UNIVERSITY OF DUBLIN

TRINITY COLLEGE

FACULTY OF ENGINEERING, MATHEMATICS & SCIENCES

SCHOOL OF COMPUTER SCIENCE & STATISTICS

MSc in Computer Science **CS7053**	Hilary Term 2012

Security of Networks and Distributed Systems

EXAM SOLUTIONS

Date	**Location**	**Time**
XX April 2012	**XXXX**	**XX**

Dr. Stephen Farrell

Instructions to Candidates

Please attempt 3 questions.
All questions carry equal marks.

EXAM SOLUTIONS

EXAM SOLUTIONS

Question text is in italics below.
`Answer outlines are like this.`

Question 1. (33 marks)

A manufacturing company that are setting up a new web site to sell electronic components direct contracts you, as a security consultant, to carry out a risk analysis for the site and the associated payment and other processes. Previously the company has only dealt with distributors and never directly with end-users. Their goal is to out-source as much as possible of the work including web hosting, payments, the logistics for handling shipping of the products and customer service. The main product is a component that will be used in medical devices so a high level of assurance is required that processes are documented and followed. The company expect to sell thousands of devices per month. You can make any reasonable assumptions about how the web site works, but do make those clear in your answer.

The student should take proper account of the context – healthcare, a s/w dev company etc. The main point is to produce a reasonable process that approximates what might really be used.

(a) Describe the most relevant risks (at least 5) you see, including consideration of their impact and likelihood of occurrence. (18 marks)

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 be take any value without losing marks, but for something odd (e.g. if they considered DoS 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 3 points for each good one and with 3 more for overall goodness. Possible risks would include:

- Denial-of-Service attacks on the site
- Loss of logs and tracking information (accidental or not) needed because of the medical device aspect
- Leaking of customer personally identifying data especially medical or payment information
- Hackers breaking in to or defacing the site
- Abuse of customer support blogs, forums etc. for malware distribution or C&C
- Hosting site staff or other tenants abusing the web infrastructure from within
- Cloud-providers monitoring site traffic and data for their own benefit or for the benefit of competitors or foreign governments
- Staff from out-sourced providers (e.g. payments processors, customer service) hacking into the system
- Customer service staff working for competitors
- Manufacturers staff faking orders and hiding that
- Payment processors not reporting all payments

- If the device technology were dual-use, then orders from e.g. UN embargoed countries
- etc. etc.

(b) Describe the countermeasures (which may be physical or logical) you would recommend for the 3 highest priority risks and how deploying those countermeasures affects the overall risk analysis. (10)

Mostly fairly obvious. Marking is 3 points for each with one more for overall goodness. I'll just use the first example above:

DoS prevention could involve contracting with a security provider to monitor site traffic levels and to be able to spin up additional cloud instances in the event that a DoS attack is launched; ensuring that there as few single points of failure as possible (e.g. main site in a co-lo with ability to spin up EC2 instances as needed); maintaining a “lab” site where OS and application patches are frequently deployed and regularly porting that to the live site after testing; occasionally hiring pen-testers to attempt to DoS the site as a test.

The effect of all this would be to also make hacking/defacing attempts harder but with the possible new risk of the security provider leaking sensitive or customer data to which they need access (either to the public or to competitors). There is also an opex and capex cost associated with this countermeasure.

(c) How and when should the company re-evaluate the security of their site after it has gone live? (5)

Marking is straight from 5. When: Probably within weeks of the initial start and annually thereafter. How: carry out a design review to ensure deployment is still what you'd pick now and re-design as needed; hire pen-testers and perhaps security consultants who do the ISO 17799 game or similar or a medical specific variant (not that that exists today;-)

Question 2. (33 marks)

(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, including a description of how that security protocol is used by some real application. (15)

Marks-from-10 for a good description of the scheme, with e.g. the TLS handshake and application layer properly described. 5 marks for properly describing a real use case such as IMAP/TLS. If they describe HTTP/TLS then they need to get the CONNECT part correct. Extra marks for e.g. describing TLS MITM products, load-balancers that terminate TLS etc.

(b) What are the main potential Denial-of-Service (DoS) attack vectors that are created via the use of your chosen protocol? Describe those and potential countermeasures. (10)

Marks from 6 distributed evenly depending how many DoS-vectors they discuss, with 4 for overall goodness. Better if they identify asymmetric DoS vectors where the attacker gets a better advantage.

Most of the DoS vectors will be down to CPU consumption or state maintenance or due to extra round-trips and are fairly obvious, e.g. RSA private key operations in TLS servers. Some are more subtle, such as setting up a bad HTTP/TLS server, attracting victim clients who you then use (via OCSP responses) as the source for the actual DoS on the real target (the supposed OCSP responder). Holding half-open TLS sessions etc. can also be included. Countermeasures are mainly robust implementation and testing and provisioning appropriately with maybe use of hardware crypto modules in (front of) server farms and/or ability to spin up additional cloud instances.

