signing and verifying.

c) **Invent a new way to get spam to someone's desktop. (5)**

Straight marks from 5 for inventiveness.

Question 3:

You are asked to design a secure method for backing up large sets of files (e.g. audio libraries/"My Pictures"/entire filesystems). As part of this you need

a secure connection which, in turn requires some form of key management (e.g. TLS, Kerberos, IPSec/IKE).

a) **Describe in detail how your selected key management scheme works (10)**

This is really standard stuff so I'll just mention a couple of things that'd be needed to get 7+. Otherwise these are simply marked from 10. For TLS (which almost all of them will pick) the level of description for a really good score is essentially of the handshake protocol incl. certificates are handled therein. The issue with how only root CAs can be nominated for client-authentication should be mentioned. How CRLs and OCSP fit in should be mentioned. How DNS names fit into certs should be mentioned. The application protocol should be described (not doing so, means marks from 8).

b) **Describe how you would integrate use of this scheme into the overall backup application. (5)**

Presumably they'd have a server to which I can send backups over the secure link, and/or a server-server protocol for syncing up multiple backup servers. Maybe also a restoration protocol. Basic marks from 5 for a sensible description here. Important to be clear that mutual authentication is used when needed (easy to go wrong with TLS there).

c) **What performance problems would you expect to encounter using this scheme? (5)**

E.g. for TLS, they should not establish a new session for every file to be backed up, but need some kind of application layer protocol instead, at leas for small files. They should ensure that any required infrastructure (e.g. PKI to check client certs; ActiveDirectory if Kerberos on Windows) is sufficiently performant. The backup servers would probably need at least an option for h/w crytpo.

d) **What reliability/resilience problems would you expect to encounter using this scheme? (5)**

The gotcha one is restoring stuff that's needed for the system itself, e.g. accidentally putting back an old key pair. Bonus of 2 for getting that. Otherwise fairly typical things with connections being broken after half a filesystem has been backed up.