SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1, 2014

Outline solutions for Week 9 tut for L7: Asymmetric Cryptography and PKI

QUESTION 1

Read through *Clause 12.3 Cryptographic Controls* of *AS27002:2006 Code of practice for information security management* to answer the following questions:

a) Why is the management of cryptographic keys such an important issue (See Clause 12.3.2 *Key management*)?
b) Explain which keys need protection, and what they need to be protected against, for:
   i. Symmetric ciphers
   ii. Asymmetric ciphers.
c) In each case, explain how this protection can be provided.
d) Briefly list the main issues a key management system must deal with.

(a) Key management is required to support the organization's use of cryptographic techniques. Any compromise or loss of keys may lead to a compromise of the confidentiality, integrity or availability of information assets protected by cryptographic means.
(b) Secret (symmetric) keys and asymmetric private keys need protection against unauthorised disclosure, and *<u>all keys</u>* require protection against modification and destruction.
(c) Cryptographic techniques can be used, including certificates to provide assurance that public keys have not been modified and symmetric encryption as in Kerberos to protect keys during distribution. Physical protection of equipment used to generate, store and archive keys should also be used.
(d) Main issues are listed in 12.3.2 (pp. 81-82) of 27002:2006. These include key generation, distribution, storage, updating, revoking, recovering, archiving, destroying and auditing.

QUESTION 2

Suppose a *symmetric* cipher is to be used to provide confidentiality for messages sent within an organization.

a) How many keys are required for two people to communicate confidentially using a *symmetric* cipher?
b) How many keys are required for five people to communicate confidentially using a *symmetric* cipher, such that any two can communicate securely?
c) Before encrypted messages can be sent, each communicating party must have a copy of the secret key. How can this key distribution be performed securely if *asymmetric* ciphers are not used?

(a) Using a symmetric cipher, for two people to communicate securely, one shared secret key is required.
(b) Using a symmetric cipher, for five people to communicate securely, so that any two can share confidential messages, ten shared secret keys are required.
Each of the five people needs keys to communicate with each of the other four people (5 x 4 = 20), but the key A uses to communicate with B is the same as the key B uses to communicate with A, so total number is 20 / 2 = 10.

(c) Key distribution could be performed over a different, secure channel, perhaps ahead of the need to communicate over the insecure channel (predistribution). Alternatively, if there is a trusted third party, they can perform the role of a key server – in a similar manner to Kerberos.

QUESTION 3

The Diffie-Hellman key agreement algorithm allows two entities to establish a shared secret key without requiring the use of a secure channel. That is, they can establish a shared secret key even though the messages they send may be observed by others.

a) What sort of mathematics is required to perform Diffie-Hellman key agreement?

b) One problem with this scheme is that each entity has no assurance about the identity of the entity they are communicating with. What sort of attack is possible as a result of this problem, and what impact does this have on the security of subsequent communications?

a) The mathematics used is modular exponentiation: integer exponentiation over a finite set of integers. The modulus is a prime number.
b) Because there is no authentication of the communicating parties, a man-in-the-middle attack is possible. Carol can pretend to Alice that she is Bob, and pretend to Bob that she is Alice. Then she can establish keys to use with each of them. The messages that Alice thinks she is sending securely to Bob are in fact going to Carol (pretending to be Bob) who can read them and forward them on to Bob (even modify them if she wants to). Bob receives the messages he thinks are from Alice (but they are really from Carol). The situation is similar for messages sent from Bob intended for Alice. The impact on the security of the communications is that they are not really secure at all. Carol has access to the content (so confidentiality of communications between Alice and Bob is breached) and can even modify it (integrity breach).

QUESTION 4

Alice wants to send a confidential message to Bob. They do not have an existing shared secret key. Suppose that Alice and Bob agree to use an *asymmetric* cipher (say, RSA). Bob has a public key K_{Bpub} and the associated private key K_{Bpriv}.

a) What should Bob do with each of these keys to permit people to send confidential messages to him?

b) Outline the set of steps that Alice must follow to encrypt a message to send to Bob.

c) Outline the set of steps that Bob must follow to decrypt ciphertext received from Alice.

a) **Bob should keep his private key K_{Bpriv} secret. He should make his public key K_{Bpub} available to others.**

b) **Encryption:**

1. **Alice prepares the message M, which may include coding the message as an integer (or a series of integers, depends on the size of the message).**
2. **Alice encrypts the message using the agreed asymmetric cipher encryption algorithm (RSA) and the key K_{Bpub}, to produce the ciphertext C, where C = E(M,K_{Bpub}).**
3. **Alice transmits the ciphertext C to Bob.**

c) Decryption:

