ABSYNTHE: AUTOMATIC BLACKBOX SIDE-CHANNEL SYNTHESIS ON BLACK BOXES
AS TO THE OPINIONS AND Positions expressed in this presentation, they are those of the speakers and do not represent the views of any current or previous employer, including Intel Corporation or its affiliates.
SIDE CHANNELS

Observation: Shared resources often give rise to side channels

• L1, L2, LLC caches
• TLB
• Branch predictor state
• Store-to-Load forwarding
• Many others
SIDE CHANNELS

Most side channels are eviction based

- Original: cache attack and many variants
- Cache directory attack
- TLBleed (TLB)
- Many branch prediction based attacks (PHT, BTB)

Each can have

- Complex addressing function
- Complex structure (sets, ways, levels, inclusivity)
LESS REVERSE ENGINEERING

• Lifetimes have been spent in reverse engineering uarch structures
• Let’s just target stateless resources? No eviction.
• Examples: execution unit contention, execution port contention
• Let’s do a full multi-arch NxN covert shotgun & upgrade to side channel
ABSYNTHE: THE VISION

- Given: target code, architecture
- Automatically find secret-dependent code paths in target code
- Mix side channel primitives to improve signal strength
- Include inter-VM signal
- Upgrade synchronized secret classification to unsynchronised key recovery
ABSYNTHE: THE VISION

Covert Shotgun
Anders Fogh / September 27, 2016 / meta

Automatically finding SMT covert channels
ABSYNTHE: THE VISION

Due to the $N^2$ nature of "covert shotgun" I ran a small list of 12 instructions where some were found particularly likely to be boring. The list of instructions:

<table>
<thead>
<tr>
<th>Instruction</th>
<th>My reasoning</th>
</tr>
</thead>
<tbody>
<tr>
<td>RdSeed rax</td>
<td>Pretty slow, thus like a &quot;0&quot; signal instruction</td>
</tr>
<tr>
<td>Pause</td>
<td>The most likely &quot;0&quot; signal instruction</td>
</tr>
<tr>
<td>Nop</td>
<td>Does it get anymore benign?</td>
</tr>
<tr>
<td>Xor eax,eax</td>
<td>I used it in my last blog</td>
</tr>
<tr>
<td>Lea rax,[4<em>rax+edi+40960]:lea rdx,[8</em>eax+rdi+409623]</td>
<td>I suspected I might get into trouble with the Address generation unit, by using SIB bytes, two instructions and a constant bigger than 2048.</td>
</tr>
<tr>
<td>RdRand rax</td>
<td>Sounded interesting</td>
</tr>
<tr>
<td>Add rax,1</td>
<td></td>
</tr>
<tr>
<td>Bts rax,1</td>
<td></td>
</tr>
<tr>
<td>Bt rax,1</td>
<td>Wanted to check too near identical instructions against each other</td>
</tr>
</tbody>
</table>
OUR COVERT SHOTGUN: PRIMITIVES ON ARM VULCAN
ALL X86 INSTRUCTIONS?

LATENCY, THROUGHPUT, AND PORT USAGE INFORMATION
FOR INSTRUCTIONS ON RECENT X86 MICROARCHITECTURES

This website provides more than 400,000 pages with detailed latency, throughput, and port usage data for most instructions on many recent x86 microarchitectures. While such data is important for understanding, predicting, and optimizing the performance of software running on these microarchitectures, most of it is not documented in the official processor manuals.
ALL ON SKYLAKE
AND BROADWELL

Intel Skylake

P0, P1, P5, P0+1

writer, grouped by port

Intel Broadwell Xeon

P0, P1, P5, P0+1

writer, grouped by port
TRY ALL INSTRUCTIONS AS SIDE CHANNELS ON VULNERABLE LIBGCRYPT TARGETS
AUTOMATICALLY TUNE

- We can differentiate secrets using these side channels
- Can we do better if we mix them?
AUTOMATICALLY TUNE

- We can differentiate secrets using these side channels
- Can we do better if we mix them?
NOISE RESISTANCE
### RESULTS: FULL KEY RECOVERY, PLAIN AND GPG

<table>
<thead>
<tr>
<th>Platform</th>
<th>Target</th>
<th>Instr</th>
<th>Trials</th>
<th>Success</th>
<th>Med. BF (2^N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skylake</td>
<td>ED25519</td>
<td>DE1</td>
<td>7</td>
<td>1.00</td>
<td>7.9</td>
</tr>
<tr>
<td>Skylake</td>
<td>ED25519</td>
<td>Instr2</td>
<td>7</td>
<td>1.00</td>
<td>15.8</td>
</tr>
<tr>
<td>Skylake</td>
<td>ED25519</td>
<td>Instr1</td>
<td>7</td>
<td>1.00</td>
<td>15.8</td>
</tr>
<tr>
<td>Skylake</td>
<td>GPG/ED25519</td>
<td>DE1</td>
<td>7</td>
<td>0.71</td>
<td>29.7</td>
</tr>
<tr>
<td>Skylake</td>
<td>GPG/ED25519</td>
<td>Instr2</td>
<td>7</td>
<td>0.86</td>
<td>22.5</td>
</tr>
<tr>
<td>Skylake</td>
<td>GPG/ED25519</td>
<td>Instr1</td>
<td>7</td>
<td>1.00</td>
<td>17.4</td>
</tr>
</tbody>
</table>
CONCLUSION

• ABSynthe is a useful side channel analysis kit
CONCLUSION

- ABSynthe is a useful side channel analysis kit
- New, multi-arch side channel results
CONCLUSION

• ABSynthe is a useful side channel analysis kit

• New, multi-arch side channel results

• Thank you for listening