Information Security – Theory vs. Reality

0368-4474, Winter 2015-2016

Lecture 2: Architectural side-channels (2/2)

Lecturer:
Eran Tromer

Course agenda

Architectural side-channel attacks (cont.)

L3 Flush+Reload attack

[Yarom Falkner 2014]

- Target outermost cache, shared between all CPU cores (typically L3)
- RSA key extraction from GnuPG 1.4.13
- Target specific memory block (instead of cache set)
- Exploits memory deduplication (content-based page sharing)
  - Common code, libraries, data across VMs
  - Supposedly safe (nominally, no new information flow)

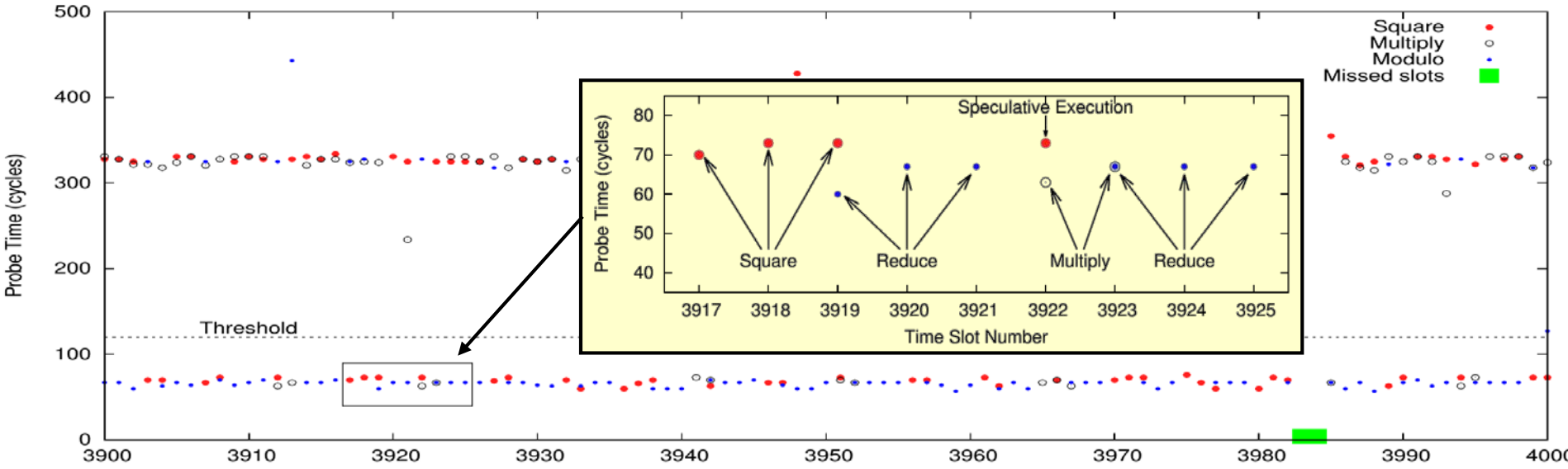
L3 flush+reload attack (cont.)

To measure a memory block b, the attacker:

- Achieve page sharing of b with victim
- Flush block b using x86 `clflush` instruction
  - Flushes block from all cache levels
  - Normally used for synchronization / performance
- Wait until victim runs
- Measure time to read the block b
  - Fast → victim accessed b
  - Slow → victim did not access b

