University of Oslo
INF3510 Information Security
Spring 2018
Workshop Questions & Answers

Lecture 4: Key Management and PKI

Question 1

a. Why is the management of cryptographic keys such an important issue?
b. Three main key categories are: i) symmetric secret keys, ii) asymmetric public keys and iii) asymmetric private keys. Explain which type of security services/protections (i.e. confidentiality, integrity and authenticity) that is/are required for each key category.
c. Describe security mechanisms/methods that can be used to implement the required security service/protection for keys.
d. Briefly list the main processes/steps of key management.

Answer

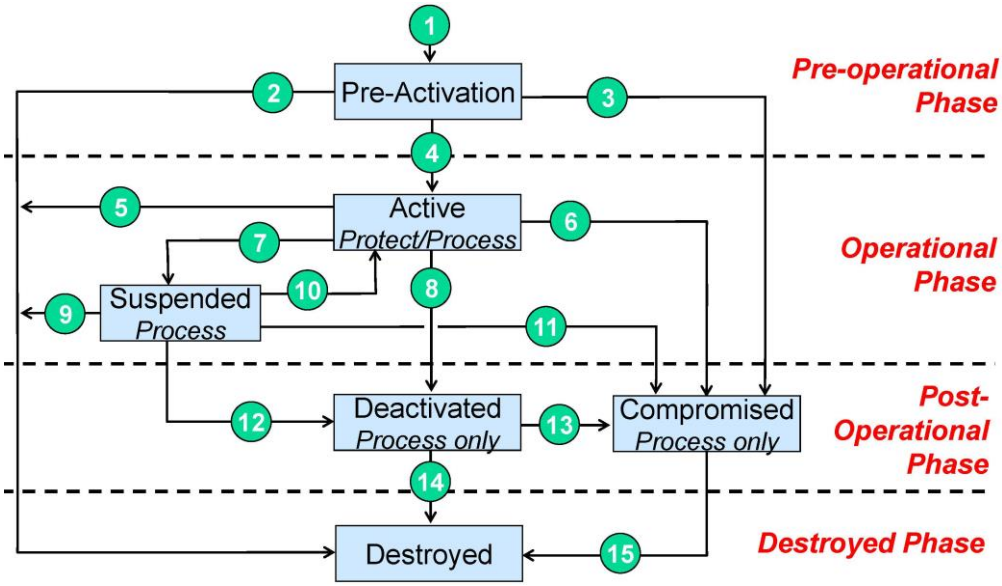
a. The strength of any cryptographic security solution depends on the strength and protection of the cryptographic keys. Cryptographic keys are exposed to many threats; hence the threats must be understood so that protection of cryptographic keys can be managed with appropriate security controls. Key management is basically the set of security controls for protecting the cryptographic keys.
b. Required protection is:
i) Symmetric secret keys and ii) asymmetric private keys must always be kept confidential (i.e. protected against unauthorised disclosure) and must have integrity/authenticity (i.e protected against falsification / unauthorized modification).
Iii) Asymmetric public keys must have integrity/authenticity (i.e. protected against falsification / unauthorized modification).
c. Physical protection and access control can be used to protect cryptographic keys, and is in fact the only way to protect root keys. Tamper proof devices can be used to generate, store and archive keys. Human memory can also be used to store keys/passwords. Cryptographic techniques can be used for all other cryptographic keys, including certificates to protect public keys against modification, and encryption to provide confidentiality protection of secondary keys or session keys during distribution.
d. The main processes of key management include key generation, distribution, storage, updating, revoking, recovering, archiving, destroying and auditing.

Question 2

a. Explain the diagram for key states and transitions between key states, as illustrated in NIST SP800-57, Figure 5, p.85.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
b. When a key is active, it may be designated to protect only, process only, or both. Referring to the 19 key types described in NIST SP800-57, give two examples of key types that are designed to protect only, two examples of key types that are designed to process only, and two examples of key types that are designed to both protect and process.
c. Explain why key types 17, 18 and 19 are misnomers. Suggest better names for those key types.

Answer

a. The state transition diagram is shown below.



b. Keys in active state:
   - Protect only: private signature (type 1)key and public key transport key (type 11)
   - Process only: public signature key (type 2) and private key transport key (type 10)
   - Protect and process: symmetric authentication key (type 3) and symmetric encryption key (type 6)

c. The term authorization is used in the sense of access control. It would be better to call these access control keys, or access keys.

Question 3

Describe reasons why online services can benefit from public-key cryptography? Why is symmetric key cryptography alone not suitable for online services?

Answer

Authentication and non-repudiation are important security services in online service provision. Public key cryptography can provide those services. Symmetric key cryptography cannot provide non-repudiation services since message authentication with a MAC only provides evidence that one of the parties with the shared key (for example a merchant and a customer) sent the message, but not which one. A public key infrastructure also provides a more scalable key management solution than using manual or TTP (Trusted Third Party) based distribution of symmetric keys. In practice a combination of public key and symmetric key cryptography provides the needed services, scaleability, as well as efficient computation.

Question 4

a. What is the spoofing problem with respect to public keys?
b. Explain how digital certificates can provide a solution to the spoofing problem.
c. Which are the conditions for having trust in a digital certificate? Justify your answer.
d. Is a digital signature the same as a public-key certificate? Justify your answer.

Answer

a. The spoofing problem is when an attacker replaces a public key (say Alice's public key) with a different key whose private key is known to the attacker. This allows the attacker to pretend to be Alice (e.g. read encrypted mail intended for Alice).
b. A digital certificate logically binds a public key to an entity — the CA is vouching for it.
c. 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 if you can verify the CA signature on the certificate. This means you need an authentic copy of the CA's public key.
d. No, a digital signature is not the same as a digital certificate. A digital signature in general is a cryptographic checksum on a data record. A public-key certificate is a specific type of data record containing a public key, the name of the key owner and some other data, as well as the digital signature created by a CA.

