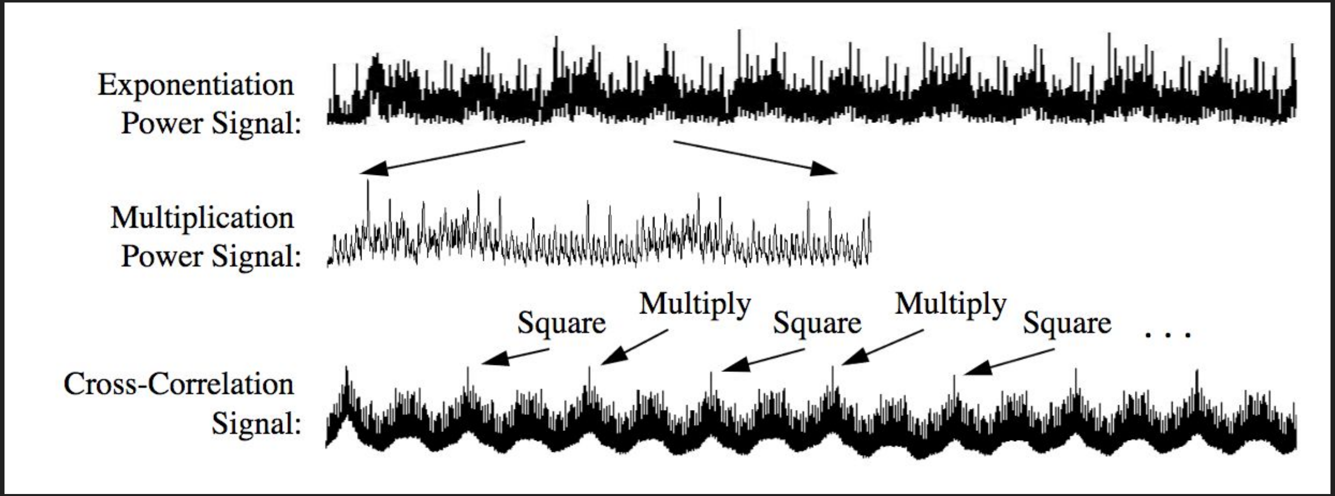
Side-Channel Attacks on Everyday Applications

Taylor Hornby[†‡]

(With thanks to Prof. John Aycock[†])

University of Calgary[†]

Zcash[‡]



T. Messerges et al. *CHES,* 1999.

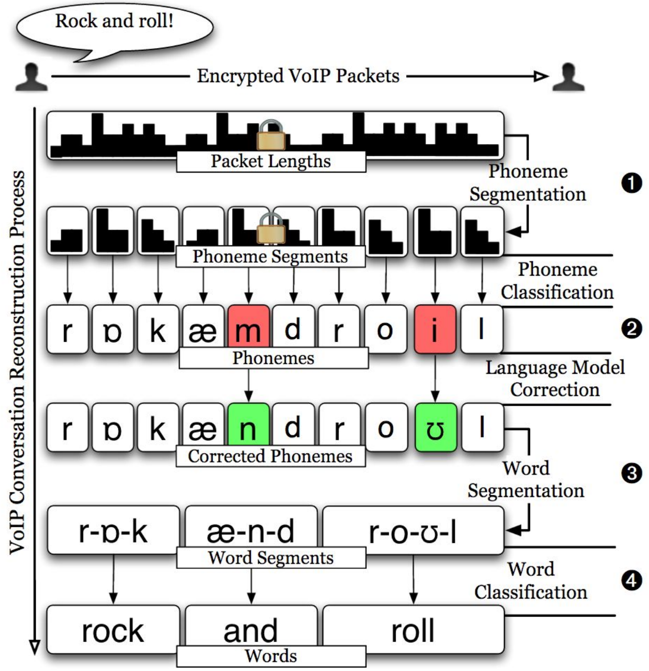
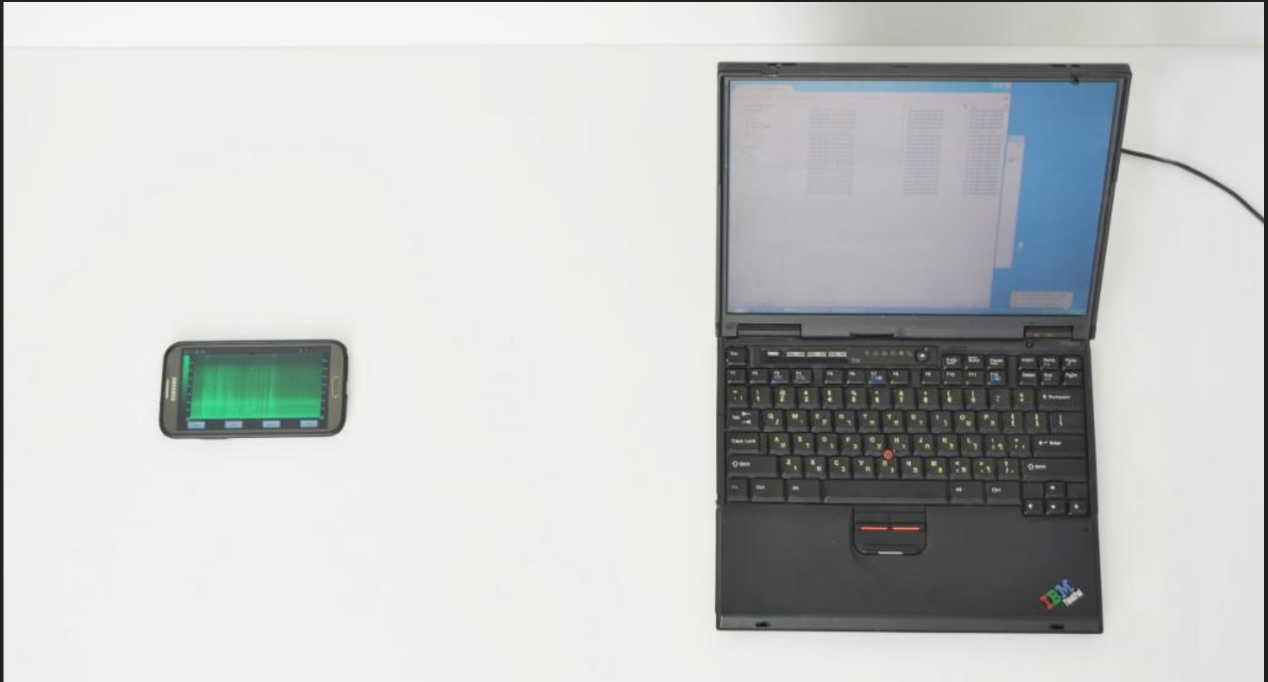


Figure 2. Overall architecture of our approach for reconstructing transcripts of VoIP conversations from sequences of encrypted packet sizes.

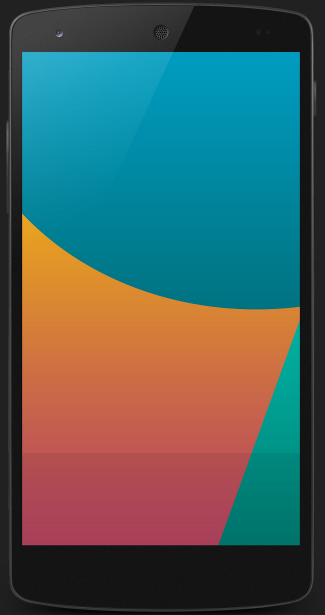
A. White et al. *IEEE S&P*, 2011.

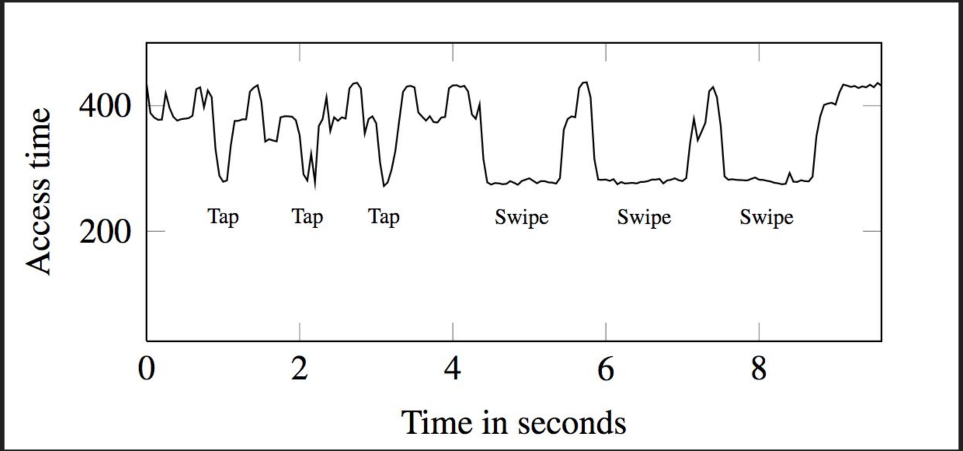


D. Genkin et al. *CRYPTO*, 2014.

Side channels affect more than crypto.

