Comments and Solution for Assignment 3

1. **(4) X.509 PKI**
   The purpose of this assignment is to help you to understand the hierarchical system of public key management employed in modern commercial Web infrastructure.
   Pick five public key certificates of **different certificate authorities** (CA) that came preinstalled with the Web browser on the computer of one of your group members. For each certificate write an explanation to the following questions:
   1. What business does the certificate owner do?
   2. For which purposes can your browser trust this certificate?
   3. Which organization issued and signed this certificate?
   4. Does your group trust the signature? Explain why or why not?
   5. Are their other certificates in the same browser that are signed by the key from this certificate?
   6. What is needed for an organization to get a certificate issued by this CA?

Sample solution:

1. (The following certificates are obtained in Internet Explorer 7.0.5730.11 with the Root Certificate Update (KB931125) from Microsoft installed)

Root CA #1: Hongkong Post Root CA

Business	Provider of postal services and digital certificate issuing services to entities in Hong Kong
Trusted purposes	Server authentication, client authentication, secure email, time stamping, 1.3.6.1.5.5.7.3.9
Issuing CA	Hongkong Post Root CA (owned by Hongkong Post)
Do we trust the signature?	Yes. The browser does not detect any problems with the certificate, and the CA is owned by the Hong Kong government.
Other certificates from same CA?	None.
Procedures to getting certificate	The applicant must be an entity (person or organization) in Hong Kong to apply for a certificate. The applicant needs to submit a completed application form, along with the required documents (for proof of identity) and the appropriate application fees, in person to any Hong Kong Post office. The certificate authority then reviews each application to ensure its authenticity. Upon approval, the CA sends out the PIN (i.e. password) and the certificate to the applicant separately via mail. Application procedures differ between different types of certificates. Details can be found at http://www.hongkongpost.gov.hk/product/ecert/apply/index.html.

Root CA #2: VeriSign Trust Network

Business	Provider of information, communications, and security-related services. This includes SSL certificate issuance and managed PKI services.
Trusted purposes	Server authentication, client authentication, secure email, code signing
Issuing CA	VeriSign Trust Network (owned by VeriSign, Inc.)
Do we trust the signature?	Yes. The browser does not detect any problems with the certificate, and the CA is a well-known company in the certificate issuing business.
Other certificates from same CA?	None.
Procedures to getting certificate	First of all, the applicant needs to generate a Certificate Signing Request (CSR), which is a string generated by the applicant's web server software. Afterwards, the applicant goes to the VeriSign website and fills out an online application form. Upon validation and approval, VeriSign will email the certificate to the applicant. The detailed application procedures can be viewed at http://www.verisign.com/ssl/ssl-information-center/ssl-enrollment-process/index.html.

Root CA #3: thawte Primary Root CA

Business	thawte is a mainly engaged in the business of issuing SSL certificates, and is one of the leading global CAs.
Trusted purposes	Server authentication, client authentication, secure email, code signing
Issuing CA	thawte Primary Root CA (owned by thawte, Inc.)
Do we trust the signature?	Yes. The browser does not detect any problems with the certificate, and the CA is a well-known company in the certificate issuing business. Moreover, thawte CA is owned by VeriSign, another trusted company.
Other certificates from same CA?	None.
Procedures to getting certificate	Similar to the VeriSign application procedures, the applicant generates a CSR and completes an online form. The applicant also has to provide

	documentation proving his/her identity. After the application is approved, an email will be sent to the applicant. This email contains the link at which the newly generated certificate can be downloaded. The application procedures can be viewed at http://www.thawte.com/en/guides/pdf/enroll_ssl_eng.pdf.

Root CA #4: RSA Security 2048 V3

Business	Provider of security solutions for businesses. This includes, but not limited to, digital certificate issuance.
Trusted purposes	Server authentication, client authentication, secure email, code signing, time stamping
Issuing CA	RSA Security 2048 V3 (owned by RSA Security Inc.)
Do we trust the signature?	Yes. The browser does not detect any problems with the certificate, and the CA is a well-known company in the security field.
Other certificates from same CA?	None.
Procedures to getting certificate	There is no detailed documentation regarding the application process. Unlike the CAs mentioned above, the application process is not entirely online. The applicant would first have to go into a contractual agreement with RSA (presumably by contacting the sales team), after which he/she can then fill out the form at http://www.rsa.com/go/keon_root_signing_service/index.asp to request for a certificate.

