Robust Cache Covert Channels in the Cloud

Michael Schwarz
April 4th, 2017
Today we have seen that we can build *covert channels* using DRAM.

- Today we have seen that we can build covert channels using DRAM.
A fast covert channel

• Today we have seen that we can build covert channels using DRAM
• The cache is faster, let’s exploit this fact
A fast covert channel

• Today we have seen that we can build *covert channels* using DRAM
• The *cache is faster*, let’s exploit this fact
• We want to build a covert channel which...
A fast covert channel

- Today we have seen that we can build **covert channels** using DRAM
- The **cache is faster**, let’s exploit this fact
- We want to build a covert channel which...
  - works across virtual machines
A fast covert channel

• Today we have seen that we can build **covert channels** using DRAM
• The **cache is faster**, let’s exploit this fact
• We want to build a covert channel which...
  • works across virtual machines
  • runs on the Amazon cloud
A fast covert channel

• Today we have seen that we can build *covert channels* using DRAM
• The *cache is faster*, let’s exploit this fact
• We want to build a covert channel which...
  • works across virtual machines
  • runs on the Amazon cloud
  • is fast (*i.e.*, multiple kB/s)
A fast covert channel

• Today we have seen that we can build **covert channels** using DRAM
• The **cache is faster**, let’s exploit this fact
• We want to build a covert channel which...
  • works across virtual machines
  • runs on the Amazon cloud
  • is fast (i.e., multiple kB/s)
  • is free of transmission errors
Today we have seen that we can build covert channels using DRAM.
The cache is faster, let’s exploit this fact.
We want to build a covert channel which...
  • works across virtual machines
  • runs on the Amazon cloud
  • is fast (i.e., multiple kB/s)
  • is free of transmission errors
  • is robust against system noise
Challenges

Cross-VM side channel
Challenges

- Cross-VM side channel
- Communication channel
Challenges

- Cross-VM side channel
- Communication channel
- Synchronization
Challenges

- Cross-VM side channel
- Communication channel
- Synchronization
- Error correction
Challenges

Cross-VM side channel

Communication channel

Synchronization

Error correction

Stream
We can use Prime+Probe for the side channel

- Prime+Probe is a last-level cache side channel
Cross-VM side channel

We can use **Prime+Probe** for the side channel

- Prime+Probe is a *last-level cache* side channel
- Exploits the *timing differences* of cached and uncached data
We can use **Prime+Probe** for the side channel

- Prime+Probe is a last-level cache side channel
- Exploits the timing differences of cached and uncached data
- The last-level cache is shared among all VMs
Cross-VM side channel

We can use **Prime+Probe** for the side channel

- Prime+Probe is a **last-level cache** side channel
- Exploits the **timing differences** of cached and uncached data
- The last-level cache is shared among all VMs
- No further requirements
We extend Amazon’s product portfolio
We extend Amazon’s product portfolio
We extend Amazon’s product portfolio
Building an SSH connection

TCP-over-Cache (RFC?)

TCP Client (e.g. ssh)

TCP ↔ File

File System

Covert Channel

Hypervisor

Prime+Probe

Last Level Cache (LLC)
Demo

https://www.youtube.com/watch?v=d_TmocWyEDY