1. **Bob receives the ciphertext C.**

2. **Bob decrypts the ciphertext using the agreed asymmetric cipher decryption algorithm (RSA) and the key K_{Bpriv}, to recover the message M, where M = D(C;K_{Bpriv}).**
3. **Bob decodes the message, if necessary, to recover the plaintext.**

QUESTION 5

Alice wants to send a message and an associated digital signature to Bob. Alice has a public key K_{Apub} and the associated private key K_{Apriv}. Similarly, Bob has a public key K_{Bpub}, and the associated private key K_{Bpriv}. Explain the cryptographic steps necessary for:

a) Alice to generate her digital signature, and
b) Bob to verify Alice's digital signature.
c) Repeat parts a) and b) if an additional step, hashing the message, is included in the digital signature formation and verification in order to reduce the computational overhead.
d) Digital signatures provide a means to obtain non-repudiation.
   i. What is non-repudiation?
   ii. Why is this important for e-commerce?
   iii. Why is symmetric cryptography alone unable to provide non-repudiation?

a) Alice's signature generation:

i. **Alice prepares message M (which may include coding the message).**
ii. **Alice inputs the message and Alice's private key to the signature creation algorithm to obtain SigA(M).**
iii. **Alice sends SigA(M) and M to Bob.**

b) Bob performing signature verification:

i. **Bob receives message M and claimed signature SigA(M).**
ii. **Bob inputs SigA(M), M and Alice's public key to the signature verification algorithm.**
iii. **If the output is Yes then Bob can be assured that SigA(M) is the signature on message M formed by Alice. If it is NO, then Bob has noassurance that the signature on the message was formed by Alice. It may be a different message or a signature formed by someone else.**

c) Alice's signature generation: similar to a) except the message is hashed, and the signature performed on the hash of the message.

Bob performing signature verification: similar to b) except Bob hashes the message he receives, and inputs the signature and the hash of the message into the verification process. If the verification process output is

YES then Bob can be assured that the message he received has the same hash value as the message M signed by Alice, and if the hash function is collision resistant then it is highly likely it was the message Alice sent. If it is

NO then, as before, Bob has no assurance that the signature on the message was formed by Alice. It may be either a different message (so the hash would be different) or the signature was formed by someone else (so Alice's public key won't work to verify it).

d) Non-repudiation:

i. **is a security service that ensures that users cannot falsely deny an action has occurred.**
ii. **It is useful if it necessary to resolve a dispute about some action that has occurred, for example whether a contract was signed or a transaction authorised. Digital signatures provide authentication of the message sender, integrity and non-repudiation, so that is useful for e-commerce.**
iii. **Symmetric crypto cannot provide non-repudiation as message authentication using a MAC only shows that one of the parties who**

knows the shared secret key formed the MAC (for example shopper and merchant), and a third party (judge) will not be able to decide which of those two parties performed the action.

QUESTION 6

AUSCERT use PGP to create message signatures for their Security Bulletins and email announcements. You will need to access AusCERT website to answer the following questions. Locate:

a) The AusCERT PGP key and use this to answer the following questions:

  i. When did AusCERT's current PGP key come into effect?
  ii. What can this key be used for?
  iii. How can people get a copy of AusCERT's new PGP key?
  iv. When does this key expire?

b) **ESB 2013.0408** and use this to answer the following questions.

  i. There are two signatures included in this bulletin (Scroll down, they are near the bottom). Who created these signatures?
  ii. What can the signatures be used for (why are they included in the Bulletin)?
  iii. Does either signature involve the use a hash function? If so, which hash function?

c) In order to verify these signatures, the appropriate keys must be located. AusCERT's public key was located in (a). Locate the other public key relevant to this message and record the following details:

  i. Key length
  ii. Key fingerprint

a) AusCERTS PGP Public key

  i. AusCERT's new PGP key comes into effect on 21 June 2013.
  ii. AusCERT will use their private key for signing Bulletins, and subscribers can use this public key for validating AusCERT communications (emails and Security bulletins).
  iii. A copy of AusCERT's current public key is available from the AusCERT website, follow links: (Home -> About AusCERT -> AusCERT Public Key) or go to http://www.auscert.org.au/render.html?it=1967:
  iv. The 4096R indicates this is a 4096 bit public key to use with the RSA signature algorithm. The first few lines are:

```
mQINBFHD3jEBEAC+kZH4nTBvsk0eLXGzkuj7I5ssMgd0gPVTUII6AQMsbg6LCgfl
BXeU6jb+YaKi1aZiGSM9a5zxPQTkzKkRzv7WHmn9/ZNiALT/TFUGoOL6zWAEZQUX
vfQJ1ZEy7iEoN378r6COUb+2dbcELSzTAOcEr89jR2OJ0kHuTomqlZVmv37Oa7rl
W3CTVQhKKIjibj2tl0rRI7tGPoqbFf2l3BAUUE1VRkOyN+kqvWlJyjzGHrVz33jf
TCTPEvvBhkQotu/N4uLLJoBUwdA27M4x505wo3wKNO/BOGWGJwpL4Ywe/BcjpSM+
```

  v. This key expires on 21 June 2015.

