VERNAM Group

Security & Privacy @ WPI

Cache Attacks Enable Bulk Key Recovery on the Cloud

Mehmet Sinan Inci, Gorka Irazoqui, Berk Gulmezoglu, Thomas Eisenbarth and Berk Sunar

CHES'16, August 2016

Santa Barbara, CA

WPI

Outline

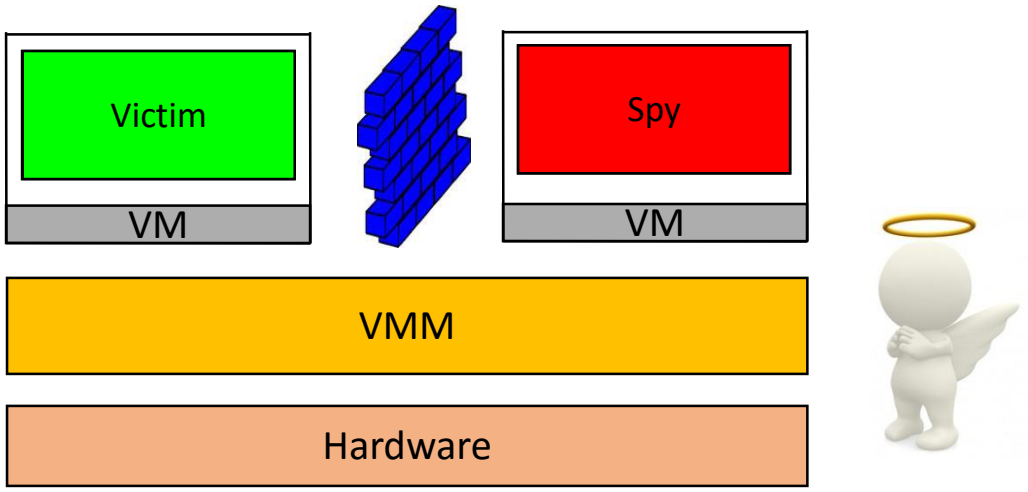
- **Motivation**
- Co-location Detection
- Key Recovery Attack
- Conclusion

Cloud Computing

- CSPs: many users on shared, homogeneous platforms
- Users rent VMs, share physical systems
- **Shared resources ➔ Information Leakage?**

Security through Isolation

- Virtual Machines: Abstraction of physical machine
- Hypervisor (VMM) ensures isolation through virtualization
- VMs can feel each other's load on low-level shared resources → potential side channels



Is Isolation Secure?

Select Attacks in the Cloud Scenario:

- *Hey you get off my cloud [RTSS09]*
  - First co-location in a public cloud
- *Cross-VM Side Channels and Their Use to Extract Private Keys [ZJRR12]*
  - Shows feasibility in cross-VM setting
  - Assumes shared L1-cache
- *Prime+Probe on LLC [LY+15]*
  - Targets LLC cache: cross-core cross-VM setting
  - Square and multiply exponentiation
  - Sliding window exponentiation

[RTSS09] Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. *Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-party Compute Clouds.* ACM CCS '09
[ZJRR12] Zhang, Y., Juels, A., Reiter, M. K., and Ristenpart, T. *Cross-VM Side Channels and Their Use to Extract Private Keys.* ACM CCS '12
[LY+15] Liu, F., Yarom, Y., Ge, Q., Heiser, G., & Lee, R. B. (2015). *Last-Level Cache Side-Channel Attacks are Practical*. S&P '15

Motivation

1. Collect fine grain SC leakage on **commercial cloud**
   - Amazon EC2, the largest public cloud
   - Over 10X the computing than the next 14 CSPs
     http://fortune.com/2015/05/19/amazon-tops-in-cloud/
2. Recovering RSA keys
   - Libgcrypt 1.6.2
   - Recently Patched
   - Still widely used

55% of TLS hosts on EC2

3. Stealing keys in bulk!
   - No faulty RNGs, only hardware leakage
   - Perfectly configured systems are vulnerable

[HEN12] Heninger, N., Durumeric, Z., Wustrow, E., and Halderman, J. A. *Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices*. USENIX Security 12

[BER13] Bernstein, D. J., Chang, Y.-A., Cheng, C.-M., Chou, L.-P., Heninger, N., Lange, T., and Van Someren, N. *Factoring RSA keys from certified smart cards: Coppersmith in the wild*. ASIACRYPT 2013

Outline

- Motivation
- **Co-location Detection**
  - Targeted Attack
  - Bulk Recovery
- Key Recovery Attack
- Conclusion

First Step: Co-Location

- First success in 2009 on AWS [RTS09]:
  1. Much smaller EC2
  2. Launch many instances on cloud
  3. Check if any are co-located

- How to detect Co-location?
  - Ping time
  - IP address of instance or hypervisor?
  - Disk drive performance?

