SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1, 2014

Tutorial Questions for Lecture 7: 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.

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?

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?

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.

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?

QUESTION 6

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

a) The Auscert PGP public key (look under ‘About AusCERT’ and scroll down) 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 PGP key?
    iv. When does this key expire?
b) Security bulletin **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

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.

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 advantages and disadvantages of each of these three models.

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?

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 are 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?