Department of Electronics

Cryptography

Fall 2019

Hasan Mahmood

hasan@qau.edu.pk

Week 16 (18, 19 December 2019)

Zero-Knowledge Technique

- Thieves set up a fake automatic teller machine at a shopping mall
- When a person inserted a bank card and typed in an identification number, the machine recorded the information but responded with the message that it could not accept the card.
- The thieves then made counterfeit bank cards and went to legitimate teller machines and withdrew cash, using the identification numbers they had obtained

Zero-Knowledge Techniques

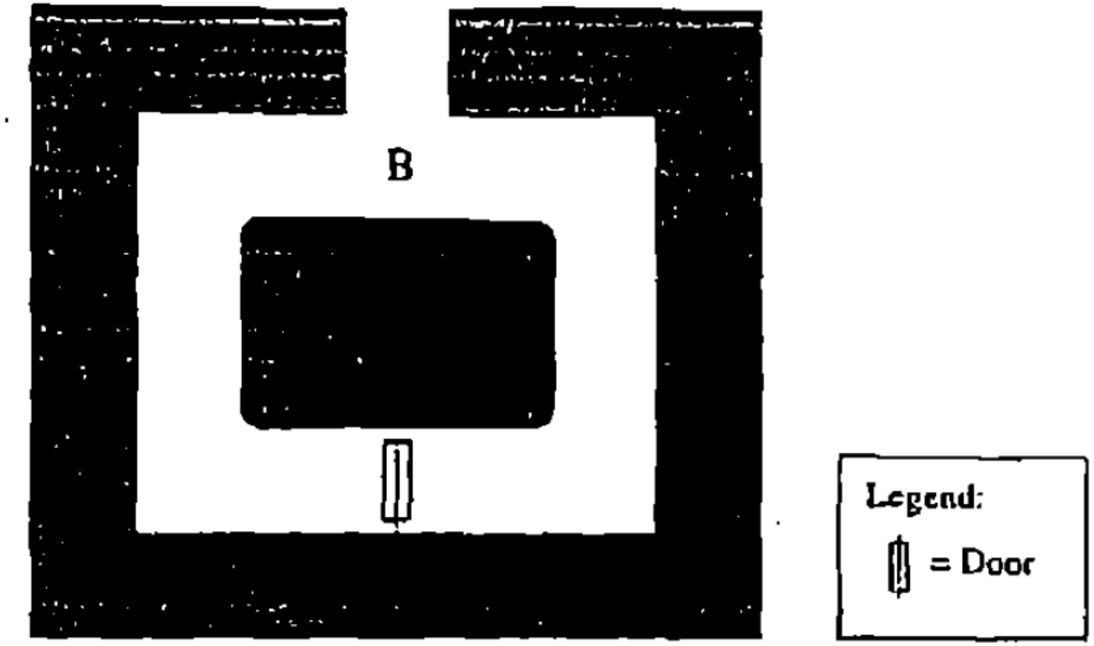
- How can this be avoided?
- There are several situations where someone reveals a secret identification number or password in order to complete a transaction.
- Anyone who obtains this secret number, pins some (almost public) identification information (for example, the information on a bank card), can masquerade as this person.
- What is needed is a way to use the secret number without giving any information that can be reused by an eavesdropper.
- This is where zero-knowledge techniques come in.

The Challenge-response Protocol

- The basic challenge-response protocol is best illustrated by an example due to Quisquater, Guillou, and Berson |Quisquater et al.]
- Suppose there is a tunnel with a door
- Peggy (the prover) wants to prove to Victor (the verifier) that she can go through the door without giving any information to Victor about how she does it.
- She doesn't even want to let Victor know which direction she can pass through the door (otherwise, she could simply walk down one side and emerge from the other).

The Challenge-response Protocol

- Peggy enters the tunnel and goes down either the left side or the right side of the tunnel.
- Victor waits outside for a minute, then comes in and stands at point B
- He calls out “Left” or “Right" to Peggy
- Peggy then comes to point B by the left or right tunnel, as requested
- This entire protocol is repeated several times, until Victor is satisfied in each round
- Peggy randomly chooses which side she will go down, and Victor randomly chooses which side he will request.



- Since Peggy must choose to go down the left or right side before she knows what Victor will say, she has only a 50% chance of fooling Victor if she doesn't know how to go through the door.
- Therefore, if Peggy comes out the correct side for each of 10 repetitions, there is only one chance in 2^10 = 1024 that Peggy doesn't know how to go through the door.
- At this point, Victor is probably convinced, though he could try a few more times just to be sure.

Eve

- Suppose Eve is watching the proceedings on a video monitor
- She will not be able to use anything she sees to convince Victor or anyone else that she, too, can go through the door.
- Moreover, she might not even be convinced that Peggy can go through the door.
- After all, Peggy and Victor could have planned the sequence of rights and lefts ahead of time.
- By this reasoning, there is no useful information that Victor obtains that can be transmitted to anyone.

Proof

- Note that there is never a proof, in a strict mathematical sense, that Peggy can go through the door
- But there is overwhelming evidence, obtained through a series of challenges and responses.
- This is a feature of zero-knowledge “proofs."

Mathematical Version of the Procedure

- There are several mathematical versions of this procedure, but we'll concentrate on one of them
- Let $n = pq$ be the product of two large primes
- Let y be a square mod n with gcd(y,n) = 1
- Recall that finding square roots mod n is hard; in fact, finding square roots mod n is equivalent to factoring n
- However, Peggy claims to know a square root s of y
- Victor wants to verify this, but Peggy does not want to reveal s.

Method…continued…

1. Peggy chooses a random number r_1 and lets $r_2 \equiv s r_1^{-1} \pmod{n}$, so

$$r_1 r_2 \equiv s \pmod{n}.$$

   She computes

$$x_1 \equiv r_1^2, \quad x_2 \equiv r_2^2 \pmod{n}$$

   and sends x_1 and x_2 to Victor.

2. Victor checks that $x_1 x_2 \equiv y \pmod{n}$, then chooses either x_1 or x_2 and asks Peggy to supply a square root of it. He checks that it is an actual square root.

3. The first two steps are repeated several times, until Victor is convinced.

- Of course, if Peggy knows *s*, the procedure proceeds without problems
- But what if Peggy doesn't know a square root of *y*?
- She can still send Victor two numbers x_1 and x_2 with $x_1 x_2 = y$. If she knows a square root of x_1 and a square root of x_2, then she knows a square root of $y = x_1 x_2$
- Therefore, for at least one of them, she does not know a square root
- At least half the time, Victor is going to ask her for a square root she doesn't know.
- Since computing square roots is hard, she is not able to produce the desired answer, and therefore Victor finds out that she doesn't know *s*.