b) ESB2013.0408:

  i. There are two signatures in the bulletin. One is a signature by Apple (further into the middle of the Bulletin) it was at the end of their original message, and has been incorporated into the AUSCERT ESB. The signature right at the end of the message is created by AUSCERT.
  ii. The signatures can be used to verify that the message is from Apple (just the internal part) or AUSCERT (the whole bulletin) and has not been altered (That is, they authenticate the message sender and also provide message integrity assurance).
  iii. Both of the signatures use the SHA1 hash function.

iv. **The Apple Product security PGP public key used to sign the message (with an expiry date of May 14, 2014) is available from: https://ssl.apple.com/support/security/pgp/**
It is a 4096 bit RSA public key, and the Key Fingerprint is:
1B7E 5354 8C25 39C9 4083 72BF 6E68 C714 D026 1077

QUESTION 7

Suppose that Alice and Bob use an *asymmetric* cipher (say, RSA) to communicate confidentially. They have their public keys in a file that is available on the corporate network. Another employee, Carol, wants to know what they are communicating. Carol cannot break the RSA algorithm, but is able to access and alter the file containing their public keys.

a) How does altering the public keys help Carol to gain access to the confidential communications between Alice and Bob?
b) Which messages is Carol able to access?
c) Explain how a *digital certificate* be used to provide a solution to this problem.
d) How much trust can be placed in a digital certificate? Justify your answer.
e) Is a digital signature the same as a digital certificate? Justify your answer.
f) One of the services provided by AusCERT is Certification (of public keys). List the three types of certificates available from AusCERT.

a) When Carol replaces a public key (say Alice's public key) with a different key whose private key is known to her, this allows Carol to pretend to be Alice (for example, to read encrypted mail intended for Alice). Note that the private key that Alice (the real Alice) has is not the corresponding private key for the public key that Carol has posted as Alice's, so now Carol can read the mail intended for Alice, but Alice cannot. The situation is similar for Bob.
b) Carol will have access to all messages intended for Alice or Bob after she alters the public keys. The messages sent before this (using their real public keys) are not available to Carol.
c) A digital certificate is an electronic file that contains information identifying a particular entity (say, Alice) and also the public key belonging to that entity. The certificate binds a public key to an entity. The CA who issued the certificate (and signed it with a digital signature) is vouching for the information. The certificate provides a solution to the spoofing problem if it is issued by a recognised certification authority which has procedures in place to check identification details before providing certificates.
d) You can trust the information in the certificate (ID-public key binding) if you trust the issuing CA to have identified the certificate owner and you can verify the CA signature on the certificate. This means you need an authentic copy of the CA's public key.
e) No, a digital signature is not the same as a digital certificate. Alice's digital certificate will be *the same* each time she sends it, but her digital signature on a message *will differ* as the message content differs (or the hash of the message content, if hashing is used as part of the signature process). A digital certificate is a specific type of message signed by the CA.
f) Digital certificates offered by AusCERT are
  i. Server Certificates (for authenticating servers),
  ii. Personal Certificates (two levels: Standard and High, used for authenticating users, securing individual email, etc) and
  iii. Code-signing Certificates (for authenticating software that is distributed over the internet).

QUESTION 8

a) Describe the features of each of the following PKI trust models:
   i. Strict hierarchical PKI trust model
   ii. User-centric PKI model
   iii. Browser PKI model

b) Outline the relative advantages and disadvantages of each of these three models.

a) Features (See lecture slides 61 to 69).

i. The hierarchical model is highly regulated. A single root CA is the root of a tree, this provides certificates to intermediate CAs (nodes), who provide certificates to users (the leaves).

ii. The user-centric model is less structured. Connections are between users - any users can certify each other whenever they want to.

iii. The browser model consists of the preloaded certificates installed by the browser vendor, and Installed certificates are used as trusted "root" CA certificates for verifying incoming certificates. The browser user is trusting the browser vendor who supplied the installed certificates, rather than a root CA.