M. Backes, et al. *USENIX Security*, 2010.

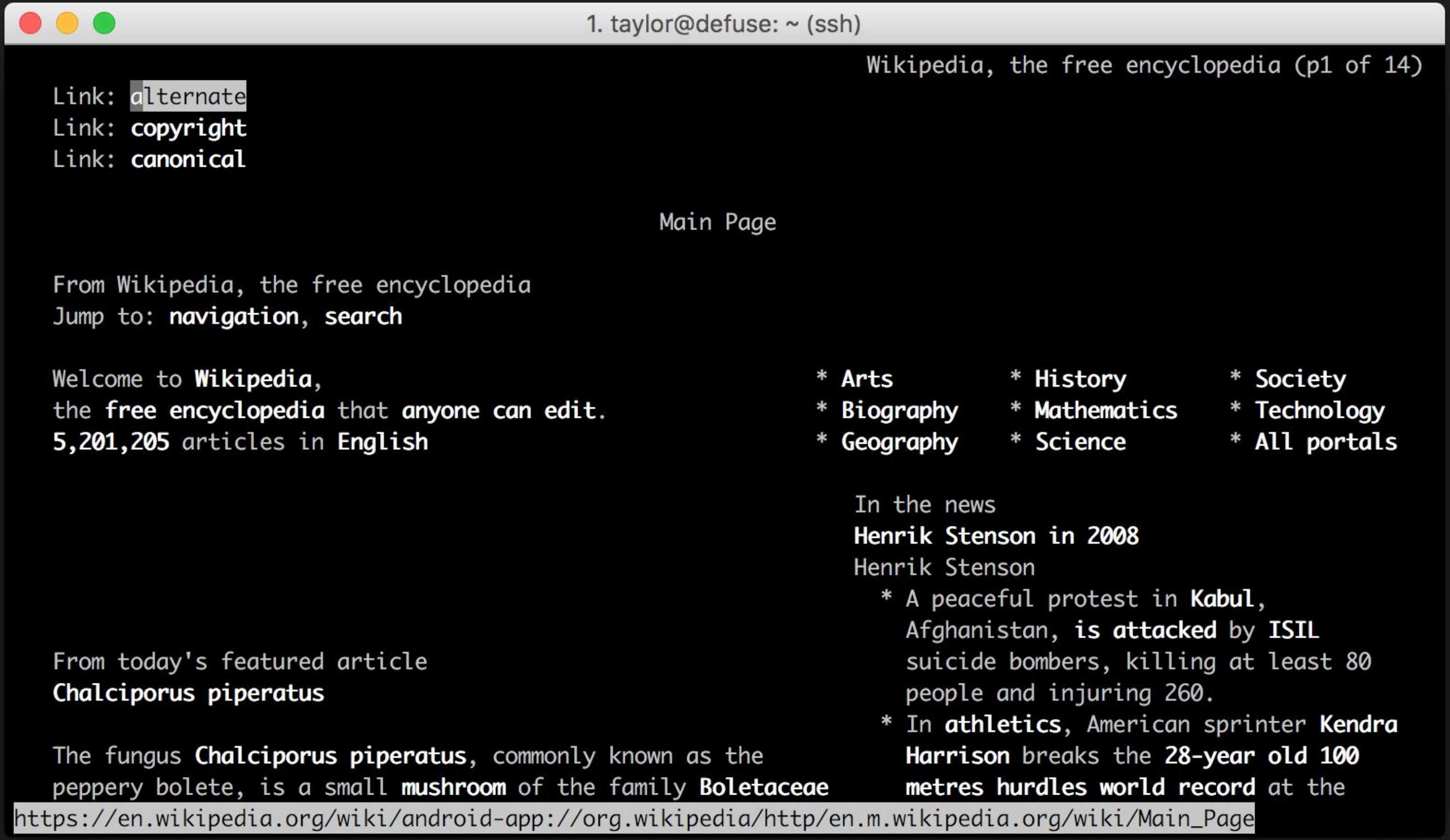




M. Lipp et al. *USENIX Security*, 2016.

A New Attack

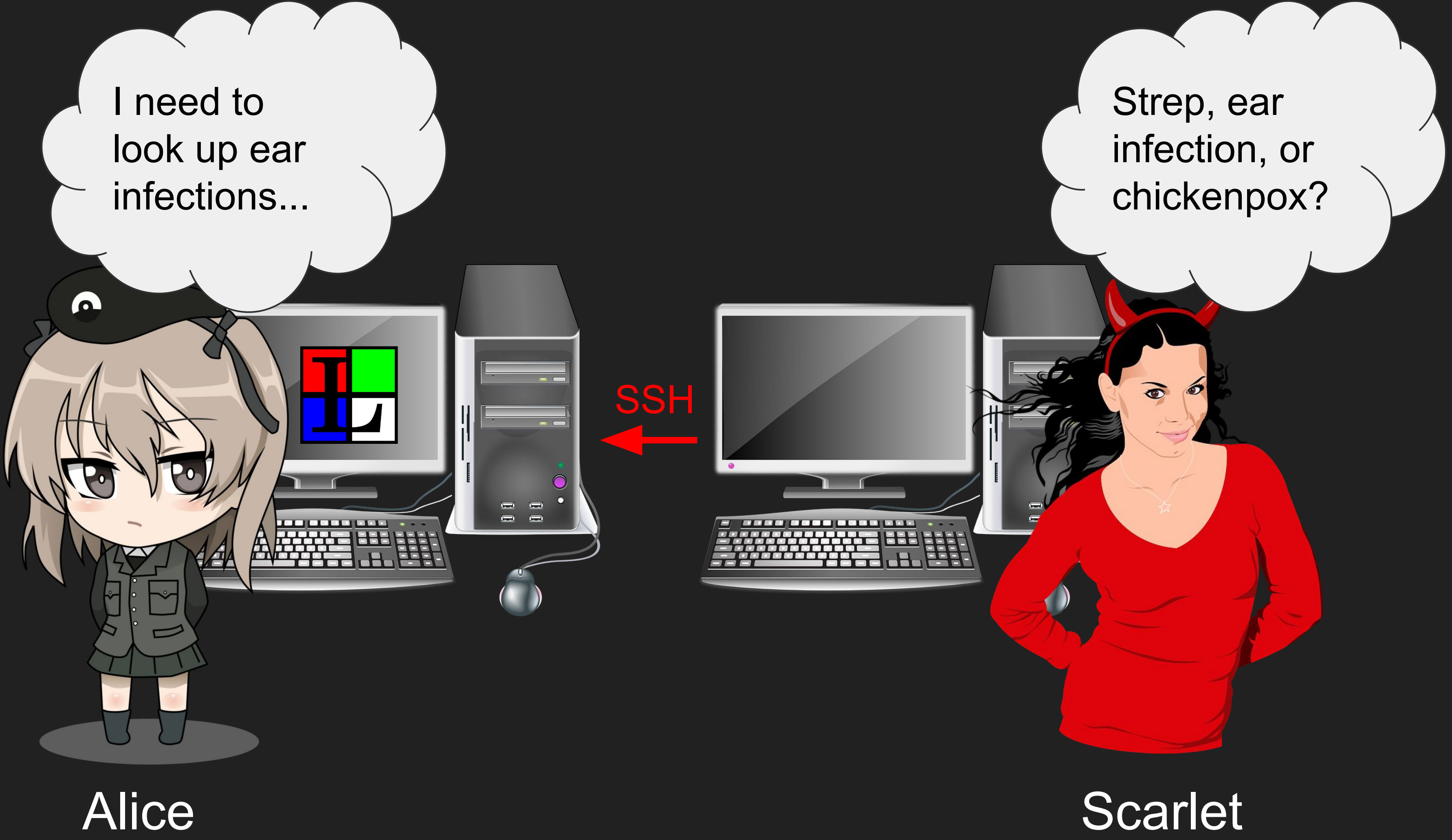
- Continue the “non-crypto” trend.
- Download my code and make better attacks!

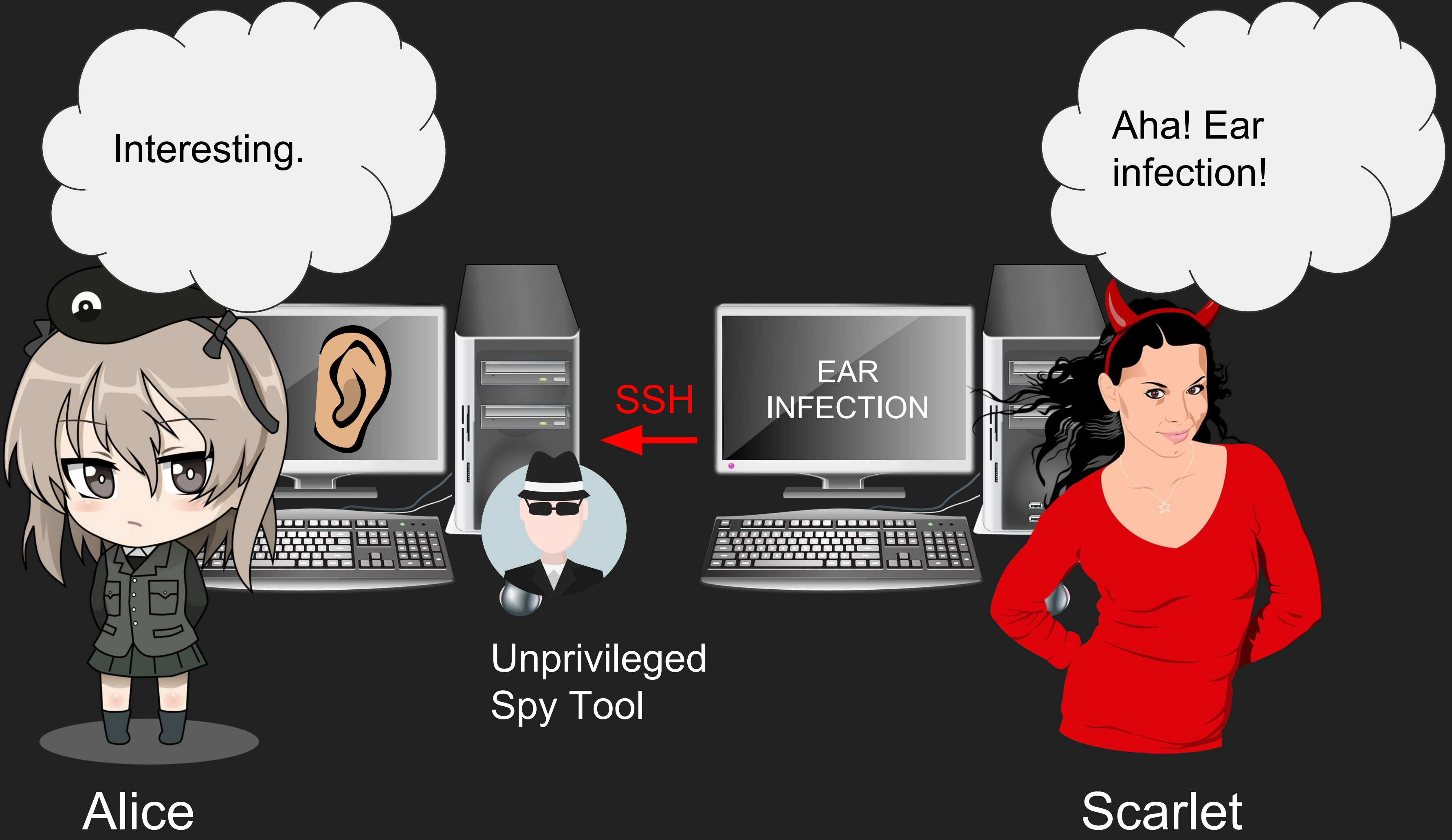


```
                                      Wikipedia, the free encyclopedia (p1 of 14)
   Link: alternate
   Link: copyright
   Link: canonical

                                   Main Page

   From Wikipedia, the free encyclopedia
   Jump to: navigation, search

   Welcome to Wikipedia,                             * Arts        * History       * Society
   the free encyclopedia that anyone can edit.       * Biography   * Mathematics   * Technology
   5,201,205 articles in English                     * Geography   * Science       * All portals

                                                       In the news
                                                       Henrik Stenson in 2008
                                                       Henrik Stenson
                                                         * A peaceful protest in Kabul,
                                                           Afghanistan, is attacked by ISIL
   From today's featured article                           suicide bombers, killing at least 80
   Chalciporus piperatus                                   people and injuring 260.
                                                         * In athletics, American sprinter Kendra
   The fungus Chalciporus piperatus, commonly known as the  Harrison breaks the 28-year old 100
   peppery bolete, is a small mushroom of the family Boletaceae  metres hurdles world record at the
https://en.wikipedia.org/wiki/android-app://org.wikipedia/http/en.m.wikipedia.org/wiki/Main_Page
```