[RTSS09] Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. *Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-party Compute Clouds.* ACM CCS '09

Co-Location in 2016

AWS EC2:

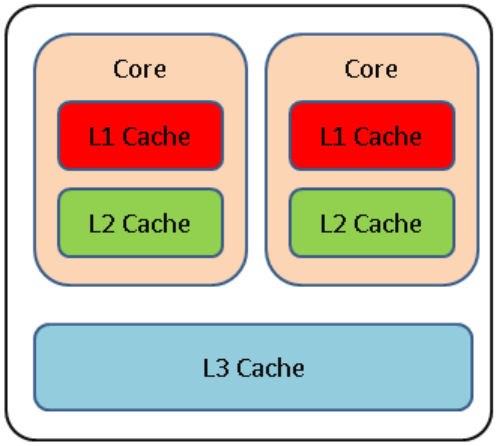
- Constant time Pings
- HDDs replaced with SSDs
- No Hypervisor IP
- **Known side channels are closed**

➢New methods needed

- LLC Covert Channel
- Software Profiling in LLC

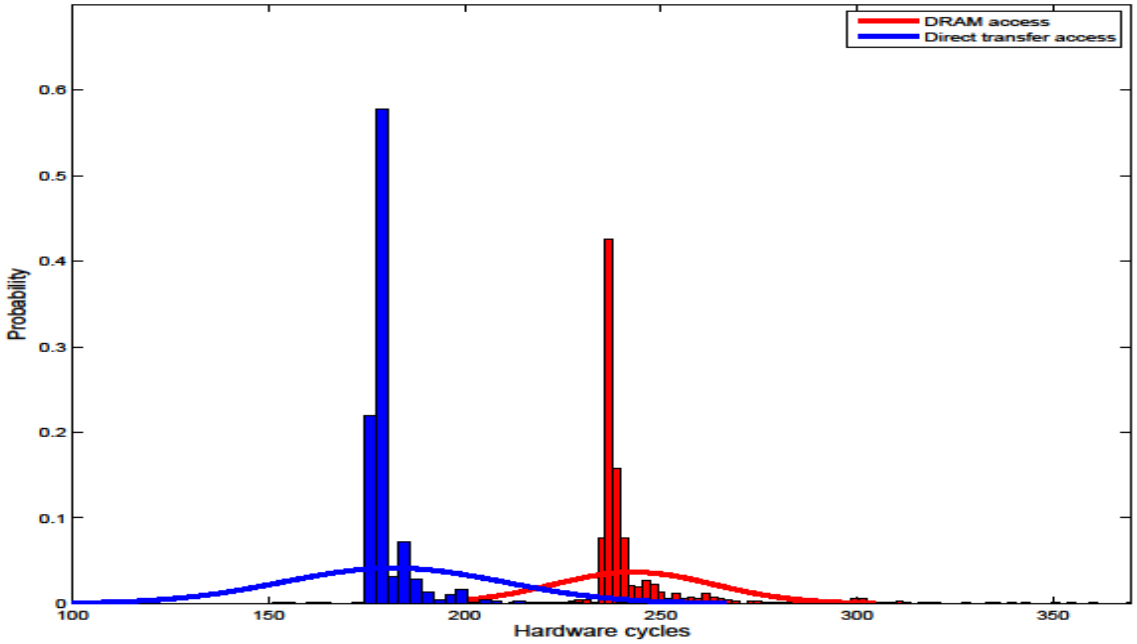
Architectural Side Channels
→difficult to prevent

LLC Covert Channel



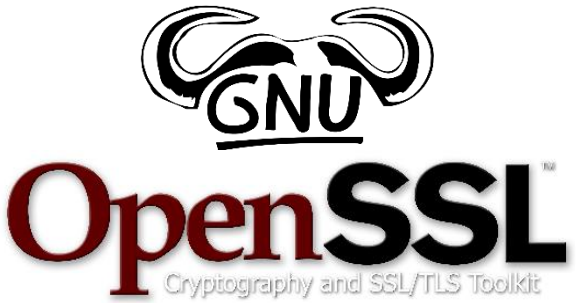
- Communicate covertly through the LLC
- P+P a predetermined cache set
- Check access times