L3 flush+reload attack on GnuPG's RSA

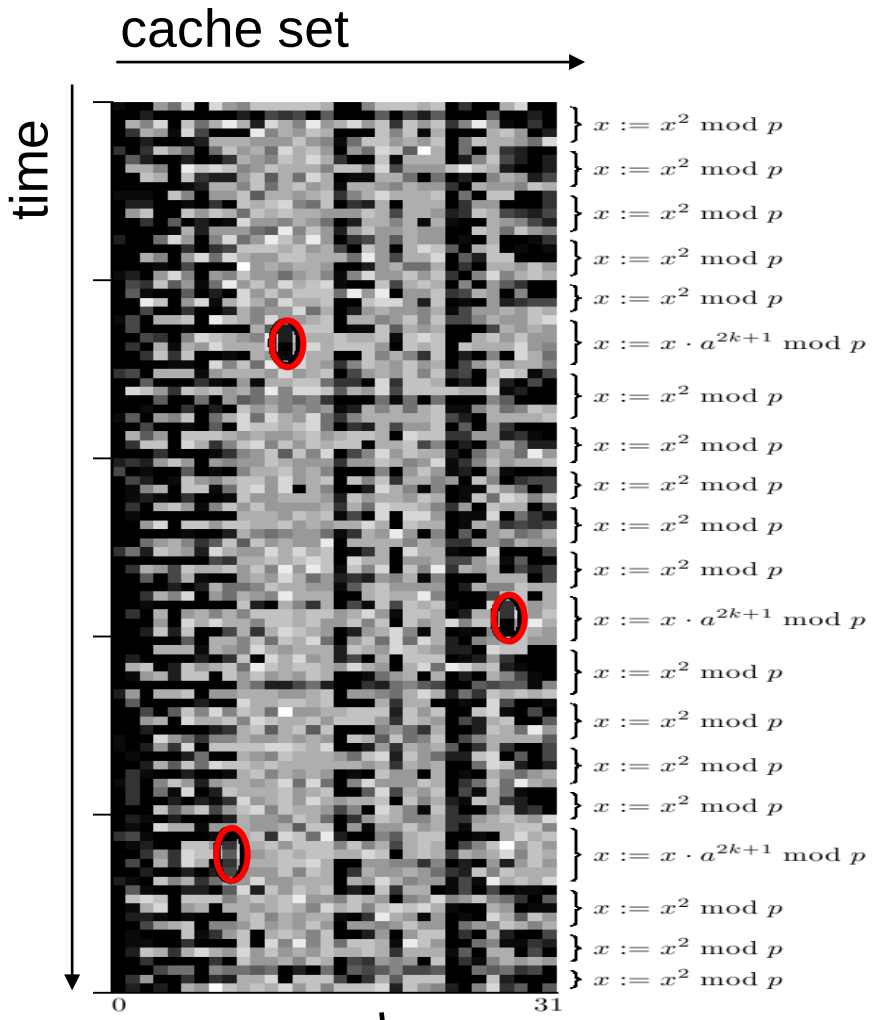
- GnuPG 1.4.13 uses square-and-multiply exponentiation.
- Repeatedly measure blocks in the code of the `square`, `multiply` and `modulo` routines.
- Read out the bits from the sequence during a single RSA decryption
  - `multiply` between adjacent `square` → key bit is 1
  - No `multiply` between adjacent `square` → key bit is 0



[Yarom Falkner 2014]

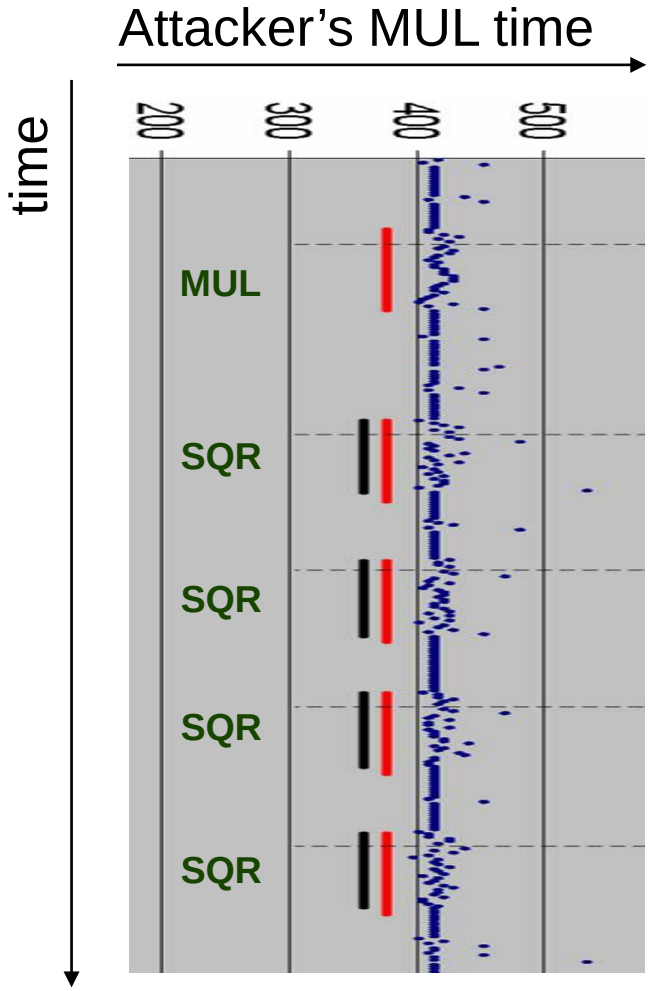
Other attacks on RSA

Cache attack using HyperThreading
[Percival 05]



On whiteboard:
m-ary exponentiation

ALU multiplier attack
[Aciicmez Seifert 2007]



Victim's operation

Other architectural attacks
(Whiteboard discussion)

- Covert channels [Hu ’91, ‘92]
- Hardware-assisted
  – Power trace [Page ’02]
- Timing attacks via internal collisions
  [Tsunoo Tsujihara Minematsu Miyuachi ’02]
  [Tsunoo Saito Suzaki Shigeri Miyauchi ’03]
- Model-less timing attacks [Bernstein ’04]
- RSA [Percival ’05]
- Exploiting the scheduler [Neve Seifrert ’07]
  – Improve temporal resolution by causing victim to get tiny time slice
- Instruction cache Aciicmez ’07]
  – Exploits difference between code paths
  – Attacks are analogous to data cache attack
- Branch prediction [Aciicmez Schindler Koc ’06–’07]
  – Exploits difference in choice of code path
  – BP state is a shared resource
- ALU resources [Aciicmez Seifert ’07]
  – Exploits contention for the multiplication units
- *Many followups*

Mitigation

(classroom discussion)