COMPSCI 314 S2 T 07 Assignment 3

Department of Computer Science
The University of Auckland

V1.0 posted 20 September 2007
V1.2 posted 28 September 2007 (changes shown in red)

Due 9:00am, Friday 5 October 2007
in https://adb.ec.auckland.ac.nz/adb/

- This assignment will contribute 5%/(15%+15%) = 16.67% to your coursework mark, and 5% to your overall course mark.
- There are 30 marks available on "regular" questions, and 3 bonus marks are available on very difficult questions.
- Bonus marks will increase the total marks of any student who is not awarded all 30 marks from the regular questions. Bonus marks will not cause any student's total marks on this assignment to exceed 30.
- No marks will be awarded if you merely state a correct answer. To obtain full credit, your script must *clearly* explain *why* your answer is correct.
- Plagiarism will not be tolerated. Your explanations must be in your own words.
- If you require additional information in order to answer a problem, you should briefly explain why this information is necessary and why your assumptions about the "missing values" or "missing facts" are reasonable.
- You may submit your assignment either in PDF format (preferred) or in MS Word.

Q1. According to Shay, "A virus is a collection of instructions attached to an executable file that does something the original executable file was not designed to do."

a. What security property of the executable file is violated when it is infected by a virus (according to Shay's definition)? Explain briefly. **[2 marks]**

b. Which security properties of a computer system might be violated, if it executes a file which has been infected by a virus? Explain briefly. To receive credit your answer must discuss all three of the basic "CIA" properties. **[3 marks]**

Q2. Shay describes the Internet worm as follows.

> "In November 1988 a Cornell graduate student released a worm into the Internet, which invaded thousands of Sun 3 and VAX computers ... This worm was of the so-called harmless variety; it did not damage any information or give away any of the secret passwords it uncovered.
>
> "On the other hand, it was a serious breach of security. It replicated quickly throughout the Internet, clogging communications and forcing many systems to be shut down. ...
>
> "The worm itself was written in C and attacked UNIX systems through flaws in the software. ... In one approach, it used a utility called **fingerd** that allows

one user to obtain information about other users. ... The flaw that was exploited was that the fingerd program's input command (the C language `gets` command) did not check for buffer overflow. Consequently, a worm running on a remote machine could connect to the fingerd program and send a specially constructed message that overflowed the fingerd program's input buffer.

"... Because of the overflow, ... when fingerd finished, ... the worm was now connected to the shell. From that point the worm communicated with the shell and eventually sent a copy of itself, thus infecting the new machine. The worm then proceeded to inspect system files, looking for connections to other machines it could infect.

"It also attacked a password file trying to decipher user passwords. Deciphering a password allowed the worm to attack other computers where that user had accounts. ..."

a. Did the author of the internet worm (as described in the quoted material above) violate the confidentiality, integrity, or availability of the fingerd utility? Explain briefly. **[2 marks]**

b. Did the author of the internet worm (as described in the quoted material above) violate the confidentiality, integrity, or availability of any file? Explain briefly. **[2 marks]**

c. Assume, for the moment, that the internet worm did *not* modify any file on any Unix filesystem, and that it read only files which could be legitimately read by any authorised user of that system. Under this assumption, are your answers to the preceding two questions (2a and 2b) still correct? Explain briefly. **[1 marks]**

d. Did the internet worm (as described in the quoted material above) mount an interception, modification, interruption, or fabrication attack on the legitimate messages carried on the internet? When answering this question, you should assume that the Cornell graduate student who released this worm was authorised to send internet messages (such as email) from their computer to any other user of the internet. **[1 bonus mark]**

Q3. Consider the following regulation. "Users shall... use only the login name(s) assigned to you by the University and shall not allow any other person to use your login name(s) to access one of the Universities' computer systems without the express permission of the Director of that system."

a. Which of the five "security functions" defined in set #5 of your lecture slides are addressed by this regulation? Your answer should briefly explain how each of these functions is addressed.

b. Which of the five "security functions" are *not* addressed by this regulation? Your answer should briefly explain a reasonable way in which each of these functions might be addressed, in a more extensive set of regulations regarding the use of login names.

Total for these two questions: **[5 marks]**

Note: our department's complete regulations are published at http://www.cs.auckland.ac.nz/administration/policies/ComputerScienceComputingServices.pdf.

Q4. Shay describes the TLS and SSL protocols at pages 320-322 as a seven-step process.