➢ Noise prone
  - ➢ Many Neighbors
  - ➢ Variety of load
  - ➢ 40% of sets



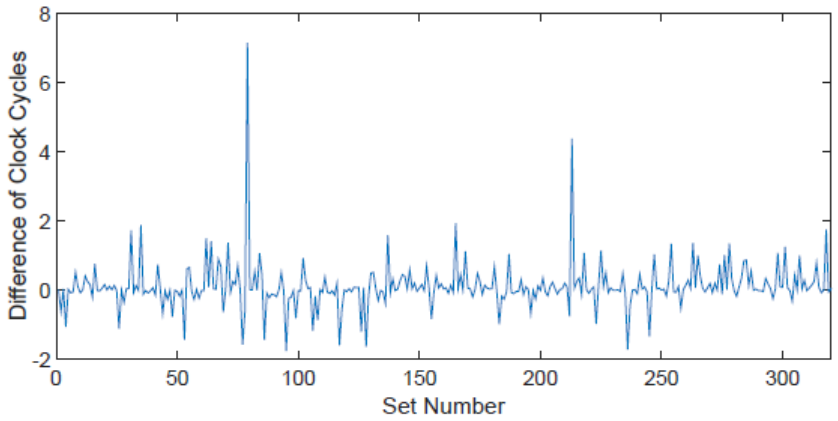
Software Profiling in LLC

- P+P to **profile** a portion of the LLC
  - Baseline profile
  - Code execution profile
- Function offset within memory page is known
  - 4K pages -> Reveal 12 bits
  - 5 bits are unknown hence 32 candidates
  - 10 cores -> 32x10 = 320 set candidates
- Tested:
  - RSA (Libgcrypt 1.6.2)
  - AES (OpenSSL 1.0.1g, C implementation)

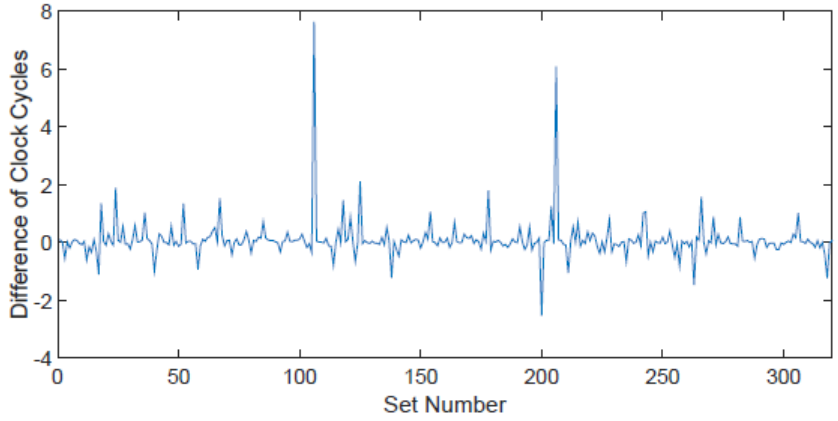


LLC Profiling: RSA Results

- Periodic pattern: Multiplication function (_gcry_mpi_powm)
- Two different co-located machines
- Two set-slice pairs have higher access times (4-8 cycles) in average 10 experiments



(a) RSA Analysis for the first co-located instance



(b) RSA Analysis for the second co-located instance

Co-location Recap

- **Targeted Scenario:**
  - LLC Covert Channel
  - Software profiling in LLC
- **Bulk Recovery Scenario:**
  - Co-location detection is **NOT** required
  - Used to detect vulnerable software

Outline

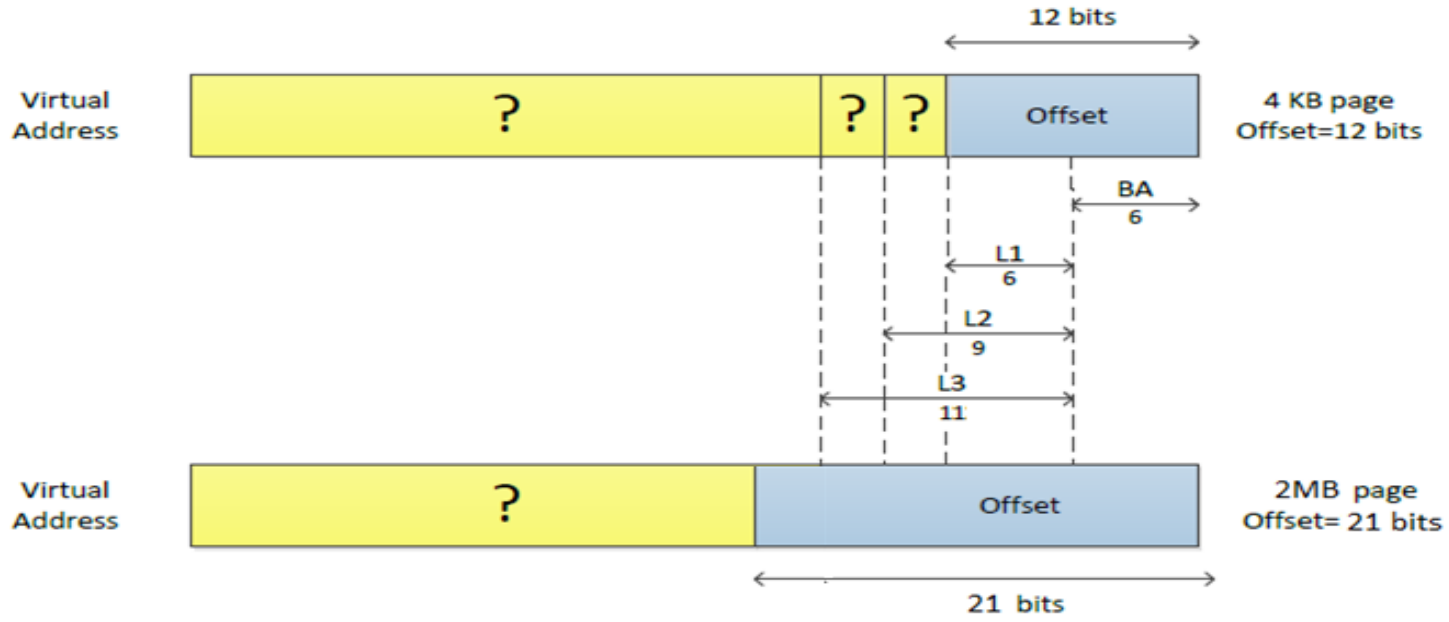
- Motivation
- Co-location Detection
- **Key Recovery Attack**
- Conclusion