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?
SSH
Alice
Scarlet

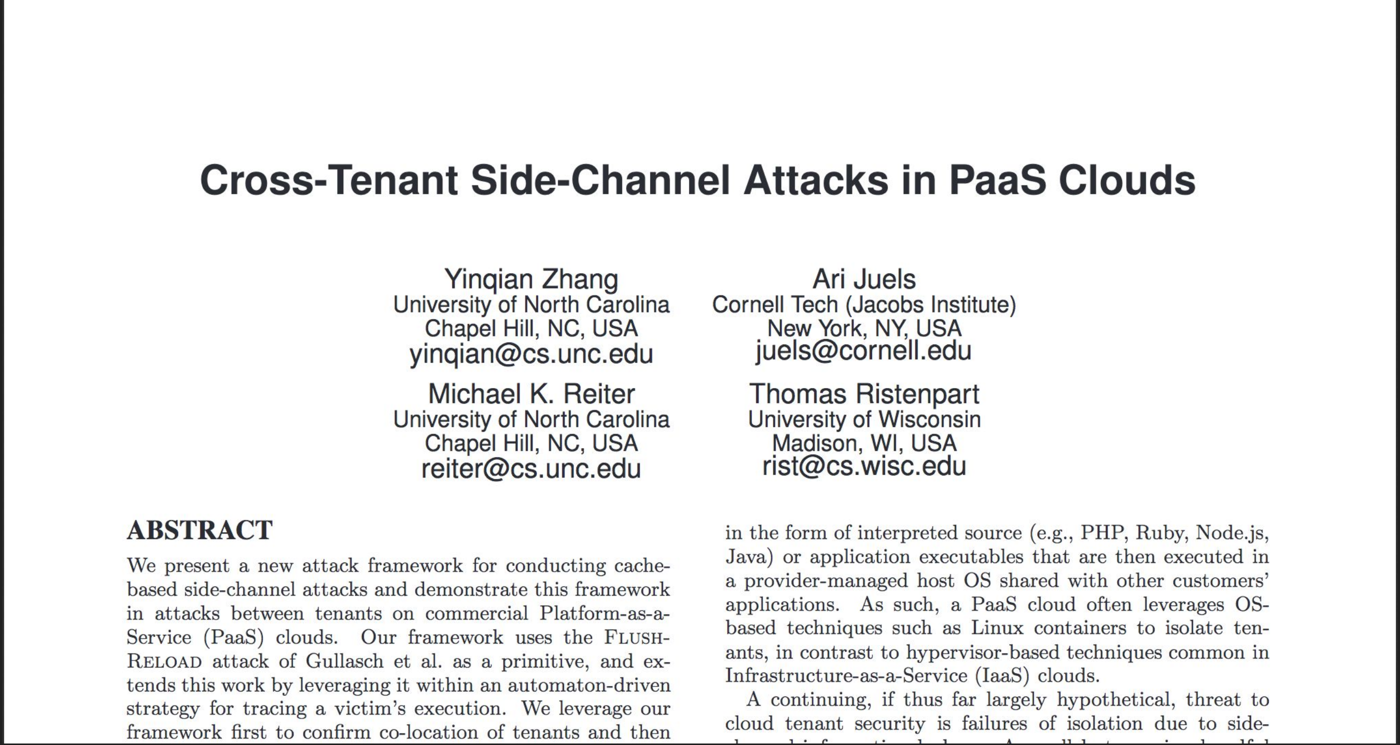

Interesting.
Aha! Ear infection!
SSH
EAR INFECTION
Unprivileged Spy Tool
Alice
Scarlet

Background: Flush+Reload

Flush+Reload Breaking Crypto

- 2013/2014: “Flush+Reload: A High-Resolution, Low Noise, L3 Cache Side Channel Attack.
- 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

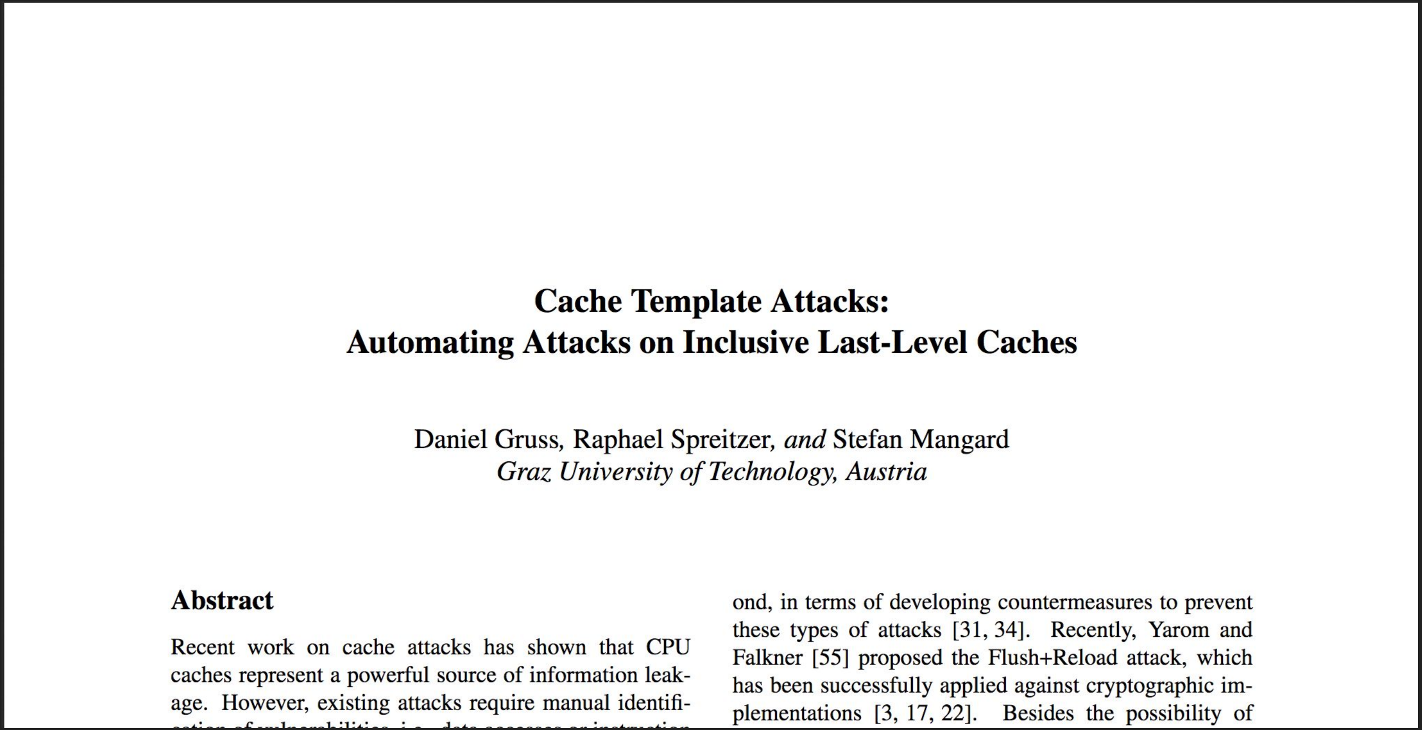
ABSTRACT

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-

Y. Zhang et al. *CCS*, 2014.



Cache Template Attacks:
Automating Attacks on Inclusive Last-Level Caches

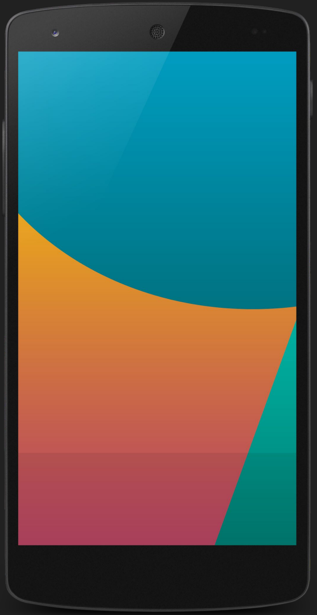
Daniel Gruss, Raphael Spreitzer, *and* Stefan Mangard
Graz University of Technology, Austria

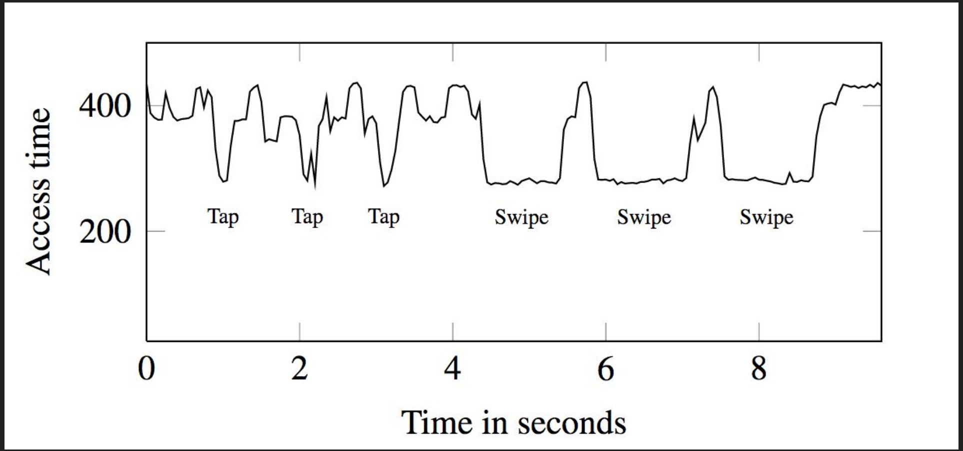
Abstract

Recent work on cache attacks has shown that CPU caches represent a powerful source of information leakage. However, existing attacks require manual identifi-

ond, in terms of developing countermeasures to prevent these types of attacks [31, 34]. Recently, Yarom and Falkner [55] proposed the Flush+Reload attack, which has been successfully applied against cryptographic implementations [3, 17, 22]. Besides the possibility of

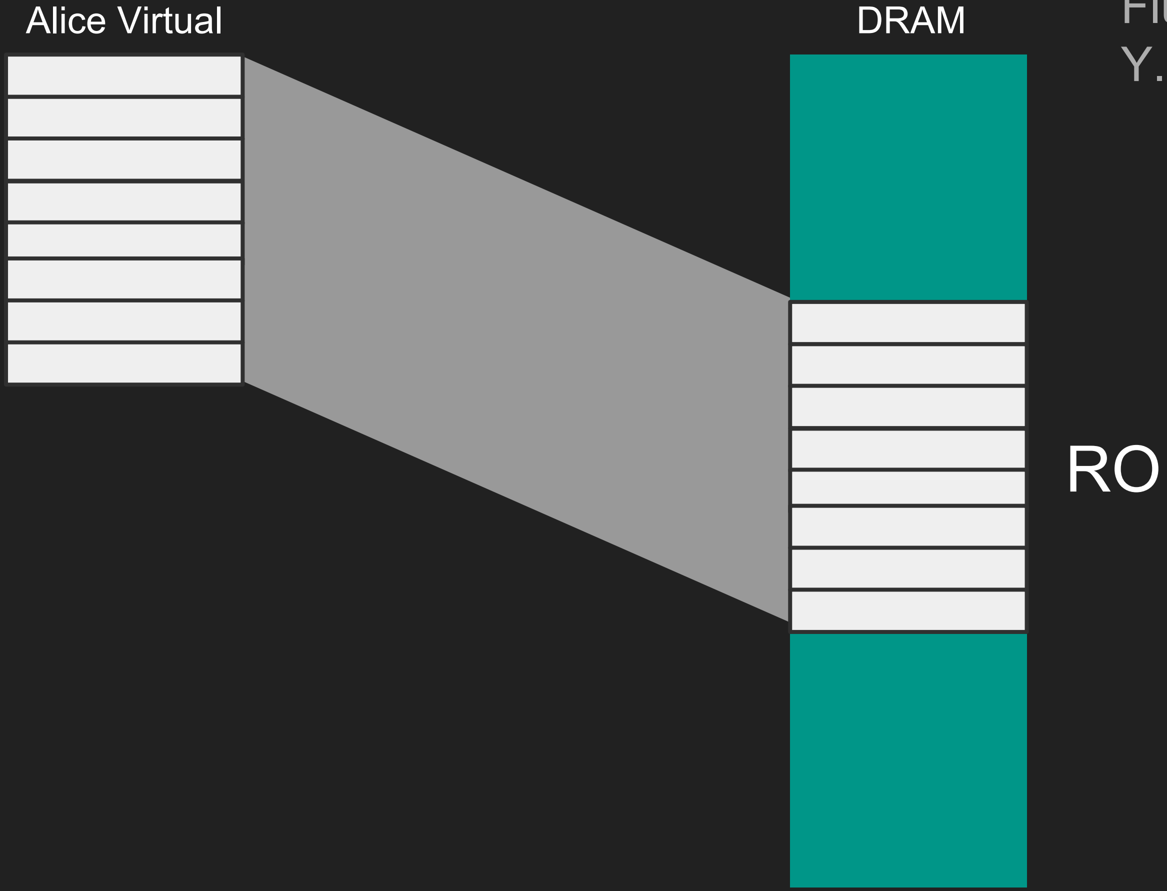
D. Gruss et al. *USENIX Security,* 2015.



