Lecture 9: Side Channels
Revisiting Threat Models
Side Channels

"Security is lax on this side."
Differential Power Analysis
Power Trace for AES
AES

- Key Expansion: $sk \rightarrow (rk_1, ..., rk_{n+1})$
- AddRoundKey:
- SubBytes:
- ShiftRows:
- MixColumns:
DPA on AES
DPA on AES
Timing Attacks

res = 1;
while (exp > 0) {
    if (exp % 2 == 1) {
        res = res * base % p;
    }
    base = base^2 % p;
    exp >>= 1;
}
return res;
Timing attacks on RSA

- Naïve square and multiply
- Sliding window (with Chinese Remainder Theorem)
Cache Attacks

- Processor (P)
- Cache (S)
- Main Memory (M)
- Disk/Flash (D)

Cache Accesses (10 or fewer cycles)
Main Memory Access (100s of cycles)
Disk Access (100,000s of cycles)
Set Associate Caches
Cache Attack on AES
Cache Attack on AES

- Allocate contiguous byte array of size $S \cdot W \cdot B$ with start address congruent to start address of AES lookup table
- Read from each memory block of array
- Trigger encryption of message $m$
- For each index (offset is cache line size): compute total time to read all $W$ array values mapped to that cache line
Cache Attack on AES
Do Side Channel Attacks work remotely?
Remote Timing on RSA
Cloud Providers

Cloud providers:

- Amazon Web Services
- Windows Azure
- Rackspace
- Google Compute Engine
- Salesforce.com
- Heroku
- Dropbox

In the context of cloud computing:

- Infrastructure-as-a-service
- Platform-as-a-service
- Software-as-a-service
Cache Attacks on EC2 Instances
Achieving Co-Residency
Detecting Co-Residency

Instances co-resident

Instances co-resident

Instances NOT co-resident
Mitigating Side Channels

- Forced Equivalence
- Blinding
- LR Crypto