UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab 9: Digital signatures and Key establishment

Exercises from Lectures 14 and 16.

QUESTION 1

Suppose that RSA signatures are used with a hash function h that is not one-way (that is, the attacker can invert the hash function).

Show how an existential forgery is possible against such signatures. In other words, how can an attacker form valid signatures S from e and n alone?

QUESTION 2

(a) Show that the verification equation for Elgamal signatures works. That is, if (r, s) is a valid Elgamal signature, then $g^M \equiv y^r r^s \pmod{p}$.

See slides 17-18 of Lecture 14.

(b) Similarly check that the verification equation works for DSA signatures.

Check from slide 21 of Lecture 14.

QUESTION 3

The original Elgamal digital signature scheme did not include a hash function H as a system parameter. The message m was used directly in the algorithm instead of $H(m)$ as in DSA. This enables an attack called existential forgery. Pointcheval and Stern generalized the case and described two levels of forgeries[1]:

(a) **The one-parameter forgery.** Given an element e such that $1 < e < p - 1$, find how to construct r and s to get (r, s) as a valid signature for the message $m = es \bmod (p - 1)$ (using parameters g and y).

(b) **The two-parameters forgery.** Given elements e, v such that $1 < e, v < p - 1$ and $\gcd(v, p - 1) = 1$, find how to construct r and s to get (r, s) as a valid signature for the message $m = es \bmod (p - 1)$ (using parameters g and y).

The one-parameter forgery is a special case of the two-parameter forgery, when $v = 1$.

[1] https://www.di.ens.fr/david.pointcheval/Documents/Papers/1996_eurocrypt.pdf

cont/...

QUESTION 4

Suppose the parameters $p = 23$, $q = 11$, $g = 3$ are used for the DSA signature.

(a) Show that g has order q as required.
Hint: To show that 3 has order 11, we need to check that $3^{11} \equiv 1 \pmod{23}$ but it is not true that $3^j \equiv 1 \pmod{23}$ for $1 < j < 11$.
(b) If the private key is $x = 5$, what is the public key y?
We recall that $y = g^x \pmod{p}$.
(c) Compute a valid signature for a message M whose hash value is assumed to be $SHA(M) = 8$.
Hint: Try with $k = 2$.
(d) Show that the verification equation works for your signature.
Hint: Calculate w, u_1, u_2.

QUESTION 5

We suppose that the same value of the random k is used to generate *two* different DSA signatures.

Show that this is sufficient for an attacker to find the private signing key.

N.B.: This was the attack used to break the Sony Playstation 3 in 2010 because their implementation used a fixed k. Sony used the elliptic curve version.

QUESTION 6

Discuss the advantages and disadvantages of using key predistribution, session key distribution and key agreement protocols in the following scenarios:

- a corporate network such as UC's Intranet;
- a small company or domestic environment;
- Internet communications (e.g. HTTPS, secure email).

Hint: In our comparison, we assume that key agreement is based on public keys, which requires a supporting Public Key Infrastructure (PKI) to register users, issue certificates, revoke certificates, etc.

cont/...

QUESTION 7

Consider a scenario in which a client C uses Kerberos to access a printer server V. Suppose that authenticator_C is not sent in the level 3 interaction. Explain a scenario in which this can allow an attacker to obtain documents printed by C.

Hint: We can assume that an attacker is able to obtain the ticket issued to C in order to obtain access to V. See Lecture 16.

QUESTION 8

In each of the following cases, the goal is a key establishment between parties A and B. Let N_A and N_B be nonces chosen by A and B respectively, and K_{AB} be the session key. Let K_{AS} and K_{BS} be key-encrypting keys initially shared between the server S and A, and between the server S and B respectively. We assume that $\{X\}_K$ denotes authenticated encryption of message X with key K.

Find an attack on each of the following protocols:

(a) In this protocol, B includes A's challenge (nonce) in Message 4, intended to give key confirmation and key freshness.

1. $A \longrightarrow B : ID_A, ID_B, N_A$
2. $B \longrightarrow S : ID_A, ID_B, N_A, N_B$
3. $S \longrightarrow B : \{K_{AB}\}_{K_{AS}}, \{N_B, ID_A, ID_B, K_{AB}\}_{K_{BS}}$
4. $B \longrightarrow A : \{K_{AB}\}_{K_{AS}}, \{N_A, ID_A, ID_B\}_{K_{AB}}$

(b) In this protocol, S saves on encryption by only including the identity of the intended recipient in each field.

1. $A \longrightarrow B : ID_A, ID_B, N_A$
2. $B \longrightarrow S : ID_A, ID_B, N_A, N_B$
3. $S \longrightarrow B : \{N_A, ID_A, K_{AB}\}_{K_{AS}}, \{N_B, ID_B, K_{AB}\}_{K_{BS}}$
4. $B \longrightarrow A : \{N_A, ID_A, K_{AB}\}_{K_{AS}}$

(c) This protocol (published by Tatebayeshi, Matsuzaki and Newman in 1989) uses public key encryption $E_K(\cdot)$.

K_S is the public key of the server S which is assumed known by all users. The random number generated by A is used as a symmetric encryption key in Message 4. The random number generated by B is used as the session key, that is $K_{AB} = N_B$.

1. $A \longrightarrow S : ID_A, ID_B, E_{K_S}(N_A)$
2. $S \longrightarrow B : ID_A$
3. $B \longrightarrow S : ID_A, ID_B, E_{K_S}(N_B)$
4. $S \longrightarrow A : ID_B, \{N_B\}_{N_A}$

Hints: The question-answer sheet of the lab will contain sample attacks. You may be able to find others. Moreover, it might help to visualise the protocols and attacks if you draw the message flows between the parties A, B, S (and the external attacker C).