P+P in Last Level Cache

How to gain control over LLC?

- Hugepages!
- Page Offset becomes 21 bits
- Eviction sets for LLC can be constructed

What about the cache slice selection?



Cache Slice Selection

f	Hash function $H(p) = h_0(p) \| \neg(nl(p)) \cdot h'_1(p) \| \neg(nl(p)) \cdot h'_2(p) \| nl(p)$
h_0	$p_{18} \oplus p_{19} \oplus p_{20} \oplus p_{22} \oplus p_{24} \oplus p_{25} \oplus p_{30} \oplus p_{32} \oplus p_{33} \oplus p_{34}$
h'_1	$p_{18} \oplus p_{21} \oplus p_{22} \oplus p_{23} \oplus p_{24} \oplus p_{26} \oplus p_{30} \oplus p_{31} \oplus p_{32}$
h'_2	$p_{19} \oplus p_{22} \oplus p_{23} \oplus p_{26} \oplus p_{28} \oplus p_{30}$
nl	$v_0 \cdot v_1 \cdot \neg(v_2 \cdot v_3)$
v_0	$p_9 \oplus p_{14} \oplus p_{15} \oplus p_{19} \oplus p_{21} \oplus p_{24} \oplus p_{25} \oplus p_{26} \oplus p_{27} \oplus p_{29} \oplus p_{32} \oplus p_{34}$
v_1	$p_7 \oplus p_{12} \oplus p_{13} \oplus p_{17} \oplus p_{19} \oplus p_{22} \oplus p_{23} \oplus p_{24} \oplus p_{25} \oplus p_{27} \oplus p_{31} \oplus p_{32} \oplus p_{33}$
v_2	$p_9 \oplus p_{11} \oplus p_{14} \oplus p_{15} \oplus p_{16} \oplus p_{17} \oplus p_{19} \oplus p_{23} \oplus p_{24} \oplus p_{25} \oplus p_{28} \oplus p_{31} \oplus p_{33} \oplus p_{34}$
v_3	$p_7 \oplus p_{10} \oplus p_{12} \oplus p_{13} \oplus p_{15} \oplus p_{16} \oplus p_{17} \oplus p_{19} \oplus p_{20} \oplus p_{23} \oplus p_{24} \oplus p_{26} \oplus p_{28} \oplus p_{30}$ $\oplus p_{31} \oplus p_{32} \oplus p_{33} \oplus p_{34}$