b) Advantages and Disadvantages

i. The hierarchical model is highly structured. The advantages of this are that it is very easy to find certification pathways, and it is suitable for use in highly structured organisations. This also scales well as size of organization size increases. The disadvantages are that it requires a single root CA, and that compromise of a node compromises everything below that point (single point of failure).

ii. The user-centric model is more anarchic - users can certify and trust any other users that they want to. Advantages include the simplicity of the model (at least for a small number of users) and the fact that it does not require expensive infrastructure to operate. However, the disadvantages are that the decisions on trust rely entirely on individual users' judgment. This may work well with technical users who are aware of the issues, but not the general public. It is not an appropriate model for trust-sensitive areas such as finance and government.

iii. Browser model advantage: Ease of use, root certificates form some starting points for trust. Disadvantages include limited certification path processing, and the list of trusted certificates being controlled by user - not well protected from modification attacks. Users tend to automatically accept incoming certificates that cannot be verified by the trusted certificates. They may even accept and install self-signed certificates. Cross certification and revocation are not well supported, and there is no formal legal agreement established between users and CAs.

QUESTION 9

Investigate the digital certificate issued to QUT Virtual. Using a browser log in to the QUT Virtual site. Click on the padlock icon (it may be crossed through in Firefox but you can still get the information) and obtain the certificate information (View Certificate). You will need to view the details of the certificate to answer some of these questions.

a) What is the purpose of this certificate?
b) Who is the certificate issued to?
c) Who is the certificate issued by?
d) What is the validity period for this certificate?
e) Which X.509 certificate version is used?
f) Which cryptographic algorithm is used to sign the certificate?

g) What type of public key algorithm is certified, and what is the key size?
h) What is the certification path back to the (browser) root CA?

The detailed values are not the most important thing here. The main thing is to get a feeling for what information is stored in the browser and observe the features of the browser PKI. You should find all of the answers to the questions above on the certificate.
(a) Purpose: ensures the identity of a remote computer (IE) or supports authentication for the site you are viewing. (Firefox)
(b) Issued to: qutvirtual2.qut.edu.au (you can find this on the certificate general tab)
(c) Issued by: AUSCERT Server CA.
(d) The validity date - from 22/07/2011 to 22/07/2014.
(e) The certificate version - V3 (find this on Details tab)
(f) The cryptographic scheme used for certificate signature - SHA1 with RSA encryption
(g) The type of public key algorithm certified and the key size. RSA, 2048 bits (h) Check certification path tab: from qutvirtual2 -> AusCERT Server CA -> UTN-UserFirst-Hardware -> AddTRUST External User CA

QUESTION 10
Investigate some of the other digital certificates you have stored. (For IE, you can check certificates through “tools' ‘Internet Options' ‘Content') Can you find any certificates which:

a) Have validity periods of less than one year
b) Have validity periods of more than five years?
c) Have already expired?
d) Are there any ‘untrusted' certificates listed (you may need to scroll across to find these)?
e) Suppose there have been some fraudulent certificates issued that are not currently listed by your browser as ‘untrusted'. What are the security implications for the browser model in this situation?

Again, the details are not the important part of the exercise and will vary across different installations. The important thing is to start looking at the certificates and see what information is provided.

a) Normally certificates issued to end users (which could be organisations) have lifetimes such from one to ten years. For example, the digital certificate issued for QUT Virtual has approximately a three year lifetime.
b) To find certificates with longer validity periods, check the certification path of the certificate issued to QUT Virtual. This was issued by a CA called AusCERT Server CA. The validity period of their certificate is just over ten years (from 2009 to 2020). You can also see that this CA is certified by the UTN-UserFirst-Hardware Certification Authority. That certificate is valid for 15 years (2005 to 2020). The root CA is a pre-installed certificate with a validity period from 2005 to 2020, and it is self signed (Issuer and Issued to fields are the same). It is common for Root CA's to have self signed certificates – who else can certify their key?
c) You can probably find CA intermediate certificates which have expired. Both IE and Firefox give some kind of warning when you open an expired certificate (they might tell you that the certificate has expired, or that the validity cannot be confirmed).
d) There are lots of untrusted or fraudulent certificates – your browser should have some certificates issued by Comodo and some DigiNotar certificates from 2011, and some TURKTRUST certs from 2012, among others.

e) **If there are certificates currently installed in your browser that are actually fraudulent, but your browser has not listed as untrusted, you (the user) will make trust decisions based on the apparent validity of the certificates. For example, you may consider a website as legitimate, when in fact the site is spoofed.**