NSA Playset:
JTAG Implants
Introductory Rites
Today’s Clergy

- Electrical Engineering education with focus on CS and Infosec
- 10 years of fun with hardware
  - silicon debug
  - security research
  - pen testing of CPUs
  - security training
- Hardware Security Training:
  - Secure RTL design
  - Low-cost physical attacks
  - “Applied Physical Attacks on x86 Systems”

Joe FitzPatrick
@securelyfitz
joefitz@securinghardware.com
Today’s Clergy

- Degrees in Electrical and Computer Engineering
- 10+ years designing, implementing, and testing SoC silicon debug features
- Hardware and firmware pentesting

Matt King
@syncsrc
jtag@syncsrc.org
Welcome to the home of the NSA Playset.

In the coming months and beyond, we will release a series of dead simple, easy to use tools to enable the next generation of security researchers. We, the security community have learned a lot in the past couple decades, yet the general public is still ill equipped to deal with real threats that face them every day, and ill informed as to what is possible.

Inspired by the NSA ANT catalog, we hope the NSA Playset will make cutting edge security tools more accessible, easier to understand, and harder to forget. Now you can play along with the NSA!

More toys for sale!

Sunday at Hacker Warehouse in the vendor area!
The Penitence of Godsurge & Fluxbabbit

(TS//SI//REL) GODSURGE runs on the FLUXBABBITT hardware implant and provides software application persistence on Dell PowerEdge servers by exploiting the JTAG debugging interface of the server’s processors.

(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 1950

(TS//SI//REL) This technique supports Dell PowerEdge 1950 and 2950 servers that use the Xeon 5100 and 5300 processor families.

(TS//SI//REL) Through interdiction, the JTAG scan chain must be reconnected on
Liturgy of the DWORD: JTAG
A reading from IEEE 1149
OSI Model

- **data unit**
  - **layers**
    - **data**
    - **presentation**
      - Data Representation & Encryption
    - **session**
      - Interhost Communication
    - **transport**
      - End-to-End Connections and Reliability
    - **network**
      - Path Determination & Logical Addressing (IP)
    - **data link**
      - Physical Addressing (MAC & LLC)
    - **physical**
      - Media, Signal and Binary Transmission

Remember This?
OSI Model:
- Data
- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Media Layers:
- Packets
- Frames
- Bits

Host Layers:
- Data
- Presentation
- Session

JTAG Model:
- TDI, TDO, TMS, TCK, TRST
Physical Layer: Test Access Port
TDO unto others
As others TDI unto you
JTAG Model

TAP FSM

TDI, TDO, TMS, TCK, TRST
Data Link: TAP FSM
Data Link: TAP FSM
OSI Model

- data
- application
  Network Process to Application
- presentation
  Data Representation & Encryption
- session
  Interhost Communication
- transport
  End-to-End Connections and Reliability
- segments
- network
  Path Determination & Logical Addressing (IP)
- packets
- data link
  Physical Addressing (MAC & LLC)
- frames
- physical
  Media, Signal and Binary Transmission
- bits

JTAG Model

- IR/DR access
- TAP FSM
- TDI, TDO, TMS, TCK, TRST
Network Layer: IRs & DRs
Target-specific configuration

IR/DR access

TAP FSM

TDI, TDO, TMS, TCK, TRST
## Transport Layer: Target-Specific

<table>
<thead>
<tr>
<th>Code</th>
<th>Instruction</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>All 0’s</td>
<td>(Free for other use)</td>
<td>Free for other use, such as JTAG boundary scan</td>
</tr>
<tr>
<td>0x01</td>
<td>IDCODE</td>
<td>Selects Device Identification (ID) register</td>
</tr>
<tr>
<td>0x02</td>
<td>(Free for other use)</td>
<td>Free for other use, such as JTAG boundary scan</td>
</tr>
<tr>
<td>0x03</td>
<td>IMPCODE</td>
<td>Selects Implementation register</td>
</tr>
<tr>
<td>0x04 - 0x07</td>
<td>(Free for other use)</td>
<td>Free for other use, such as JTAG boundary scan</td>
</tr>
<tr>
<td>0x08</td>
<td>ADDRESS</td>
<td>Selects Address register</td>
</tr>
<tr>
<td>0x09</td>
<td>DATA</td>
<td>Selects Data register</td>
</tr>
<tr>
<td>0x0A</td>
<td>CONTROL</td>
<td>Selects EJTAG Control register</td>
</tr>
<tr>
<td>0x0B</td>
<td>ALL</td>
<td>Selects the Address, Data and EJTAG Control registers</td>
</tr>
<tr>
<td>0x0C</td>
<td>EJTAGBOOT</td>
<td>Makes the processor take a debug exception after reset</td>
</tr>
<tr>
<td>0x0D</td>
<td>NORMALBOOT</td>
<td>Makes the processor execute the reset handler after reset</td>
</tr>
</tbody>
</table>
That’s just MIPS.
That’s just MIPS.

X86 is different
ARM is different
Each SOC is different
That’s just MIPS.

X86 is different
ARM is different
Each SOC is different

Romans 12:2 (NIV)
Do not conform to the pattern of this world
That’s just MIPS.

X86 is different
ARM is different
Each SOC is different

Romans 12:2 (NIV) NIH
Do not conform to the pattern of this world
--- (no one uses this crap)

--- N/A - sessionless...

Target-specific configuration

IR/DR access

TAP FSM

TDI, TDO, TMS, TCK, TRST
A Reading from The second email from Joe to people with JTAG questions
JTAG Model

Boundary Scan, Run Control, Memory Access

---

---

Target-specific configuration

IR/DR access

TAP FSM

TDI, TDO, TMS, TCK, TRST
Boundary Scan
image from intelletech.com, they make stuff to read flash like this
Run Control
Run Stop Control
The Debugger’s Gospel
1149.1 Section 8.3: Private Instructions

c) If private instructions are utilized in a component, the vendor shall clearly identify any instruction binary codes that, if selected, would cause hazardous operation of the component.
Liturgy of the PCB
SAVIORBURST Payload

Replay of debug performed in OpenOCD
- Target (potentially kernel) specific

Commands are converted into a standard format (SVF/XSVF)
SOLDERPEEK Implant
Transubstantiation

https://github.com/NSAPlayset/SAVIORBURST
Transubstantiation

https://github.com/NSAPlayset/SAVIOORBURST
Communion
Concluding Rites
Solemn Invocation

Not all devices can rely on physical security

Protecting user data requires user control over hardware debug capabilities
Dismissal

I don't want to talk to you no more, you empty-headed animal food trough wiper! I fart in your general direction! Your mother was a hamster and your father smelt of elderberries!