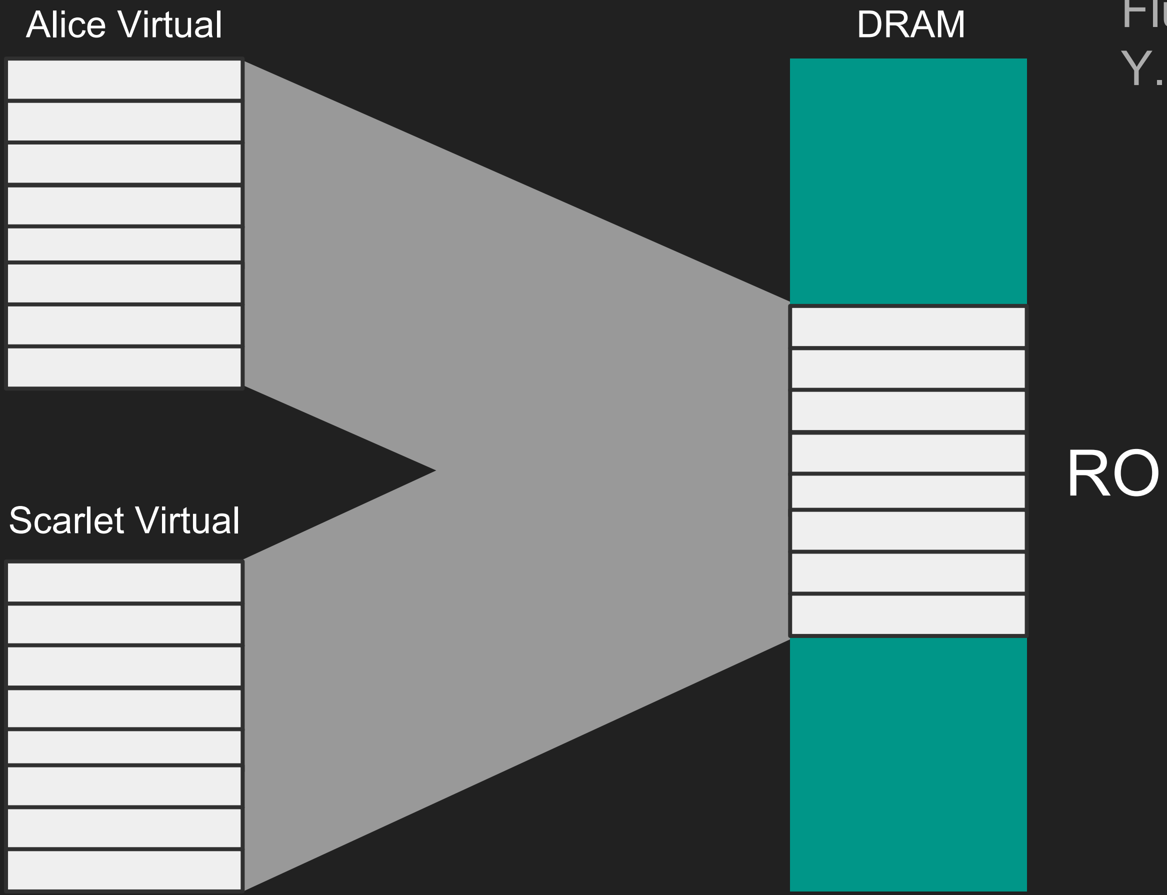


M. Lipp et al. *USENIX Security*, 2016.

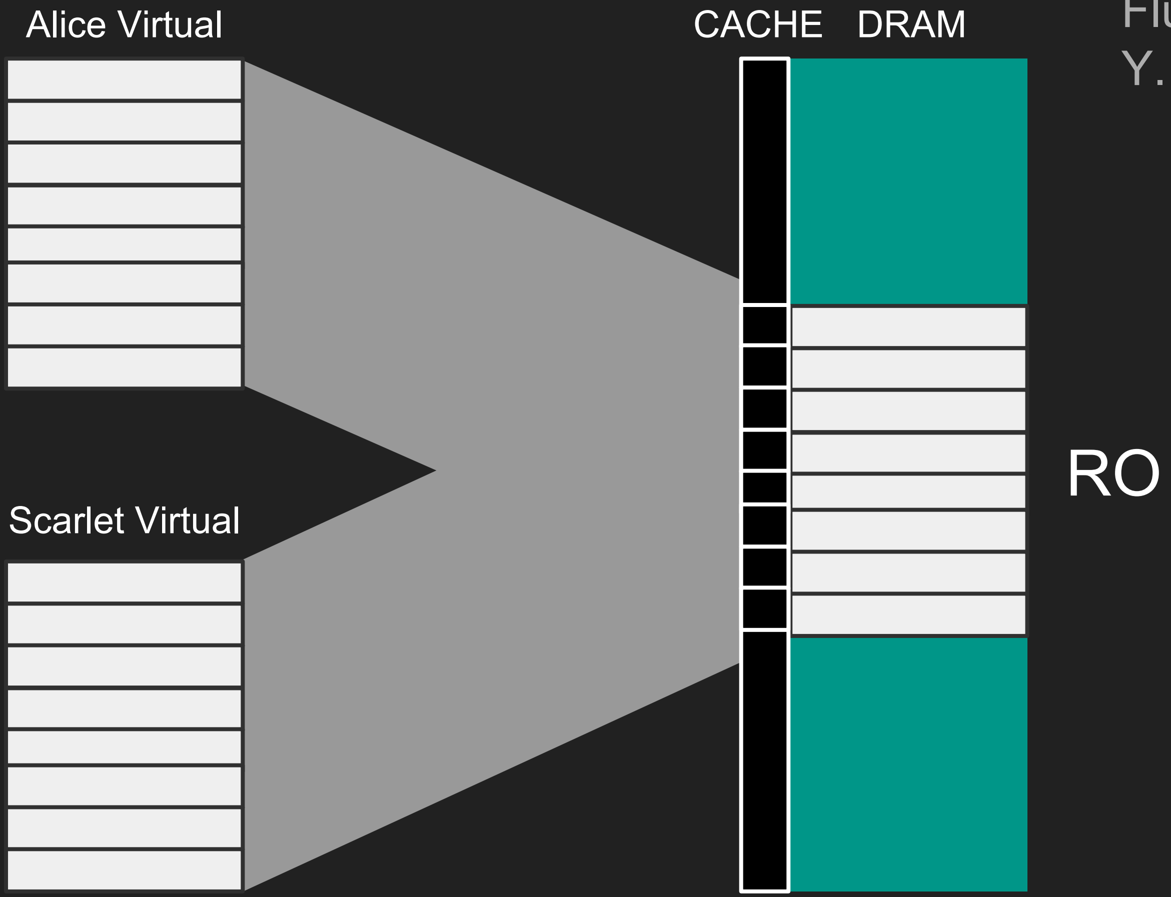
Flush+Reload by
Y. Yaram, K. Falkner.



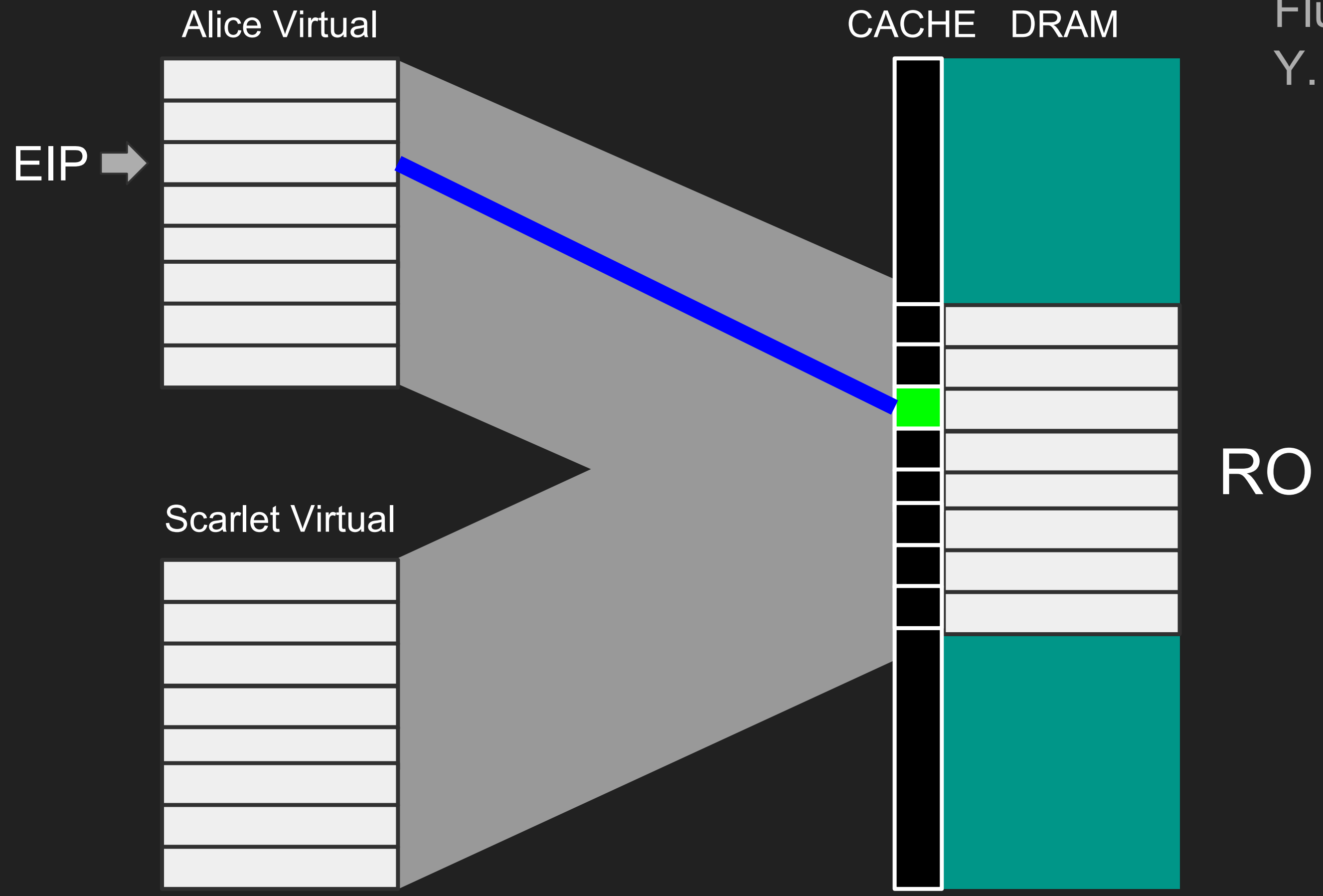
Flush+Reload by
Y. Yaram, K. Falkner.