1. The client sends information to the server. The information includes ... a list of key exchange algorithms ... (including) RSA, Diffie-Hellman, and Fortezza. ...
2. The server sends a ... key exchange specification ... chosen from among those the client suggested. ... The server also sends some randomly generated data and its certificate. ...
3. ... the client ... must validate the certificate and authenticate the server... The client performs the following steps. A problem in any step causes an alert to be issued to the user. All steps must be completed to go on.
    i. Compares today's date with the issue and expiration dates in the certificate. If today's date is not in that range, the certificate is not valid.
    ii. Checks to determine whether the CA that issued the certificate is in the list of trusted CAs.
    iii. ... [verifies the] digital signature [on the certificate]. Two digest algorithms, SHA-1 and MD5, are used. If a security breach is found in one, the other provides an extra measure of security. ... [To verify these signatures, the client accesses] the CA's public key and applies it to the digital signature to get the original digest value ... and determines whether it is the correct digest value. ... these keys are public knowledge and, in fact, are stored along with the list of CAs. ... [In most browsers, you can view] a list of CAs, ... [if you] select any one of them and click View, ... details tab, ... [you will see its] Public Key ...
    iv. Compares the domain name in the certificate with the domain name of the server. ...
4. The client creates a *pre-master secret* (a 48-byte sequence), encrypts it using the servers' public key, and sends it to the server. The client will use the pre-master secret to generate a symmetric encryption key for the secure session. The server receives the pre-master secret, decrypts it using its private key, and does similar calculations to generate the key.
5. If required, the server may authenticate the client. It's a process similar to authenticating the server, and we won't go into detail here.
6. Both client and server use the pre-master secret to generate a *master secret.* To calculate the master secret, the client feeds its randomly generated data, the randomly generated data it received from the server (recall steps 1 and 2), and the pre-master secret into hash routines that generate a 48-byte sequence. The server proceeds analogously. Both client and server then feed the master secret into hash algorithms to eventually generate session keys used to encrypted ata that they exchange later in the session.
7. The client sends the server another message confirming the creation of the session key and indicates that all further messages will be encrypted using that key ... The server sends analogous information to the client. Once both the client and the server receive these last messages, the secure session is established and secure communications ... begin.

a. What message(s) are sent in step 4 on the previous page, if the preceding messages were

   1. C → S : (E_1, E_2, E_3, ...) ... [a list of key-exchange algorithms]
   2. S → C : (E_S, R, $Cert_S$) [a key-exchange algorithm, a random number, and the server's certificate. The certificate contains the server's public key S_P.]
   3. [The client validates $Cert_S$. If the certificate is invalid, the protocol aborts.]
   4. ??

   To receive full marks, your notation for the message(s) of step 4 should be consistent with what I have written for steps 1-3. You should also provide a brief comment in square brackets. **[2 marks]**

b. In slide #19 of lecture set #5, a protocol for "user authentication" was shown. Would that protocol be appropriate for use in step 5 of the SSL protocol (as described by Shay)? Explain. **[1 bonus mark]**

c. Use a browser to examine the certificate offered by the SSL server at https://adb.ec.auckland.ac.nz/adb/. What is the date on this certificate? What CA signed this certificate? What is the domain name on the certificate? Did your browser advise you to trust this certificate? Do you think this advice is appropriate? Explain. **[2 marks]**

d. Use a browser to examine the certificate offered by the SSL server at https://jobhound.cs.auckland.ac.nz/index-s.php. Did your browser advise you to trust this certificate? Do you think this advice is appropriate? Explain. **[1 mark]**

Q5. Some specifications for the USRobotics 24 Port 10/100 Mbps Switch and the USRobotics 8 Port 10/100 Ethernet Switching Hub were given in lecture set #6.

a. Consider an application where minimum-length 100 Mbps Ethernet packets are being sent continuously from one station to another station. If these two stations are on the same link, and if no other stations were transmitting on that link, approximately how many packets per second would be transferred between these two stations? **[2 marks]**

b. If a station on one port of the USRobotics 24-port switch were transmitting minimum-length packets continuously to a station on another port of this switch, and if both stations have 100 Mbps Ethernet cards, approximately how many packets per second would be transferred? **[2 marks]**

c. If a station on one port of the USRobotics 8-port switching hub were transmitting minimum-length packets continuously to a station on another port of this switching hub, and if both stations have 100 Mbps Ethernet cards, approximately how many packets per second would be transferred? **[1 mark]**

Q6. Slide 18 of lecture set #6 shows a forwarding database for what Halsall calls a bridging hub.

a. What would Shay call this device? **[1 mark]**

b. If station 16 was disconnected from this system, what would happen to its entry in this forwarding database? When answering this question, you should assume that this bridging hub uses the "transparent bridge" algorithm described in lecture set #6. **[1 mark]**

c. If stations 1 and 9 are swapped, so that station 1 is on the right-hand repeater hub and station 9 is on the left-hand repeater hub, how long might it take for the bridging hub to "learn" their new locations? Explain briefly. **[2 marks]**

d. If stations 1 and 9 are swapped, so that station 1 is on the right-hand repeater hub and station 9 is on the left-hand repeater hub, would the repeater hubs "learn" their new locations? Explain briefly. **[1 mark]**

e. Neither the USRobotics 24-port switch nor the 8-port switching hub are specified as being 802.1Q compliant. Referring to the last slide of lecture set #6, you'll find that an 802.1Q VLAN packet is distinguished from normal ethernet packets by having an 0x8100 in the type/length field of 802.3. What do you suppose would happen if an 802.1Q VLAN packet is received on the input port of a USRobotics 24-port switch? What if it were received on the input port of a USRobotics 8-port switching hub? **[1 bonus mark]**