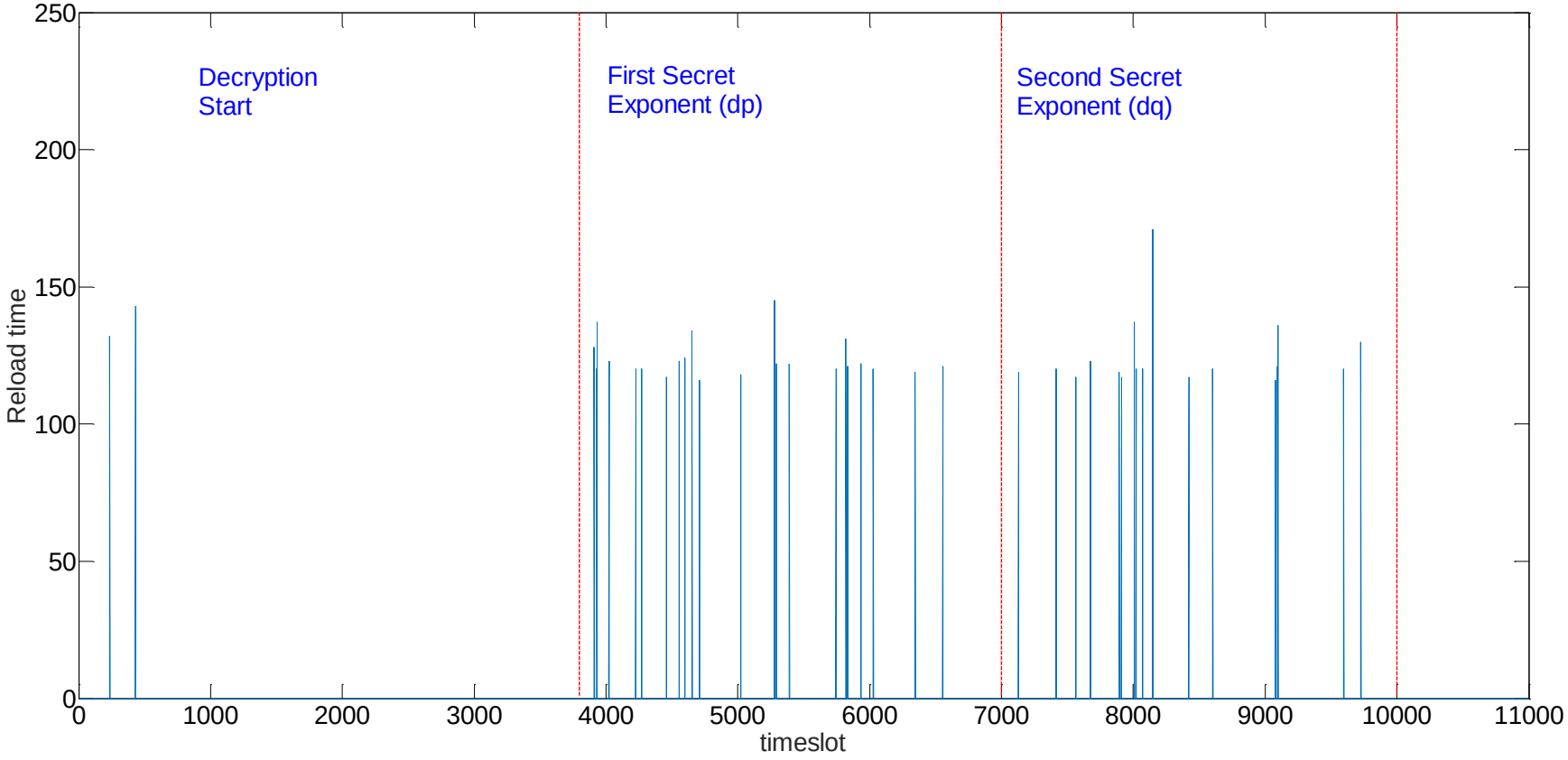
Target Cryptosystem

- Libgcrypt 1.6.2‘ s RSA implementation
  - RSA CRT with 2048 bit modulus size
  - Sliding window exponentiation (5 bits)
  - With message blinding
- **Is this state-of-the-art?**
- Libgcrypt 1.6.3 (February 2015)
  - Table accesses now satisfy constant execution flow