Root CA #5: Visa eCommerce Root

Business	Association of financial institutions worldwide that offers a wide range of payment options, such as credit cards and stored value cards.
Trusted purposes	Server authentication, client authentication, secure email, 1.3.6.1.5.5.7.3.9
Issuing CA	Visa eCommerce Root (owned by Visa International Service Association)
Do we trust the signature?	Yes. The browser does not detect any problems with the certificate, and the CA is a well-known company.
Other certificates from same CA?	None.
Procedures to getting certificate	Only certain entities may obtain a certificate issued by this CA. These entities include member financial institutions, cardholders, merchants and Visa operating units. There is no available documentation regarding the application process.

Contributed by Tik Ning Cheung, Jeannie Li, and Henry Ng.

2. **(8) PGP**

This problem has both individual and group elements to it. Your group should turn in one write up answering each of the parts labeled [group], but all key pairs, emails, etc. should be created and sent individually.

1. Read Alma Whitten's paper, "Why Johnny Can't Encrypt."

2. Locate and install a fresh version of PGP or GPG. There are versions for Unix flavors, Windows, and Macintosh. http://www.pgpi.org/ may be of use.

3. Find the PGP public keys for as many of the EECE 412 teaching staff as you can. Part of your assignment is figuring out how to locate PGP keys. Searching the Internet for PGP key servers may be of help. But beware; there may be fake keys out there. . .

Here's what you do to submit your solution to this problem:
(2) (a) **[group] Reflections on Trust**. PGP's "web of trust" model allows users to "sign" each others' public keys. Suppose Alice signs Bob's key; what, in effect, is Alice declaring when she does this? Why is it useful for people to sign each other's keys? What precautions should one take before signing someone else's key, and why are these measures appropriate?

Sample solution:

2. a) When Alice signs Bob's key, she is declaring that she believes the public key she is signing does indeed belong to Bob.
This web of trust is useful because it is a decentralized method of verifying whether or not a given public key belongs to the user that it is claimed to belong to. If several trusted people sign a public key, then Alice can be fairly confident that the public key belongs to Bob. However, if the key is not signed by anyone, then Alice may be concerned that the public key belongs to someone other than Bob.
When an individual is signing a key he should use some form of authentication to ensure that the key belongs to its claimed owner, such as meeting the person face to face and checking their photo id. The individual must authenticate the key owner because if the individual signs a key that does not belong to the claimed owner, others may mistakenly trust the key. Ensuring that only authentic keys are signed maintains the integrity of the web of trust and thus it is paramount that keys are only signed when they are known to be authentic.

Contributed by Armin Bahramshahry, Hesam Ghasemi, Anish Mitra, and Vinayak Morada.

(3) (c) **[individual] Encrypting email**. Send an encrypted, signed email to the TA with the subject "PGP is fun". In the body of the message,
- Tell us what operating system and version of PGP you are using.
- Show us the public keys you found for the EECE 412 TA; PGP fingerprints are sufficient.
- In a few sentences, explain why you do or do not believe that these keys do indeed belong to the EECE 412 TA. If you do not trust a public key, explain what would convince you otherwise. Your mail should be protected with PGP such that the EECE 412 TA, and only the EECE 412 TA, can obtain the plaintext contents. You must also sign the mail with your private key. We will only accept your first message, so make sure to get it right the first time. Are you able to finish the assignment in fewer than 90 minutes as in Whitten's experiment? Remember to cite all your sources (books, manuals, friends, etc.).

Sample solution:

```
OS: Windows XP
PGP: PGP desktop 9.5.3

EECE 412 TA public key: (PGP fingerprints)
1911 BB31 1970 69D1 2E4E  0591 3886 0E65 C956 A623

I believe the keys do belong to Joy Zhang because the email domain -
ece.ubc.ca - is not a public accessible domain. I believe our EECE
department - ece.ubc.ca - has its policy on issueing email addresses to
its staff and duplicating or faking such addresses is less likely
possible. The key is also verified by PGP Global Directory Verification
Key.
```

Contributed by Byron Leung.

4. **(7) SSH**
This problem has both individual and group elements to it.

1. All member need first to install SSH on their personal computers and learn how to log in to ssh.ece.ubc.ca. ECE's Hot to page on SSH might be of help at this step.
2. Next, each group member should create a public-private key pair and configure their ssh environment on ssh.ece.ubc.ca to login at that machine using authentication based on public key cryptography. For this step, this tutorial on OpenSSH key management might be useful.
3. Finally, the group should pick one group member and set his or her SSH environment on ssh.ece.ubc.ca so that ALL the members of the group can log from their personal computers into ssh.ece.ubc.ca under the account of the chosen group member using authentication based on public key cryptography. Upon succesful completion of this task, screenshots (one per group member)---similar to the one below---of succefull logins under the account of the chosen group member should be created and inserted in the assignment document.

