DMA Attacks in the Presence of an IOMMU

Gil Kupfer, Nadav Amit and Dan Tsafrir
Technion - Israel Institute of Technology / Computer Science Department

Classic DMA Attacks

- Direct Memory Access
  - I/O devices directly access memory
  - DMA can access any part of the memory
  - Attackers can easily take over victim

DMA Attacks

- I/O Memory Management Unit
  - Translates virtual addresses to physical addresses using page tables
  - Caches translations in TLB

Were mitigated by IOMMU

- Memory Management Unit
  - Translates virtual addresses to physical addresses using page tables
  - Caches translations in TLB

IOMMU is for devices what MMU is for processes

Inherits its design from regular MMU

Vulnerabilities We Found

- Sub page granularity
  - Buffers are typically smaller than a page
- Deferred protection
  - Unmapped pages are still accessible

Attacks We Implemented

<table>
<thead>
<tr>
<th>Attack</th>
<th>FireWire /Linux</th>
<th>FireWire /FreeBSD</th>
<th>NICs /Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>external</td>
<td>external</td>
<td>Internal</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>sub page</td>
<td>sub page</td>
<td>sub page + deferred</td>
</tr>
<tr>
<td>Owner</td>
<td>driver</td>
<td>mem allocator</td>
<td>network stack</td>
</tr>
</tbody>
</table>

Fixing requires lots of code changes...