

SIDE CHANNEL ATTACKS (continued from last class)

Lecture date: 04 / 24 / 2009

Brumley / Boneh (Contribution):

- Works against CRT optimized modexp algorithms (Kosher attack does not work here)
- Montgomery multiplication, optimization
- Sliding windows
- Karatsuba multiplication ($n^{1.7}$ vs. nm)
- Timing attacks possible on networks
eg: colocated servers

Counter measures:

1. RSA binding:

- In RSA, we have $m^d \bmod N$ (server side)
- Here, we know m is going to be multiplied with itself
- So, pick a random ' r '

Thus,

$$x = rm \bmod N$$

$$r^d m^d = x^d \bmod N$$

$$m^d = (x^d / r^d) \bmod N$$

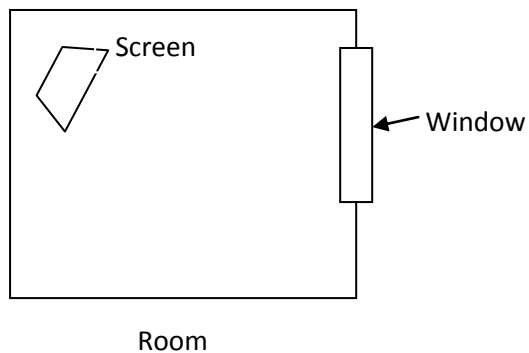
2. Fixed time delay for response

- If we idle wait -> not useful
- If we busy wait -> useful but wastes CPU

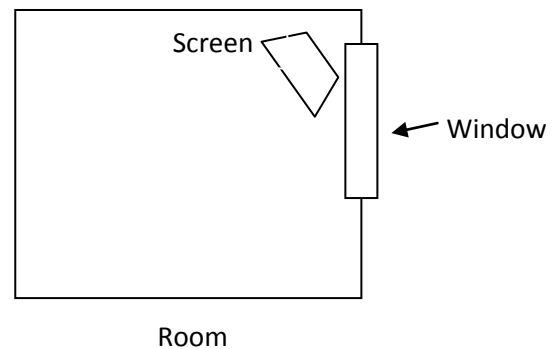
Local Side Channels:

- CPU usage
- Page Faults
- Temperature
- Cache lines
- Branch prediction registers (if BPRs not cleared, it may leak bits of secret keys)

CRT Attacks:



WRONG!!



CORRECT!! 😊

Using high speed cameras, one can observe light intensity for each pixel. So computer screen should not be facing windows in a room.

Keyboards based attacks:

- Each key makes a peculiar sound which is generally different from that of other keys on the keyboard. With key stroke “sound” loggers, one can record the sounds produced by keys and this can be used at a later point of time to identify which keys were pressed by a user.
- Logging inter-keystroke times may also help in recognising which keys the user had pressed. This could be done by constructing inter-keystroke time-tables and then looking up for closest match in such tables.