Question 5

a. Briefly describe the primary purpose of a public key infrastructure.
b. Describe and contrast the function of each of the following basic components in a PKI:
   • Certification authorities (CA)
   • Registration authorities (RA)

Answer

a. The main purpose of a PKI is to ensure authenticity of public keys. A PKI binds public keys to named entities, and enables relying parties to verify this binding. A specific public-key certificate is interpreted as: "Entity *X* owns public key *K*"
b. Respectively we have:
   - Certification authorities (CA) create, issue and revoke certificates, maintain certificate status information and issues CRLs, publish current certificates and CRLs and maintain archives of status information.
   - The Registration authority (RA) mediates between user and CA for public key registration, and is trusted by the CA to verify the identity of the certificate owner.

Question 6

a. Describe the trust model for the Browser PKI.
b. List the advantages and disadvantages of this model.

Answer

a. The browser PKI trust model is based on a relatively large number of (≈ 50) preinstalled root certificates that are used as trust anchors for validating received certificates. Each root certificate defines a separate hierarchic PKI. The user implicitly trusts the browser vendor that supplied the installed root certificates, and thereby indirectly the root CAs themselves, and their root certificates. The browser software automatically validates received server certificates that can be cryptographically traced back to a root certificate.
b. Relevant elements are:
   - Advantages: Ease of use, automated validation of server and software certificates
   - Disadvantages:
     – Root certificates not well protected from modification attacks
     – When prompted, users tend to automatically accept any certificate that does not validate, so the purpose of certificate validation is questionable.
     – Any compromised CA threatens the whole infrastructure (weakest link).

Question 7

Access to the stored root certificates in your browser is via the browser menus. For example

- Firefox: Tools → Options → Privacy & Security → Certificates → View Certificates
- Microsoft Edge: There is no way to view certificates from MS Edge, which is shocking! However, you can view the certificates stored in MS Edge by opening the (old) MS Internet Explorer browser. You can open MS Internet Explorer from MS Edge by selecting Tools (• • •) → Open with Internet Explorer. Alternatively, you can find MS Internet Explorer under Windows Accessories, together with e.g. Paint and Notepad.
- MS Explorer, select: Tools (☼) → Internet Options → Content → Certificates → Root certificates, then you will be able to examine certificates installed in your browser.

Look through root certificates installed in your browser to determine the expiration dates.

a. Which certificates have short lifetimes?
b. Can you find certificates with expiration dates in excess of ten years from now?
c. Can you find certificates that have already expired? What happens when viewing them?

Answer

The details are not important and will vary across different installations. Normally certificates are issued with lifetimes from one to ten years. CA certificates are typically self-certified and have lifetimes of 10 to 50 years. You can probably find CA certificates which have expired. Both IE and Firefox give some kind of warning when you open an expired certificate.

Question 8

a. Why is it important to have a limited cryptoperiod for keys? Give at least four reasons.
b. What is the difference between protection and processing when using keys?
c. Compare the recommended cryptoperiod for private and public signature keys according to NIST SP800-57? Would you say that the validity period of root certificates in web browsers follow the recommendations of NIST SP800-57?
d. Assuming practical QC by 2030, is the validity period of the root certificates meaningful?

Answer

a. The reasons are:
   - Limits the amount of information available for cryptanalysis of a single key.
   - Limits the damage if a single key is compromised.
   - Limits the use of a particular algorithm to its estimated effective lifetime.
   - Limits the time available for attempts to penetrate physical, procedural, and logical access mechanisms that protect a key from unauthorized disclosure.
   - Limits the period within which information may be compromised by inadvertent disclosure of keying material to unauthorized entities.
   - Limits the time available for computationally intensive cryptanalytic attacks. (in applications where long-term key protection is not required)..

b. Protection is when keys are used to encrypt and to create digital signatures, aka. Originator Usage Period (OUP). Processing is when keys are used to decrypt and to validate signatures, aka. Recipient Usage Period (RUP).
c. The validity of browser root certificates refers to the RUP, and is in accordance with the recommendation of SP800-57 for a public signature-verifying key, which is *"Several years (depends on key size)"* (Table 1, p.45). The information that can be viewed in the browsers does not say anything about the actual OUP practiced by the CAs.
d. The validity period of many root certificates is obviously too long when assuming practical QC (quantum computers) by 2030.

Question 9

What is the difference between standard server certificate and EV server certificates?

Answer

Standard certificates can be bought anonymously, EV requires legal name of buyer.
EV certificates are more expensive than standard certificates.

Question 10

a. Why is certificate revocation necessary ?
b. Which problem is solved with the "Must-Staple Protocol" ?

Answer

a. Certificate revocation is necessary for example if the owner of a certificate suspects that the private key has been compromised.
b. Previously, the OCSP protocol violated the user privacy when browsing. The "Must-Staple Protocol" allows users to browse privately.

Question 11

a. Which problem is solved with CA Authorization and Certificate Transparency ?
b. Where is the CA Authorization policy stored ?
c. What must the domain owner do in order to make sure that its CA Authorization policy is followed?
d. What must the domain owner do if it discovered that the CA Authorization policy has been breached?

Answer

a. CA Authorization can prevent rogue/compromised CAs from issuing fake certificates.
b. The CA Authorization policy is stored in the DNS record for the domain.
c. The domain owner must check the CT (Certificate Transparency) Log to see if it contains any fake certificates.
d. If the CT Log contains a fake certificate for the domain, then the fake certificate must be revoked.