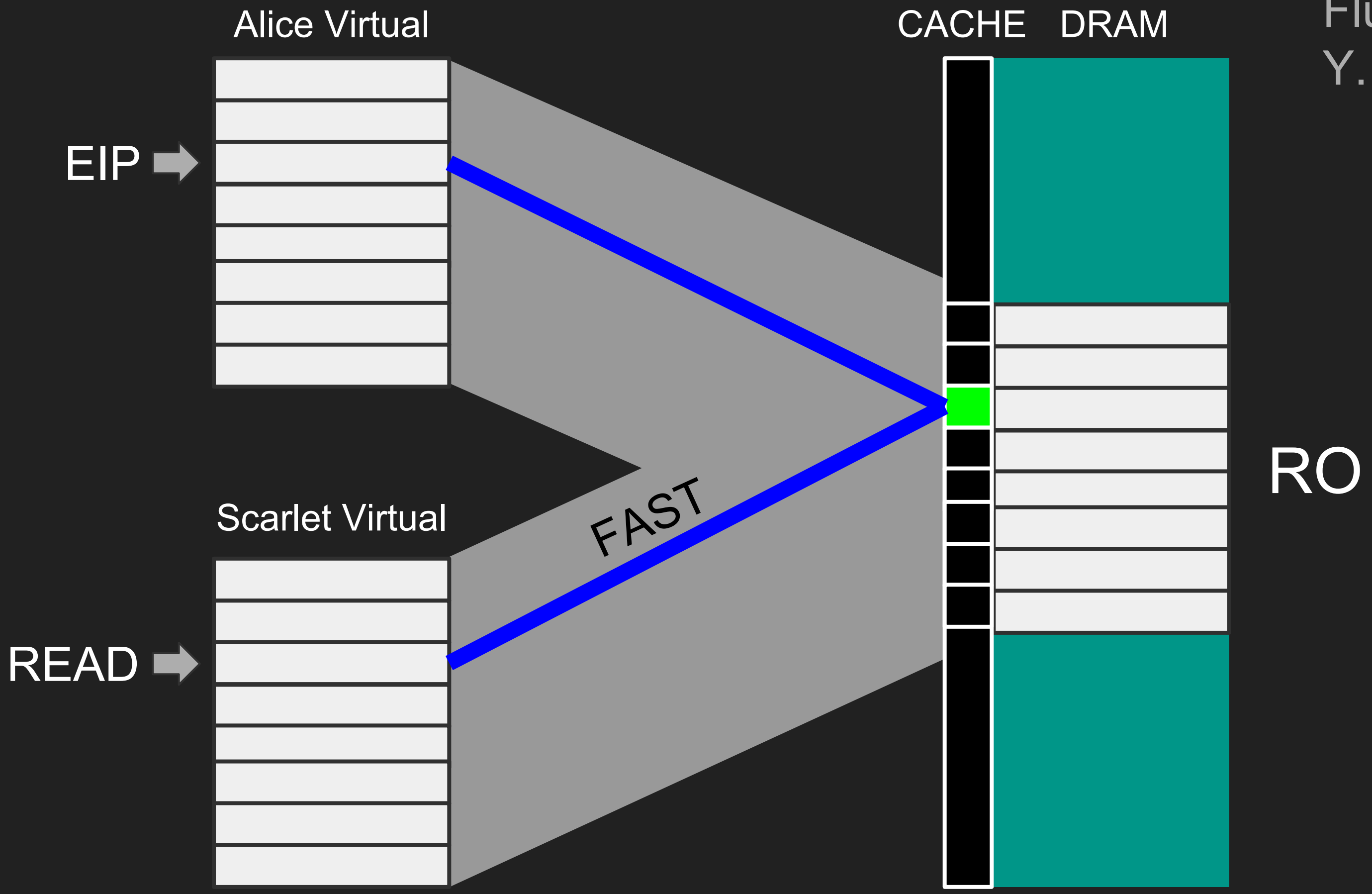
Flush+Reload by
Y. Yaram, K. Falkner.

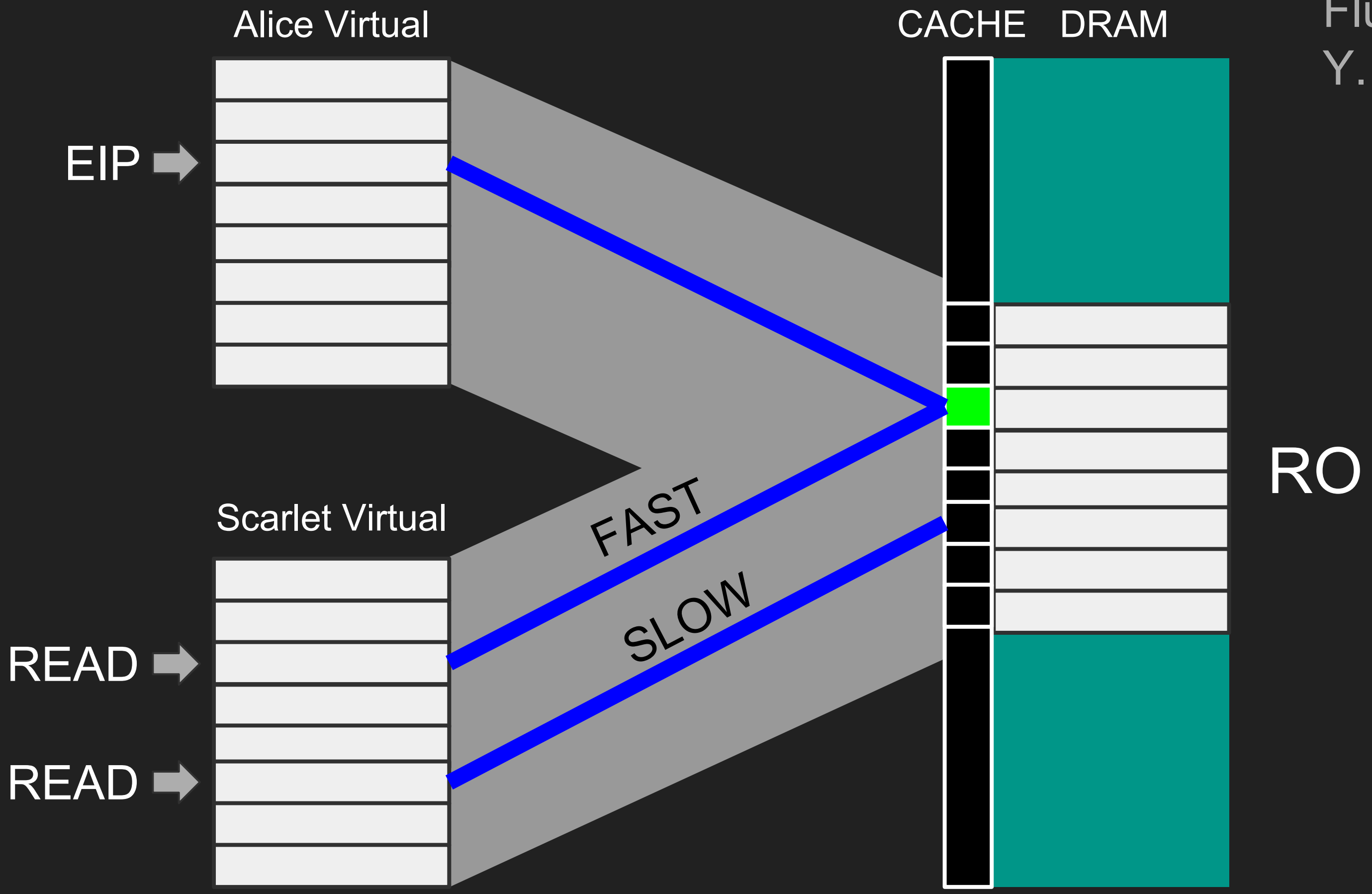


Flush+Reload by
Y. Yaram, K. Falkner.



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

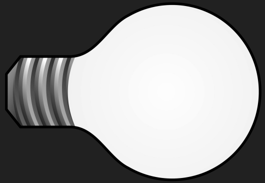




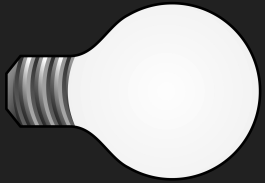
Flush+Reload by
Y. Yaram, K. Falkner.

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

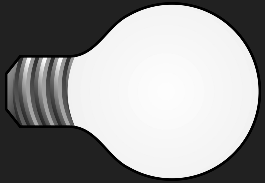
```
foo() {
    ...
}
```



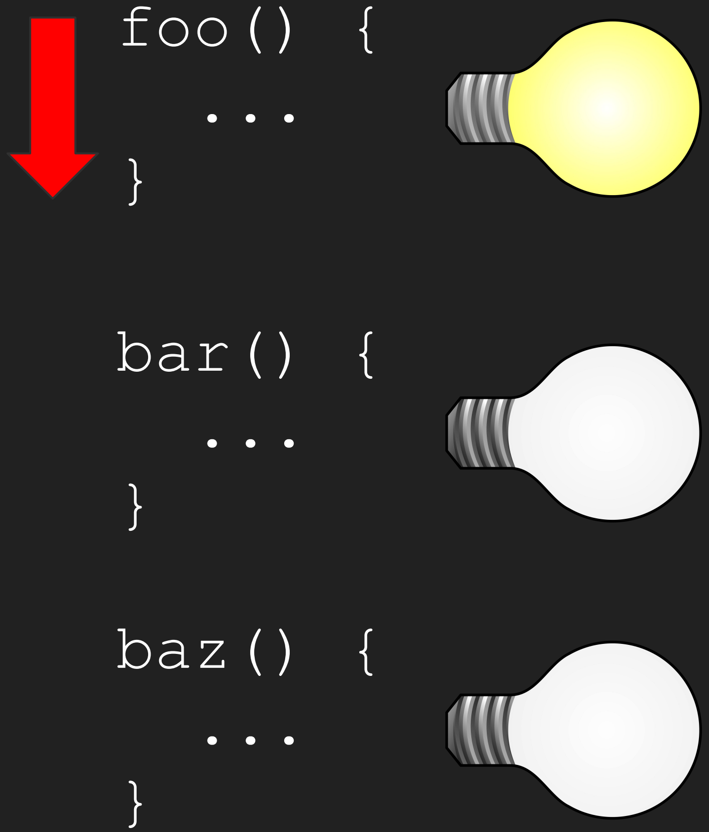
```
bar() {
    ...
}
```



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



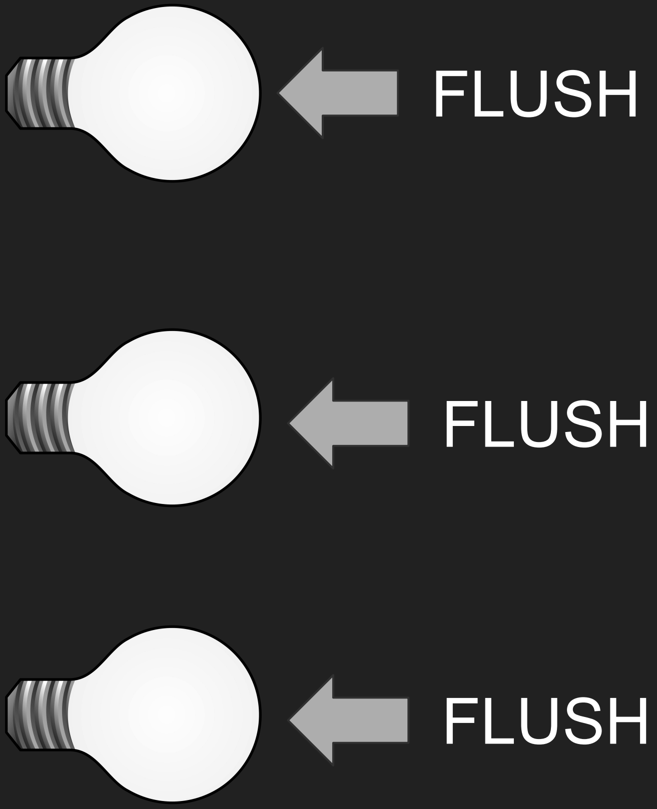
Flush+Reload by
Y. Yaram, K. Falkner.



```
foo() {
    ...
}

bar() {
    ...
}

baz() {
    ...
}
```

