

Note: April 19, 2007

Side Channel Attacks

- Timing
- Power
- Sound
- Light

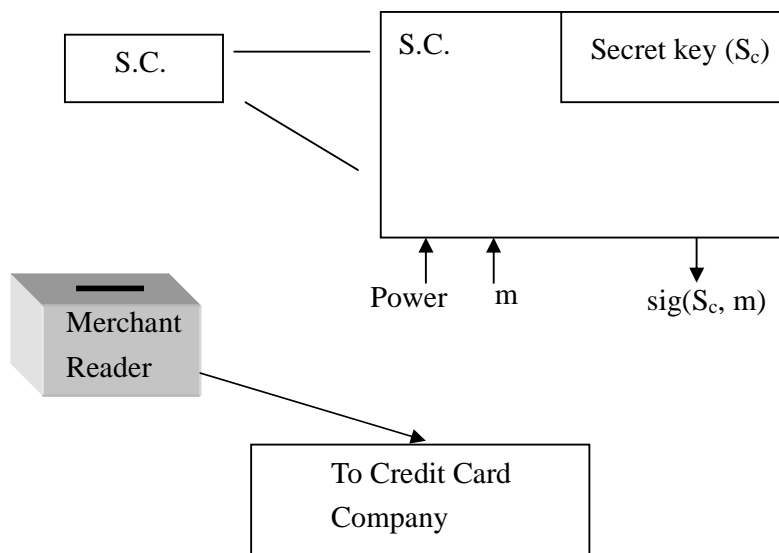
Usability & Security

- Depending on users
- Role playing

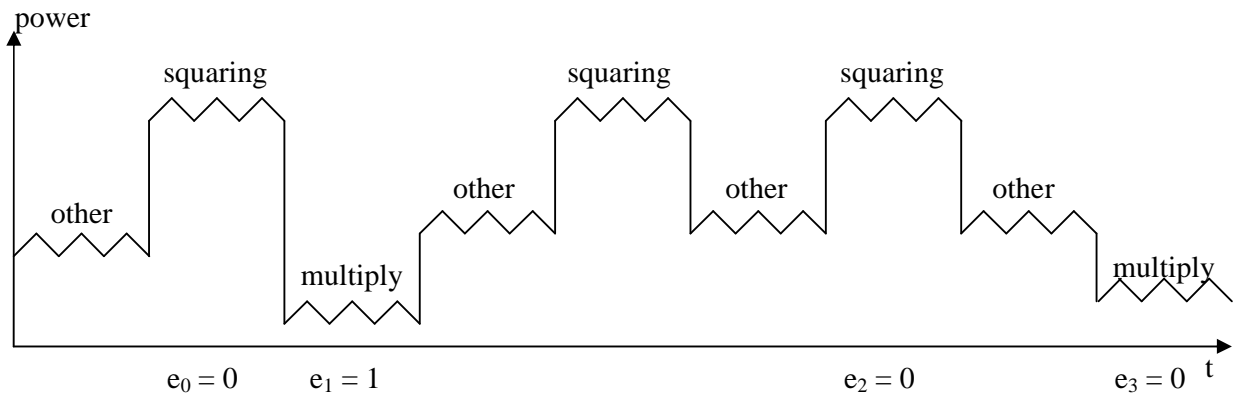
Modular Exponentiation Algorithm (Square & Multiply)

```
modexp(m, e, n) //  $m^e \bmod n$   
  Let  $e_1 \dots e_0 = e$  // the bits of  $e$   
  Let  $acc = 1$   
  for  $i = 0 \dots 1$   
    if  $e_i = 1$   
       $acc = acc * m \bmod n$   
     $m = m^2 \bmod n$   
  return  $acc$ 
```

Power Analysis (Smart Cards)



Example: (See Modular Exponential Algorithm above for detail)



Note: If see multiply, then squaring, implies $e = 1$. If see squaring w/out multiply, then $e = 0$.

Timing Attack against square & multiply

Some reductions take longer than others

- Fast reductions
- Slow reductions
- If attacker knows $acc * m$, he can predict whether reduction is fast or slow

Attacker input	time	Suppose attacker guessed $e_0 = 1$, then he can
m_0	t_0	● Compute acc & m at end of round 0
m_1	t_1	● Predict whether round 1 will be fast or slow
m_2	t_2	● Fast or slow for each message m_i
...	...	● Let f = avg. time of the fast messages
m_k	t_k	● Let s = avg. time of the slow messages.

Two cases:

1. $|s_1 - f_1|$ is small & $|s_0 - f_0|$ is small $\rightarrow e_1 = 0$
2. Suppose $|s_b - f_b|$ is large & $|s_b - f_b|$ is small $\rightarrow e_1 = 1$ & $e_0 = b$

Repeat rounds 2 ... l

Defense against Timing Attacks

Solution 1: Rewrite the code

```

modexp(m, e, n) //  $m^e \bmod n$ 
Let  $e_l \dots e_0 = e$  // the bits of  $e$ 
Let  $acc = 1$ 

```

```

for i = 0 ... l
  if ei = 1
    acc = acc * m mod n
  else //to avoid timing difference
    tmp = acc * m mod n
    m = m2 mod n
return acc

```

Solution 2: RSA Blinding

To compute $m^e \bmod n$, pick a random r

1. pick a random r
2. compute $x = (r m)^e \bmod n$
3. compute $y = r^e \bmod n$
4. return $x/y \bmod n$

Sound & Light Attacks

Light:

Scenario 1: Facing CRT monitor toward the window, where attackers can directly see the CRT monitor through the window.

Scenario 2: Facing CRT monitor away from window, where attackers can no longer directly see the CRT monitor. However, attacker can see the light that hits the white wall, which reflects the pixels' light and allows attacker to rebuild the image on the monitor.

Read article "Optical Time-Domain Eavesdropping Risks of CRT Displays" for further information about light attacks.