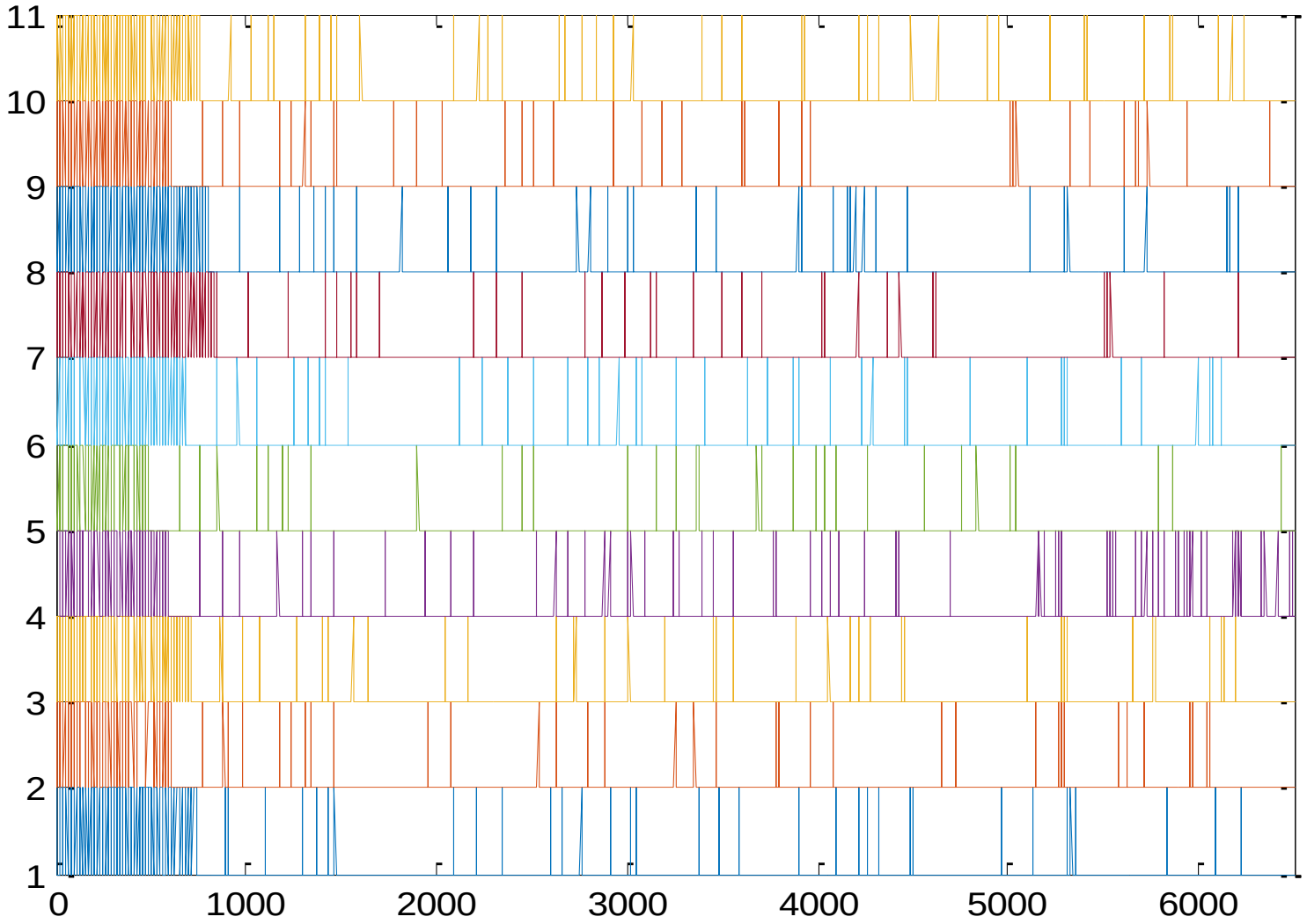
Attack Steps

1. Find cache trace of sliding window multiplicands
2. Observe several exponentiations
3. Align and process observations
4. Run error correcting key recovery to fix remaining errors