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

```
foo() {
   ...
}

bar() {
   ...
}

baz() {
   ...
}
```

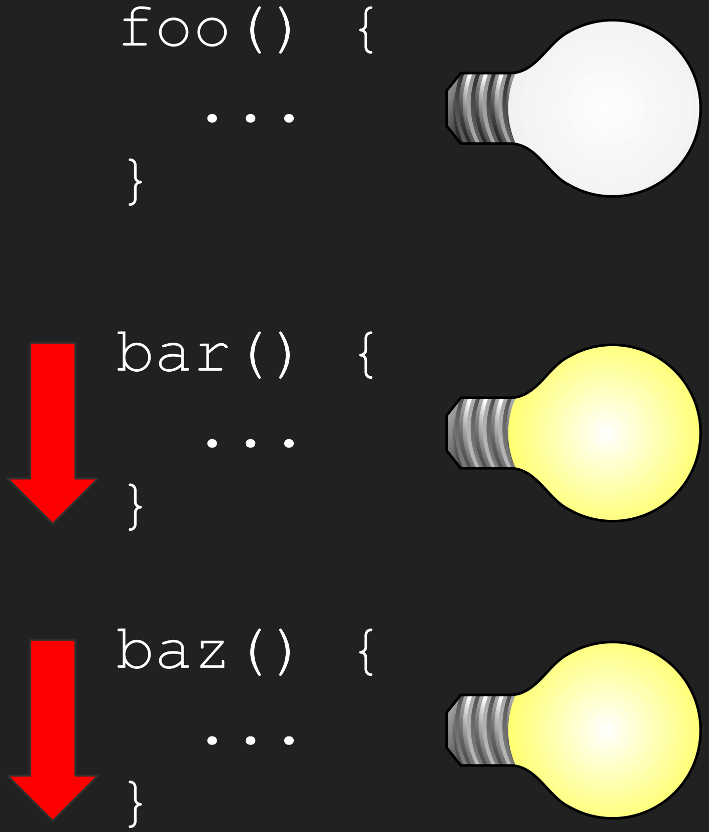


FLUSH

FLUSH

FLUSH

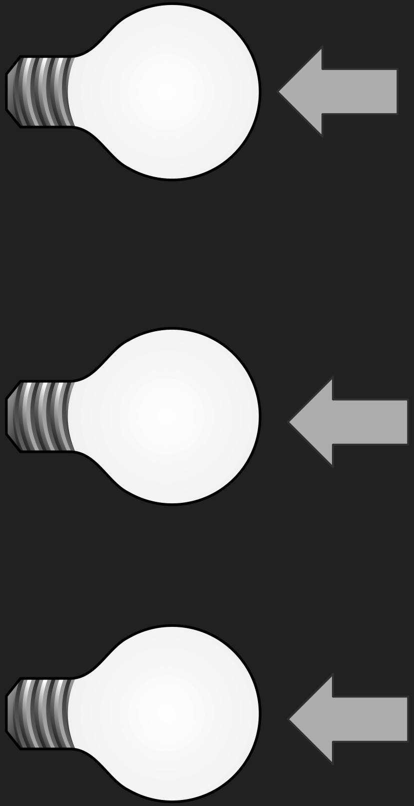
Flush+Reload by
Y. Yaram, K. Falkner.



```
foo() {
   ...
}

bar() {
   ...
}

baz() {
   ...
}
```

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

```
foo() {
   ...
}


bar() {
   ...
}

baz() {
   ...
}
```

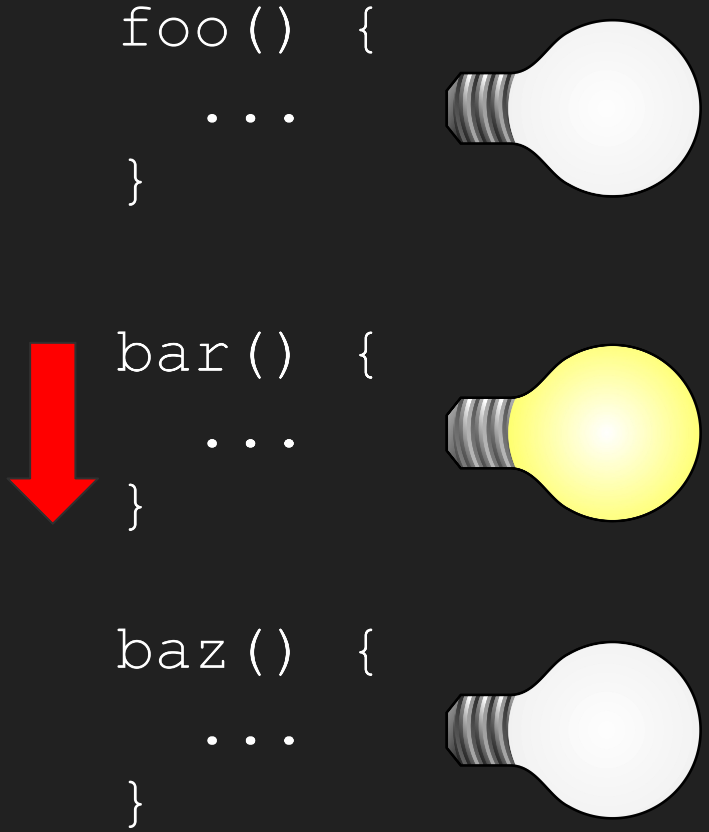


FLUSH

FLUSH

FLUSH

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



```
foo() {
    ...
}

bar() {
    ...
}

baz() {
    ...
}
```

Interesting.
Aha! Ear infection!
SSH
EAR INFECTION
Unprivileged Spy Tool

Alice

Scarlet

Put “light bulbs” on the HTML parser:

- html_stack_item()
- html_stack_dup()
- html_a()
- parse_html()

```
BDBCBCABABABACBABABCBABACBABCACABCBCACACABCABABCABCACABCBCABACACADBABDBCABDBCACB
CABDBCABDBCABDBCABCABCBCBCABCACABDCBDBCBABABDCBDBCABDACBDBCBCBABABCBCABCACBCBCBA
CBABACBACBABDBCABDBCABDBCABCBCBCBCABCABCBCABDABDCBCACBCACACBCABDABDBCABDBCABDBCB
CABCABDBCABDBCABCABDBCABDBCABCABDBCABDBCABCABDBCABDBCABCABCBDBCABDBCABABDBCACBCA
BCBCABCABDBDBCBCABCABDABDBCBCABCABCBCABCABCABDBCABDACBDBCABDBCABACBDBCABDBCABDCA
BDBCBCABCACBCABCABDBCABCABDABCBCABDBCBCBABABCBCABCABCBCBCBABACABABACBABDACBDBCAB
DBCABDBCBCABCBCABCBCABCABCBCABDBDBCBCABCABCABCACABDACBDCACBDCACBDBCBCACBCBCABDBC
ABDBCACBCABDBCABDBCBCABCABDBCABCABDCABDCABCACBCBCABDADBCBCABDBCABCABCACBCACBCACA
BDABDBCABCBCABCABDBCBCACBCBCABCABCABCABCBDBCABDBCABACBDBCABDBCABDBCABDBCABCABCAC
BCABABCBCACBABCABDBDBCBCBCBACBABACBABCABCABCBCBCBCABABACBACBABCABDABCACBDABCABDA
BCBCABACABCBCABABCABCBCABCBCABDABCBACACACABACABDBDBCABDBCABDBABCABCBCABDBACABDBA
BCABACABACABDABCBACABCABDBCBACABDBACABDBABABCABCABCABABDBCBCABDABCABCBCBABCBCBAC
ABDBCABCABCBCABDABCABCABCABCABACABCBCABD
```

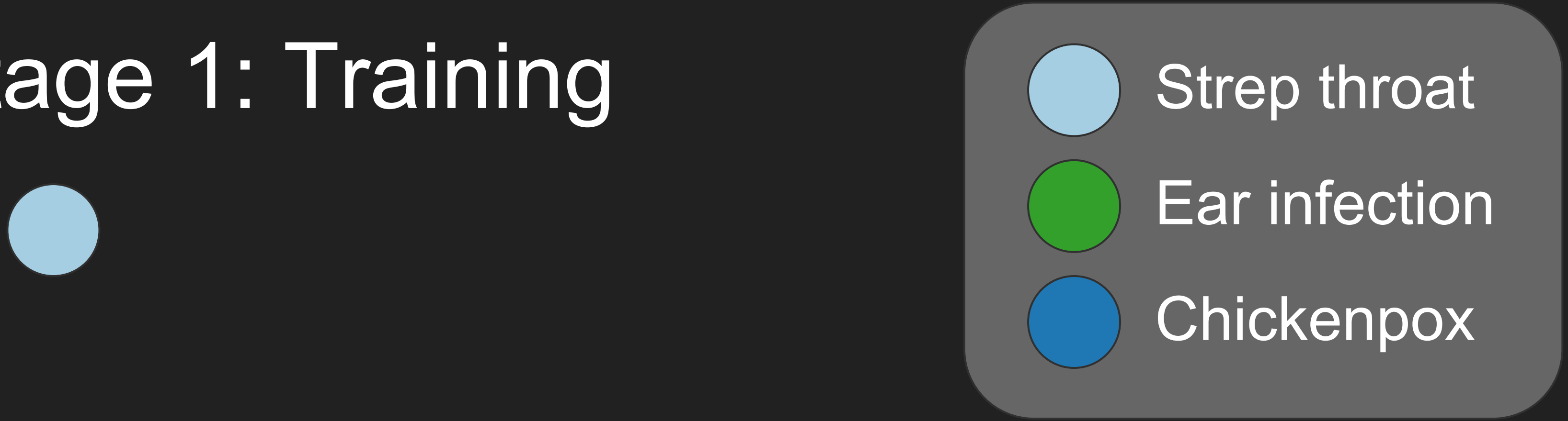
A. html_stack_item()
B. html_stack_dup()
C. html_a()
D. parse_html()

Goal: Recognize this as the *Ear Infection* Wikipedia page.

