ap your attendance ☺ ☺ ☺

TUTORIAL

CSCI361 – Computer Security

Sionggo Japit

sjapit@uow.edu.au

12 February 2024

BLIND SIGNATURE

Blind signature protocol

A blind signature protocol requires the following components:

1. A digital signature mechanism for signer.
2. Functions f and g that are known only to the sender. The function f is known as blinding function, and function g is known as unblinding function.

The blinding function f is defined as: $f(m) = m \times k^e \bmod n$

The unblinding function g is defined as: $g(m) = k^{-1} m \bmod n$

Blind signature protocol

Chaum's blind signature protocol:

Sender A receives a signature of B on a blinded message.

From this, A computes B's signature on a message m chosen a priori by A. Note: 0 £ m £ n -1. Note B has no knowledge of m nor the signature associated with m.

Blind signature protocol

Assuming we use RSA signature scheme, then B's RSA public and private keys are (n, e) and d respectively.

A need to choose k, a random secret integer satisfying $0 \le k \le n - 1$ and $\gcd(k, n) = 1$.

Blind signature protocol

Protocol:

Blinding: A computes $m' = mk^e \bmod n$ and sends m' to B for signing.

Signing: B compute $s' = (m')^d \bmod n$ which it sends to A.

Unblinding: A computes $s = k^{-1} s' \bmod n$, which is B's signature on m.

Uses s to obtain the original message m.

Blind signature protocol

For example, using the following RSA parameters:

$p = 11,\ q = 13,\ n = p \times q = 143,\ e = 37,\ d = 13,$ and $m = 74.$

Sender: Bob

Bob chooses $k = 10$. Through extented Euclidean, we

obtained $k^{-1} = 43$ (Note, we need k^{-1} to unblind later.)

Bob computes $m' = mk^e \bmod n$ (blinding the message m)

$$= 74 \times 10^{37} \bmod 143$$

$$= 74 \times 10 \bmod 143 = 25$$

Blind signature protocol

Bob sends $m' = 25$ to Alice, the signatory.

Alice receives the message m' and signs the message:

$$s' = (m')^d \bmod n$$

$$= (25)^{13} \bmod 143$$

$$= 38$$

Alice sends s'=38 to Bob.

Blind signature protocol

Bob receives s' and compute:

$$s = k^{-1} s' \bmod n$$

$$= (43)(38) \bmod 143$$

$$= 61$$

Bob can obtain the original message as follow:

$$m = s^{e} \bmod n$$

$$= 61^{37} \bmod 143$$

$$= 74$$