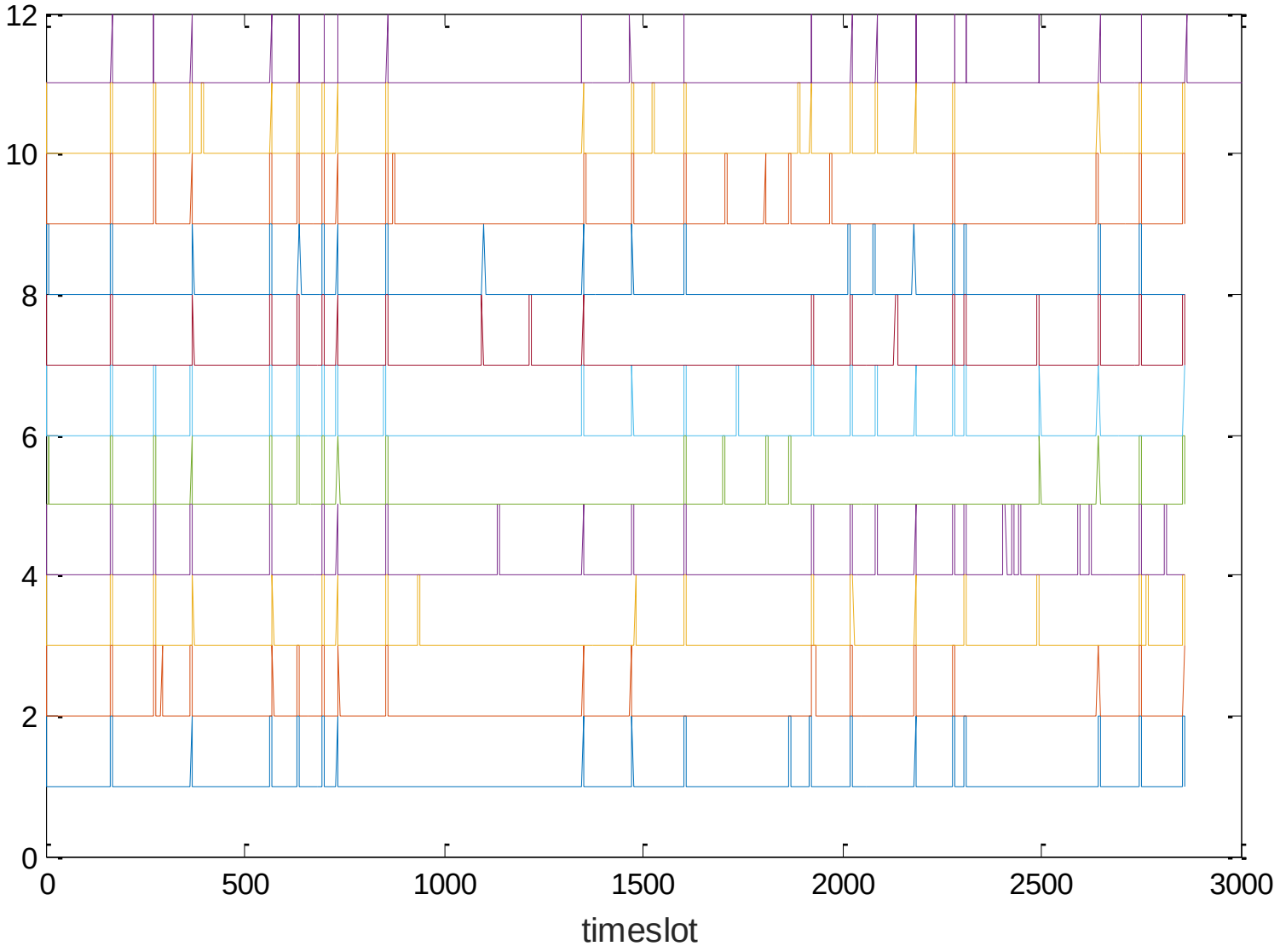
Identifying the Correct Cache Line



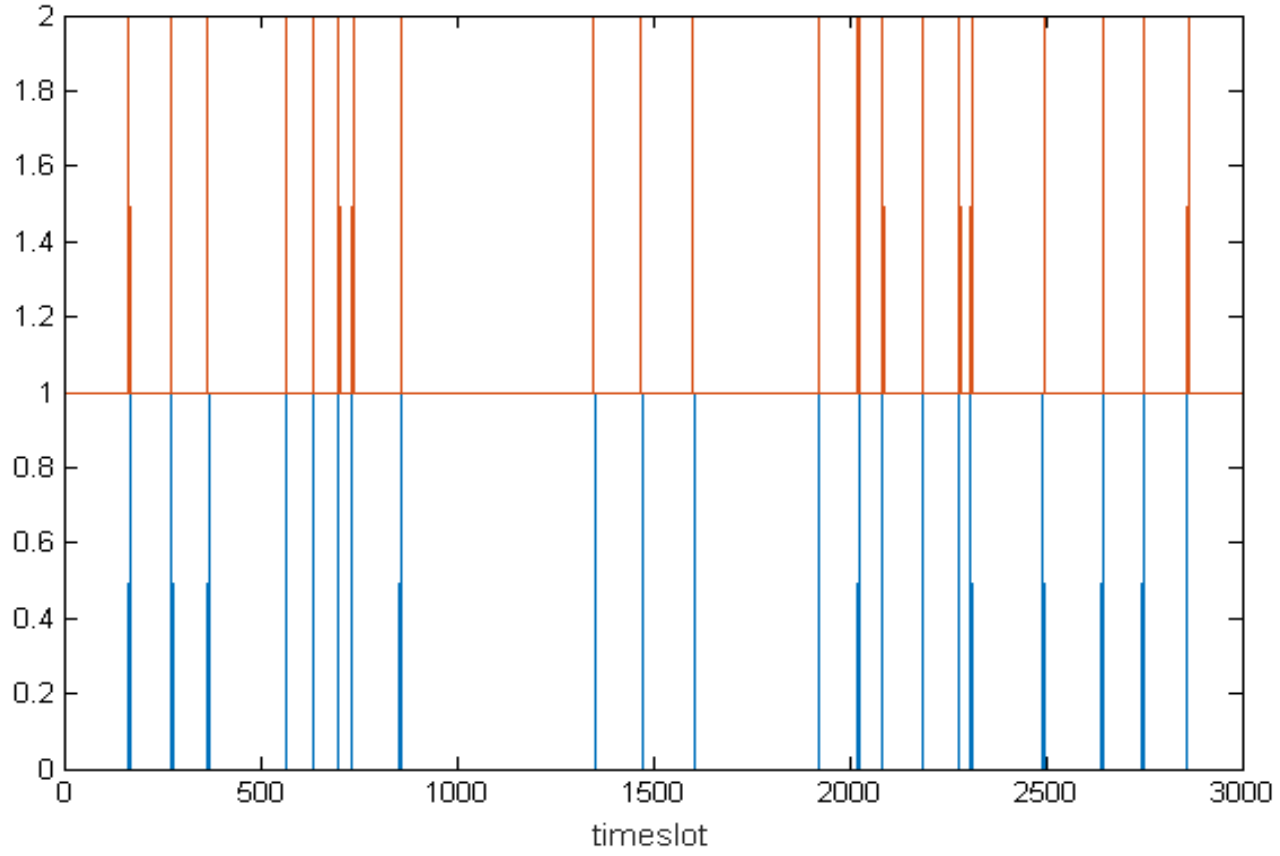
Raw Traces



After Alignment



After Alignment and Processing



- Correct (red) vs recovered (blue):