Sample solution:

4. For each group member, a public and private key pair is generated using `ssh-keygen` in the Linux/Unix environment. Specifically, the command "`ssh-keygen -t rsa`" was used to generate the keys using RSA public key encryption.

In order to log into an account using public key authentication, the public key portion of the key pairs must first be placed in the "`.ssh/authorized_keys`" directory of the target account. The account chosen by our group to experiment with was "`tncheung@ssh.ece.ubc.ca`". The public keys generated by other group members are uploaded to this account using the following command:

```
cat <location of the public key> | ssh tncheung@ssh.ece.ubc.ca 'cat
                    >> .ssh/authorized_keys'
```

The following screenshots show the group members logging into the account without using knowledge of the account's password.

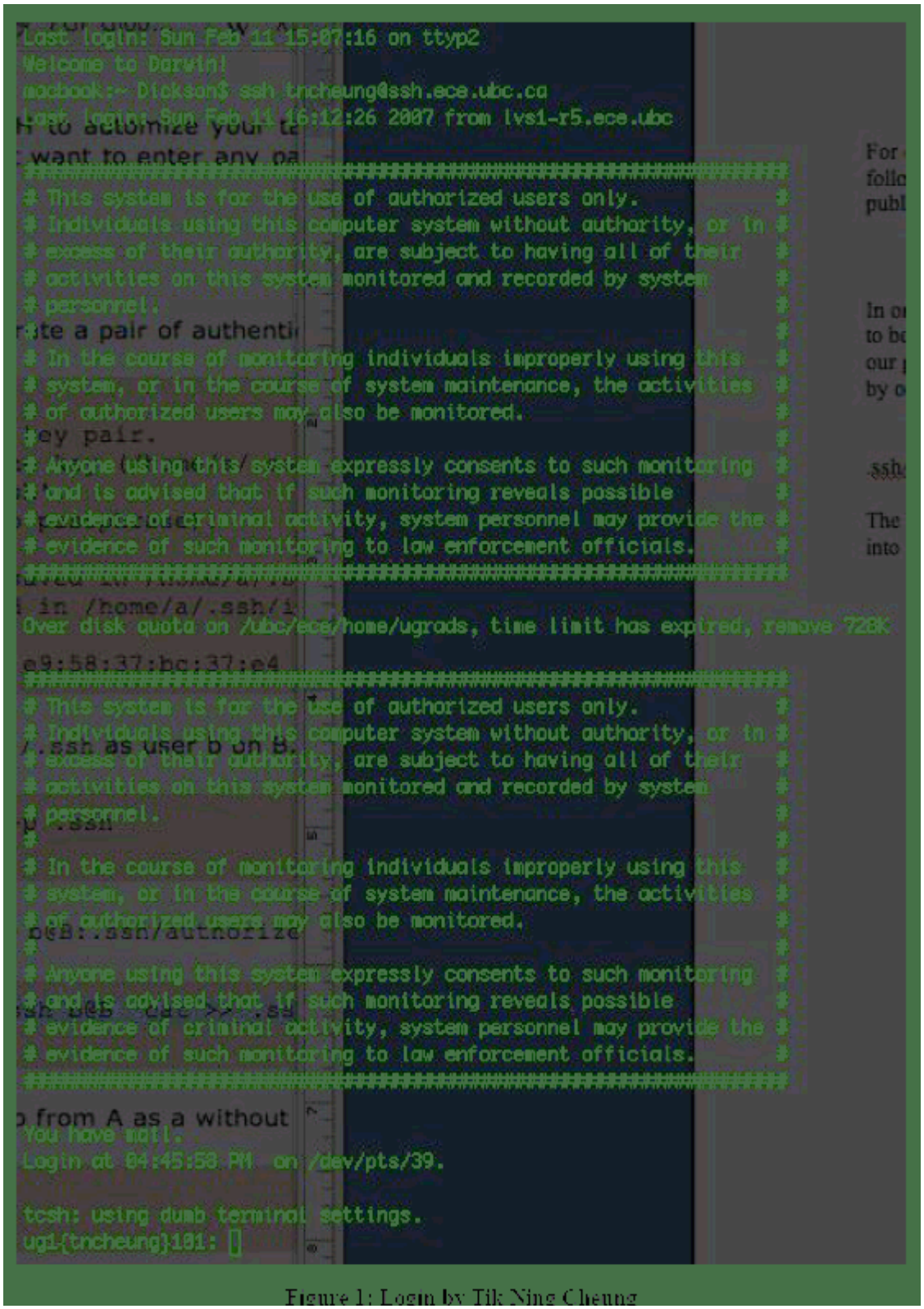

Figure 1: Login by Tik Ning Cheung

```
          ssh tncheung@ssh.ece.ubc.ca
Enter passphrase for key '/ubc/ece/home/ugrads/j/jeli/.ssh/id_rsa':
Last login: Sun Feb 11 16:07:13 2007 from lvsl-r5.ece.ubc

###############################################################
# This system is for the use of authorized users only.        #
# Individuals using this computer system without authority, or in #
# excess of their authority, are subject to having all of their   #
# activities on this system monitored and recorded by system      #
# personnel.                                                      #
#                                                                 #
# In the course of monitoring individuals improperly using this   #
# system, or in the course of system maintenance, the activities  #
# of authorized users may also be monitored.                      #
#                                                                 #
# Anyone using this system expressly consents to such monitoring  #
# and is advised that if such monitoring reveals possible         #
# evidence of criminal activity, system personnel may provide the #
# evidence of such monitoring to law enforcement officials.       #
###############################################################

Over disk quota on /ubc/ece/home/ugrads, time limit has expired, remove 728k

###############################################################
# This system is for the use of authorized users only.        #
# Individuals using this computer system without authority, or in #
# excess of their authority, are subject to having all of their   #
# activities on this system monitored and recorded by system      #
# personnel.                                                      #
#                                                                 #
# In the course of monitoring individuals improperly using this   #
# system, or in the course of system maintenance, the activities  #
# of authorized users may also be monitored.                      #
#                                                                 #
# Anyone using this system expressly consents to such monitoring  #
# and is advised that if such monitoring reveals possible         #
# evidence of criminal activity, system personnel may provide the #
# evidence of such monitoring to law enforcement officials.       #
###############################################################

You have mail.
Login at 04:12:27 PM  on /dev/pts/7.

ugl{tncheung}101:
```

Figure 2: Login by Jeannie Li

Figure 3: Login by Henry Ng

Contributed by Tik Ning Cheung, Jeannie Li, and Henry Ng.