(c) Describe any side-channel (e.g. timing, power) attacks might be attempted against a naïve implementation of your chosen protocol? (8)

Timing attacks and side-channels like Bleichenbacher based on formatting and oracles are what's called for here. Straight marks from 8 for this. Extra bonus if someone knows about cache-misses.

Question 3. (33 marks)

You are asked to design the security subsystem of a federated system for medical researchers in various research institutions (universities, hospitals) to use to interact with health research data sources for example national cancer registries, hospital patient records and other large data-sets. The data-sets are also owned and operated by research institutions and government, but contain highly sensitive health-care records including personally identifying information. The system should allow researchers in any institution to register and be granted access to only specific data relevant to their research. There are a set of special users ("approvers") who must manually approve new registrations. When a researcher issues a request for data, it will typically be necessary to filter the data so that only results that the researcher is allowed to see will be returned. For example a researcher might ask for the location and patient records of everyone in a large area who suffered from a particular disease, was under 45 years of age and who had a successful treatment. That query might be sent to multiple data-set holders, each of which runs its own system that decides what response to return. Assume there are approximately 100 data-sets, 10,000 researchers and 100 "approvers" all of whom are distributed across a single country. Ideally, the researcher will in the end see a collated form of all results returned.

(a) Outline the overall design for such a system (include a network diagram) and describe the security requirements you would propose that the system must meet. (10)

This should be a fairly straightforward web-like distributed system with federated authentication servers, access control enforcement at each data-set site and a special subsystem for registration handling. They should probably assume a VPN of sorts, maybe based on TLS rather than IPsec for this but even better if both options are available. There would need to be some middle-ware for filtering the data sets and handling queries in an application-specific way. Marks from 6 for the description and out of 4 for a good diagram that explains stuff well.

(b) Describe, in detail, the security solution you would propose to meet those requirements. (15)

This needs to cover authentication (federated, maybe using PKI or Kerberos locally or eduroam like); access control (probably a SAML based thing or Shibboleth or maybe Oauth) and with all links over some form of protected tunnel (TLS or IPsec). Audit should be mentioned. The registration subsystem would probably be web-based and there would need to be some sysadmins who can set that up. Marks from 5 for each of authentication and authorization description and 5 for overall goodness.

(c) Researchers are competitive too. Describe the various ways in which you, as a dishonest highly-competitive researcher, would attempt to abuse or game the system so as to make use of others work for your own benefit. (8)

Straight marks from 8 for sneakiness. Good if they remember to hide their tracks too. Some ideas:

- Bribery – get a sysadmin or data-set on your side to give you everything
- Steal someone else's credentials and mess about as them to see what's there
- Attack someone else's reputation
- Hack in to another researcher's laptop and monitor them from outside the system
- Hack some of the system authentication servers
- Get yourself setup as an approver and give yourself access to everything, better to socially engineer another approver to do that for a glove-puppet account you've set up so you don't get caught so easily

Question 4. (33 marks)

(a) Describe three significant security issues with the Domain Name System (DNS) and say if those are mitigated via the use of DNS security (DNSSEC). (8)

2 marks for each plus two for overall goodness. Idea is to show they get how DNS without DNSSEC is vulnerable. Possible vulnerabilities to choose include:

- Hacked caching resolver (e.g. on home router, in hotspot DNS server) as part of a bigger MITM
- DNS poisoning via racing and guessing fields
- Squatting (not mitigated)
- Cousin-domains, e.g. paypa1 (not mitigated)
- Hack a registrar
- DoS the DNS root
- Hack the authoritative DNS server for a domain
- Hack an end-host and mess with /etc/hosts or other local naming

(b) Describe the architecture and key management hierarchy of DNSSEC (15)

5 for arch; 5 for key hierarchy and 5 for overall goodness. This is a straightforward “do they know it” part of the question; they should cover all the basics as taught in class

(c) How will the deployment of DNSSEC affect end-hosts and applications running on the Internet and the management operations of registries and registrars? (10)

4 marks for how well they cover apps; 2 each for registrars and registries ops; 2 for overall goodness; points that could be made

- End-hosts will need to have trust points for the DNS root for their resolvers and will need to know DNSSEC
- Some applications will need to include their own resolver and cache in order to be sure that DNSSEC was used (e.g. a TLS implementation in a browser using DANE). Maybe that'll be an interim measure, maybe long term.
- Applications will need to start using some kind of API to tell them if names have been resolved securely.
- Middleboxes (e.g. home gateways) will need to pass DNSSEC results without messing with stuff.
- Registrars will need to include DNSSEC in their “create a domain” Uis and figure out how (or if) to charge for that.
- Registries and authoritative servers will need to do key management including roll-overs and will need to figure out validity periods for signatures (RRsig duration).
- As above for DNS within enterprises.
- ...