→little remaining noise

Algorithm 1 Windowed RSA Key Recovery with Noise

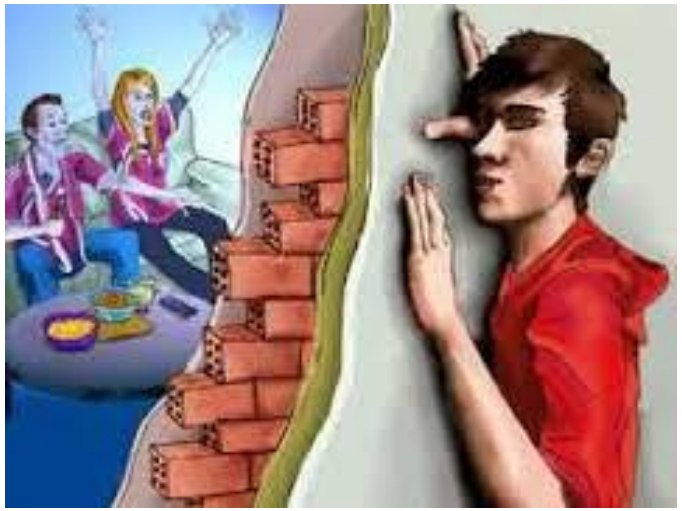
for k_p **from** 1 **to** $e-1$ **do**
  Compute $k_q = (1-k_p)(k_pN - k_p + 1)^{-1} \pmod{e}$
  while $i < |wp|$ **do**
    Process windows $wp[i], wp[i+1]$
    Introduce shifts; vary $ip[i]]$ up max_{zeros}
    for each d_p variation **do**
      Compute $X = \sum_{j=0}^{i+1} wp[j]2^{ip[j]}$
      Identify wq that overlap with $wp[i], wp[i+1]$
      Compute $Y = \sum_{j=0}^{i+1} wq[j]2^{iq[j]}$
      if $\delta(X, Y, t)$=0 **then**
        Update wp, ip, wq, iq
        Create thread for $i+1$
      end if
      if if no check succeeded **then**
        too many failures: abandon thread.
        if max_{zeros} achieved **then**
          $i = i - 1$
        end if
        Update ip, wq, iq
        Create thread for i
      end if
    end for
  end while
end for

Outline

- Motivation
- Co-location Detection
- Key Recovery Attack
- **Conclusion**

Conclusion

- Co-location can be achieved in public clouds
- Caches provide a powerful side channel
  - Key Recovery is possible!
  - Even in cloud!



- HW Countermeasures
  - Still an open problem
  - Many proposed, but cost overhead prohibitive
- SW Countermeasures
  - Recent patches of well-maintained libraries
  - Constant execution flow

NETWORKWORLD

Most read:

The Register®
Biting the hand that feeds IT

THE STACK

CLOUD

AWS customer crypto keys expo vulnerability

Alice MacGregor Fri 2 Oct 2015 11.

G+ 1 | 9 | f

Amazon has patched a vulnera flaw which could have allowed

The study revealed that a soph (EC2) instance, could have give instance.

By Brandon Butler
Network World | Oct

InformationWeek
DARKReading
CONNECTING THE INFORMATION SECURITY COMMUNITY

Radio Reports White Papers Even

ENDPOINT IoT MOBILE OPERATI

ars TECHNICA SIGN IN

RISK ASSESSMENT —

Storing secret crypto keys in the Amazon cloud? New attack can steal them

Technique allows full recovery of 2048-bit RSA key stored in Amazon's EC2 service.

DAN GOODIN - 9/28/2015, 2:55 PM

New Hack For s In Cloud

conditions, cloud giant says of

olytechnic Institute (WPI) in concept attack for stealing private ines hosted in Amazon's EC2 cloud

tware and following security best however. The cloud company

7 15 18

steal the RSA keys of other co-located

The complex attack - getting to CPU code cache isn't trivial - would, if successful, give an attacker a

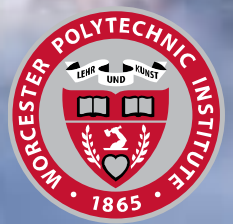
Thank you!

v.wpi.edu

msinci@wpi.edu

VERNAM Group

Security & Privacy @ WPI



WPI