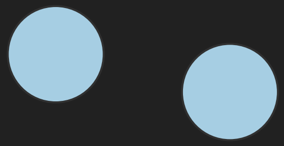
Attack Stages:

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

Stage 1: Training

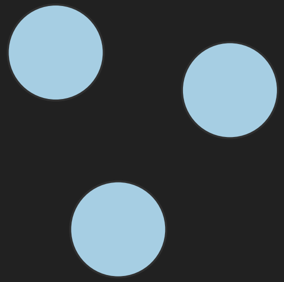


Stage 1: Training



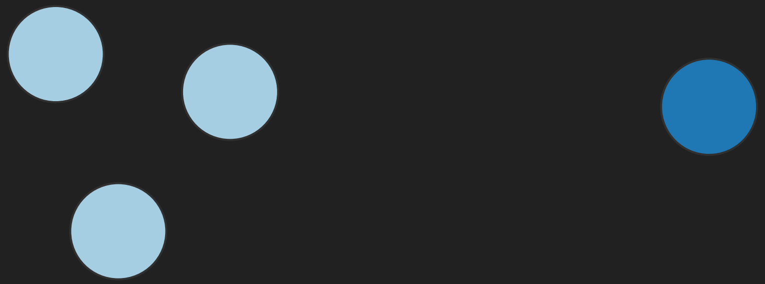
- ● Strep throat
- ● Ear infection
- ● Chickenpox

