Side-Channel Attacks on Everyday Applications

Taylor Hornby†‡

(With thanks to Prof. John Aycock†)

University of Calgary†

Zcash‡
Exponentiation Power Signal:
Multiplication Power Signal:
Cross-Correlation Signal:
Square Multiply Square Multiply Square ...
Figure 2. Overall architecture of our approach for reconstructing transcripts of VoIP conversations from sequences of encrypted packet sizes.
Side channels affect more than crypto.
A New Attack

- Continue the “non-crypto” trend.
- Download my code and make better attacks!
Input Distinguishing Attack

1. Victim runs a program on input A or B or C.
2. Attacker wants to know which one.
I need to look up ear infections...

Strep, ear infection, or chickenpox?

Alice

Scarlet
Interesting.

Aha! Ear infection!

Alice

Unprivileged Spy Tool

Scarlet

SSH

EAR INFECTION
Background: Flush+Reload
Flush+Reload Breaking Crypto

- 2014: “Recovering OpenSSL ECDSA Nonces Using the Flush+Reload Cache Side-Channel Attack”
- 2014: “Wait a Minute! A fast, Cross-VM Attack on AES”
- Lots more!
But Flush+Reload can do more.
Cross-Tenant Side-Channel Attacks in PaaS Clouds

Yinqian Zhang  
University of North Carolina  
Chapel Hill, NC, USA  
yinqian@cs.unc.edu

Ari Juels  
Cornell Tech (Jacobs Institute)  
New York, NY, USA  
juels@cornell.edu

Michael K. Reiter  
University of North Carolina  
Chapel Hill, NC, USA  
reiter@cs.unc.edu

Thomas Ristenpart  
University of Wisconsin  
Madison, WI, USA  
rist@cs.wisc.edu

ABSTRACT

We present a new attack framework for conducting cache-based side-channel attacks and demonstrate this framework in attacks between tenants on commercial Platform-as-a-Service (PaaS) clouds. Our framework uses the FLUSH-RELOAD attack of Gullasch et al. as a primitive, and extends this work by leveraging it within an automaton-driven strategy for tracing a victim’s execution. We leverage our framework first to confirm co-location of tenants and then in the form of interpreted source (e.g., PHP, Ruby, Node.js, Java) or application executables that are then executed in a provider-managed host OS shared with other customers’ applications. As such, a PaaS cloud often leverages OS-based techniques such as Linux containers to isolate tenants, in contrast to hypervisor-based techniques common in Infrastructure-as-a-Service (IaaS) clouds.

A continuing, if thus far largely hypothetical, threat to cloud tenant security is failures of isolation due to side-
Cache Template Attacks:
Automating Attacks on Inclusive Last-Level Caches

Daniel Gruss, Raphael Spreitzer, and Stefan Mangard
Graz University of Technology, Austria

Abstract
Recent work on cache attacks has shown that CPU caches represent a powerful source of information leakage. However, existing attacks require manual identification of vulnerabilities in data structures in instruction...

Flush+Reload by Y. Yaram, K. Falkner.
Flush+Reload by Y. Yaram, K. Falkner.

Diagram showing the relationship between Alice Virtual, Scarlet Virtual, CACHE, DRAM, and RO.
Flush+Reload by Y. Yaram, K. Falkner.
Flush+Reload by Y. Yaram, K. Falkner.
foo() {
    ...
}

bar() {
    ...
}

baz() {
    ...
}
foo() {
  ...
}

bar() {
  ...
}

baz() {
  ...
}
Flush+Reload by Y. Yaram, K. Falkner.

```c
foo() {
    ...
}

bar() {
    ...
}

baz() {
    ...
}
```
foo() {
  ...
}

bar() {
  ...
}

baz() {
  ...
}
foo() {
    ...
}

bar() {
    ...
}

baz() {
    ...
}
foo() {
      ...
}

bar() {
      ...
}

baz() {
      ...
}
Interesting.

Aha! Ear infection!

Alice

Unprivileged Spy Tool

Scarlet
Put “light bulbs” on the HTML parser:

- html_stack_item()
- html_stack_dup()
- html_a()
- parse_html()
Goal: Recognize this as the *Ear Infection* Wikipedia page.
Attack Stages:

1. Training - Scarlet spies on herself.
2. Spying - Scarlet spies on Alice.
3. Identification - Most similar by Levenshtein distance.
Stage 1: Training

- Strep throat
- Ear infection
- Chickenpox
Stage 1: Training

- Strep throat
- Ear infection
- Chickenpox
Stage 1: Training

- Strep throat
- Ear infection
- Chickenpox
Stage 1: Training

- Strep throat
- Ear infection
- Chickenpox
Stage 1: Training

- Strep throat
- Ear infection
- Chickenpox
Stage 1: Training

- Strep throat
- Ear infection
- Chickenpox
Stage 1: Training

- Strep throat
- Ear infection
- Chickenpox
Stage 1: Training

- Strep throat
- Ear infection
- Chickenpox
Stage 1: Training

- Strep throat
- Ear infection
- Chickenpox
Stage 2: Spying

- Strep throat
- Ear infection
- Chickenpox
Stage 3: Identification

- Strep throat
- Ear infection
- Chickenpox
Stage 3: Identification

- Strep throat
- Ear infection
- Chickenpox

Output: “Ear infection”
>90% Success

(100 pages, 10 samples)
It’s demo time.
Q&A

https://defuse.ca/BH2016