5. **(10)** Compare and contrast key management in X.509 PKI, PGP, PGP alternative, and SSH based on your experience with them. Limit your answer to one page.

In the X.509 PKI, a certification authority (CA) issues certificates that bind a public key to a 'distinguished name'. The primary difference between PGP and X.509 PKI is that instead of anyone being able to sign another person's public key, in X.509 only specific CAs are authorized to provide an organization or an individual with a certificate. This is a more trustworthy way of enforcing public key authenticity because the CAs normally conduct strict background checks on the organizations requesting certificates before issuing one to them. The disadvantage of this method is that it can be quite expensive and time consuming to obtain a certificate and therefore we feel this method is more suited to meet the needs of organizations instead of individuals.

PGP is a method of encryption that uses asymmetric cryptography to allow users to send encrypted messages to one another. An advantage for key management using PGP is that a user, such as Bob, can publish his public key openly, and individuals who want to send him private messages can do so using this public key. The use of a public/private key pair makes distribution very simple. The problem, however, is that an attacker can publish a public key, while claiming that he is Bob. PGP tries to circumvent this attack by using its web of trust policy. Ideally, the web of trust is an effective method of ensuring that keys are authentic because it requires users to sign keys that the consider trustworthy; however, the web of trust is not fool proof and attackers can still publish public keys that are not their own.

PGP alternative method is different from PGP, because the messages are not encrypted and signed. Instead, the hash of the message is posted on a website, and the intended receiver calculates the hash of the message and checks with hash of the website. The disadvantage of this method is that if the actual message is not encrypted, therefore, if someone intercepts the message, that person can read the content of the message. As the result, it is not secure way of sending message, which contain sensitive data. On the other hand, it is an easy and inexpensive way of determining if the content of the message has been changed through transmission.

In SSH the ssh-keygen is used to generate the private and public key files on the client side. User of this system needs to move the generated public key (*.pub) to the server and add the new authorization key to the end of "~/.ssh/authorized_keys" as well as setting up the permissions for this file and directory. After this operation anyone who has the private key generated out of ssh-keygen operation can login as this user without requiring the password. In order to make this process more secure, a "passphrase" is used to encrypt and decrypt the private key file. Anyone who has the private key file and the passphrase can login as the user into the system. What is important about this type of private/public key generation is that the important operation (private/public key generation) is done on the client side and only the public key is transferred over the network. Also same private key and passphrase combination can be used to login into many different systems (based on user's setup and need).

Contributed by Armin Bahramshahry, Hesam Ghasemi, Anish Mitra, and Vinayak Morada.

Comments:

1. **Some group members use the same answer for individual questions.**
2. **Some group didn't include group member's names, please avoid that.**