ECS 235B Module 47
Side Channels

Side Channels

A *side channel* is set of characteristics of a system, from which adversary can deduce confidential information about system or a competition

- Consider information to be derived as HIGH
- Consider information obtained from set of characteristics as LOW
- Attack is to deduce HIGH values from LOW values only
- Implication: attack works on systems not deducibly secure

Types of Side Channel Attacks

- *Passive*: Only observe system; deduce results from observations
- *Active*: Disrupt system in some way, causing it to react; deduce results from measurements of disruption

Example: Passive Attack

- Fast modular exponentiation:

```
x := 1; atmp := a;
for i := 0 to k-1 do begin
   if z_i = 1 then
         x := (x * atmp) mod n;
   atmp := (atmp * atmp) mod n;
end;
result := x;
```

- If bit is 1, there are 2 multiplications; if it is 0, only one
- Extra multiplication takes time
- Can determine bits of the confidential exponent by measuring computation time

Example: Active Attack

Background

- Derive information from characteristics of memory accesses in chip
- Intel x86 caches
  - Each core has 2 levels, L1 and L2
  - Chip itself has third cache (L3 or LLC)
  - These are hierarchical: miss in L1 goes to L2, miss in L2 goes to L3, miss in L3 goes to memory
  - Caches are inclusive (so L3 has copies of data in L2 and L1)
- Processes share pages

Example: Active Attack

Phase 1

- Flush a set of bytes (called a *line*) from cache to clear it from all 3 caches
  - The disruption

Phase 2

- Wait until victim has chance to access that memory line

Phase 3

- Reload the line
  - If victim did this already, time is short as data comes from L3 cache
  - Otherwise time is longer as memory fetch is required

Example: Active Attack

What happened

- Used to trace execution of GnuPG on a physical machine
- Derived bits of a 2048 bit private key; max of 190 bits incorrect
- Repeated experiment on virtual machine
- Error rates increased
  - On one system, average error rate increased from 1.41 bits to 26.55 bits
  - On another system, average error rate increased from 25.12 bits to 66.12 bits

Model

Components

- *Primitive*: instantiation of computation
- *Device*: system doing the computation
- *Physical observable*: output being observed
- *Leakage function*: captures characteristics of side channel and mechanism to monitor the physical observables
- *Implementation function*: instantiation of both device, leakage function
- *Side channel adversary*: algorithm that queries implementation to get outputs from leakage function

Example

- First one (passive attack) divided leakage function into two parts
  - *Signal* was variations in output due to bit being derived
  - *Noise* was variations due to other factors (imprecisions in measurements, etc.)
- Second one (active attack) had leakage function acting in different ways
  - Physical machine: one chip used more advanced optimizations, thus more noise
  - Virtual machine: more variations due to extra computations running the virtual machines, hence more noise

Example: Electromagnetic Radiation

- CRT video display produces radiation that can be measured
- Using various equipment and a black and white TV, van Eck could reconstruct the images
  - Reconstructed pictures on video display units in buildings
- E-voting system with audio activated (as it would be for visually impaired voters) produced interference with sound from a nearby transistor radio
  - Testers believed changes in the sound due to the interference could be used to determine how voter was voting

Quiz

Choose the correct one:

Side channel attacks are really a form of violating (integrity, non-deducibility)