Stage 1: Training

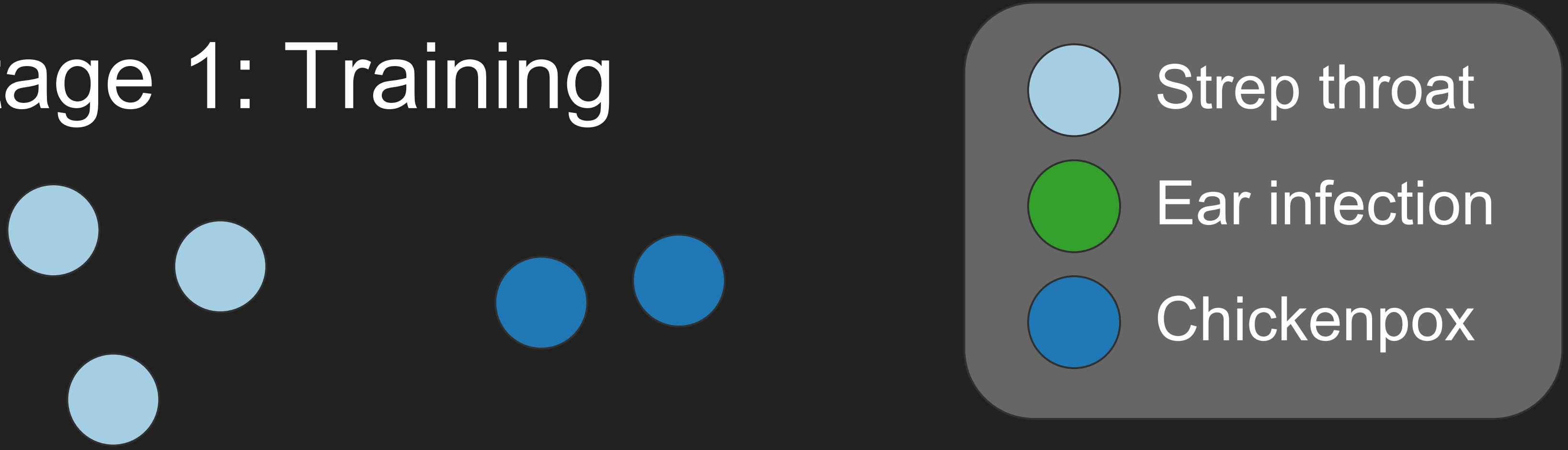


- ● Strep throat
- ● Ear infection
- ● Chickenpox

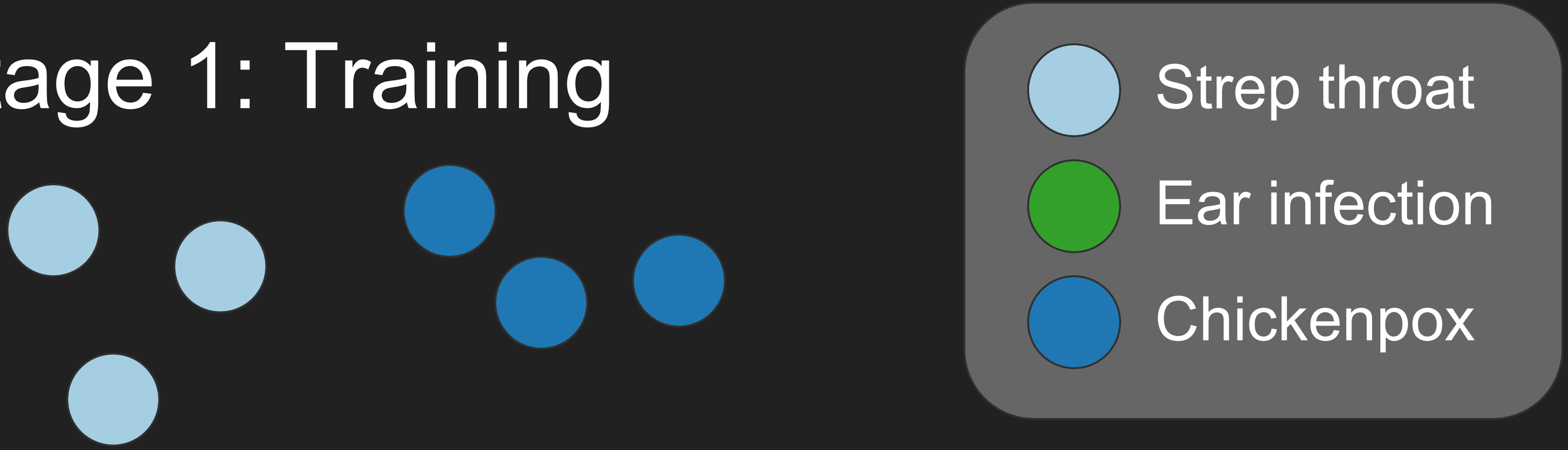
Stage 1: Training



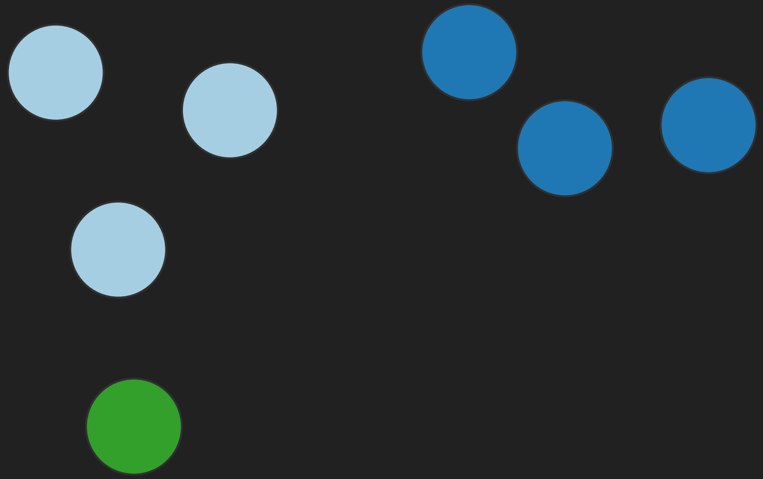
Stage 1: Training



Stage 1: Training



Stage 1: Training

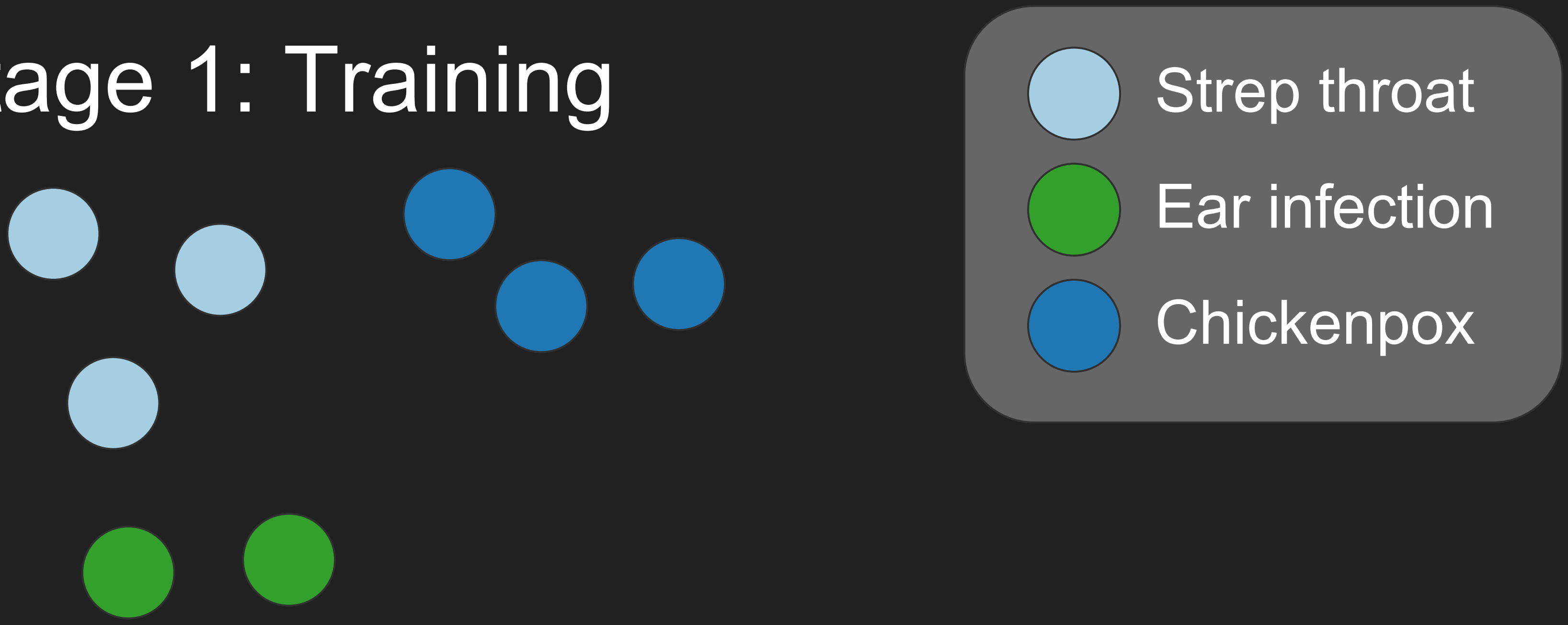


● Strep throat

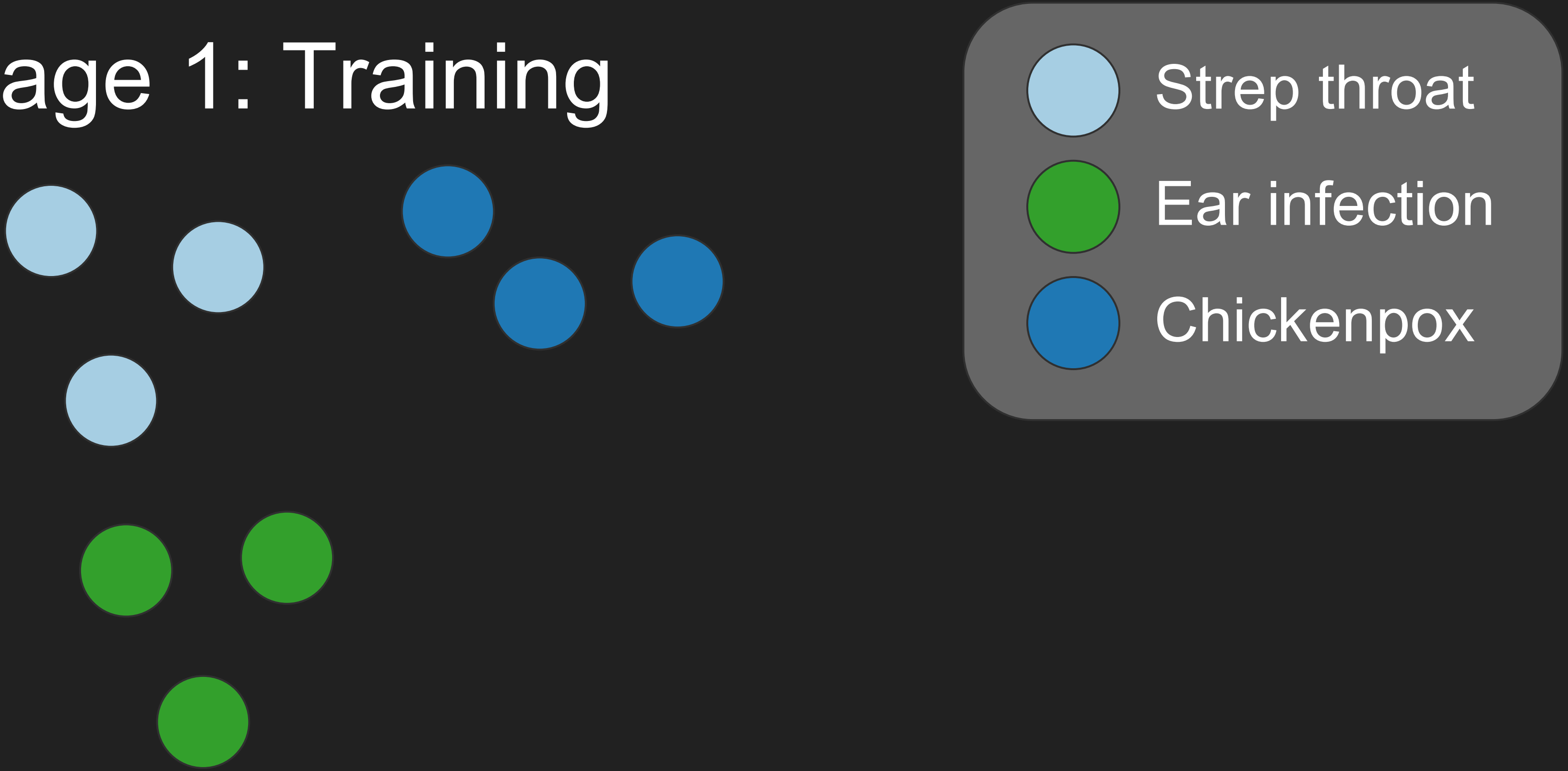
● Ear infection

● Chickenpox

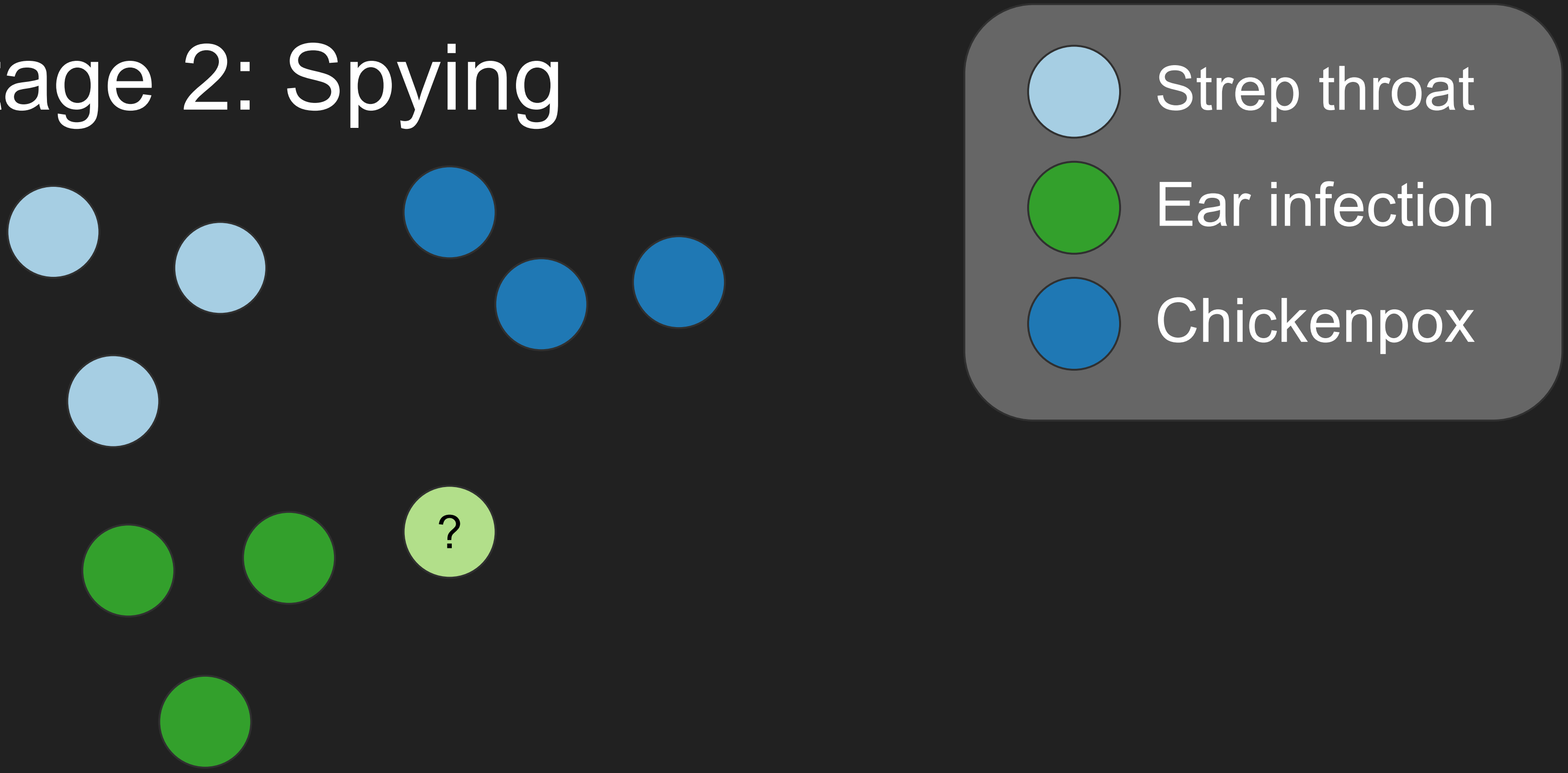
Stage 1: Training



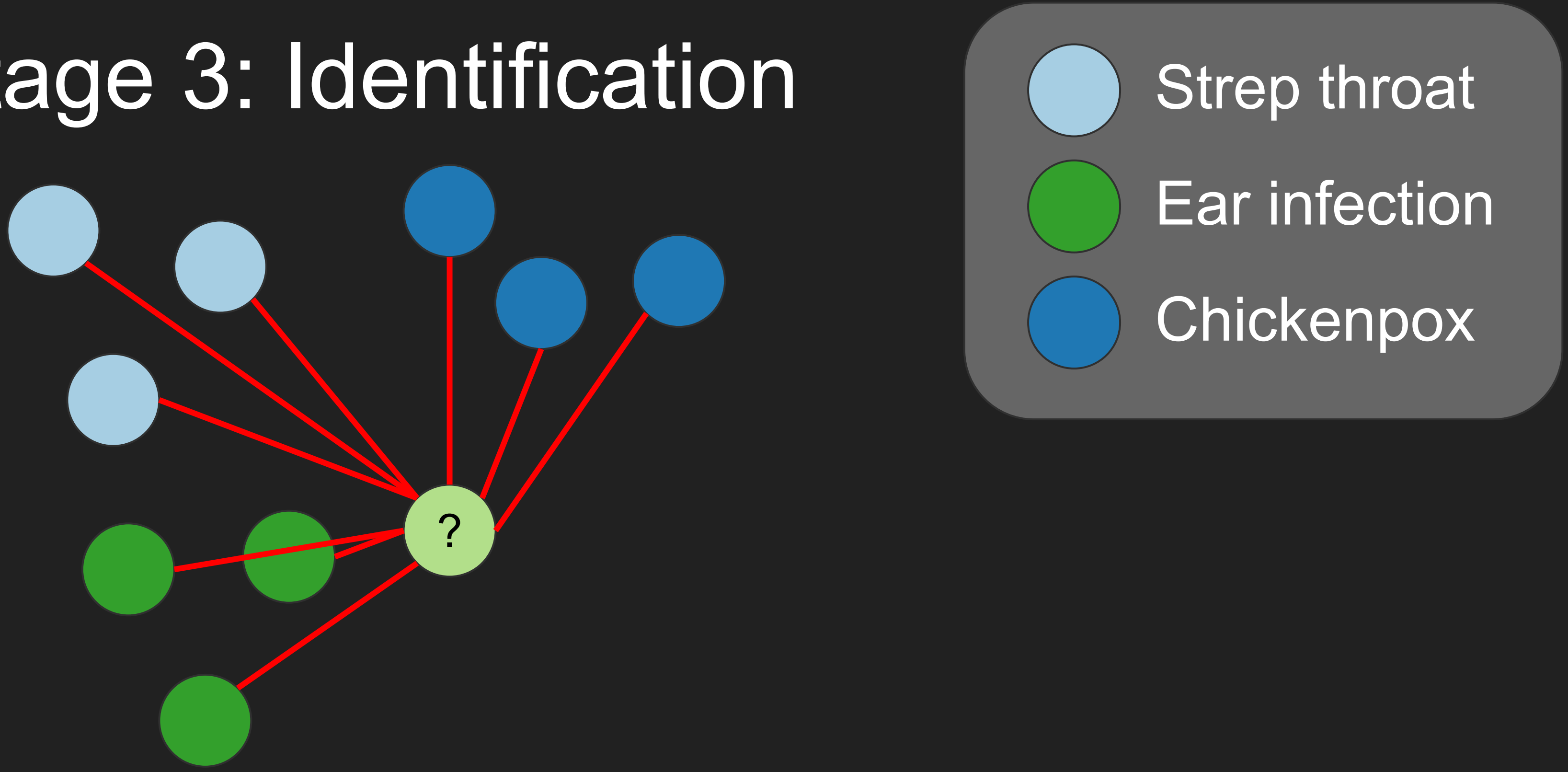
Stage 1: Training



Stage 2: Spying



Stage 3: Identification

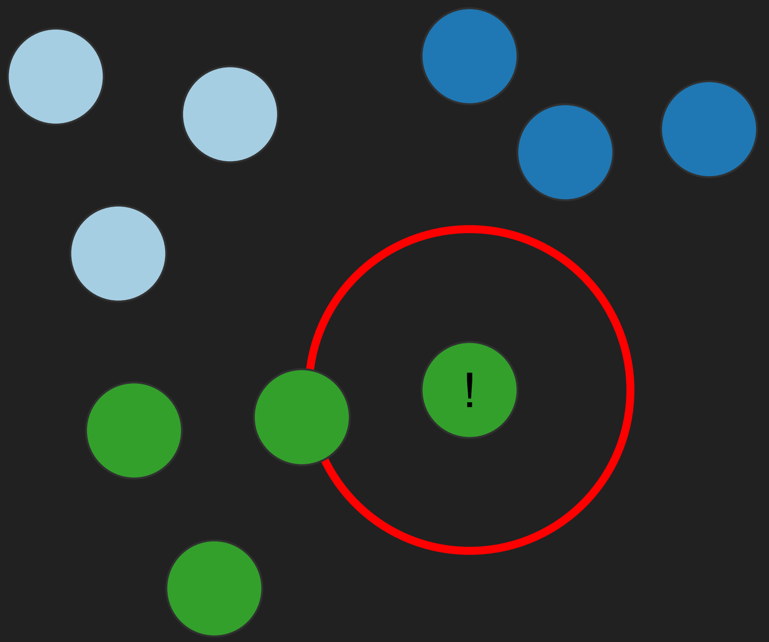


Strep throat

Ear infection

Chickenpox

Stage 3: Identification



- ● Strep throat
- ● Ear infection
- ● Chickenpox

Output: “Ear infection”

>90% Success

(100 pages, 10 samples)

It’s demo time.

https://defuse.ca/BH2016

Q&A

https://defuse.ca/BH2016