Nation-State Supply Chain Attacks for Dummies and You
-or-
Chipping Cisco Firewalls

By: Monta Elkins
Monta Elkins
- Pronounced “Montay”
- Monta.sans@geekslunch.com
- @MontaElkins Twitter
- linkedin.com/in/montaelkins

Sponsor: TDI Technologies
- https://www.tditechnologies.com/
The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

Chipping Implications

- Impossible to detect via traditional software methods until after the attack is executed
- Could be in any piece of equipment
- Will survive re-imaging the device
- Introduced in the supply chain
Was it True?

- Still looking for definitive proof
Was it True?

Doesn’t matter; Let’s make it true
How to Attack?

- Various ways may be possible
- Serial port attack seems the cheapest / easiest and most generic for Industrial Control System attacks
Target Selection

- Selecting a device
- Something in the Industrial Control System space
- But with broad interest
- How about a firewall
  - Cisco is popular
How Do Serial Ports Work?

- Simplest form
  - Transmit line (TX)
  - Receive line (RX)
  - Ground (Gnd)
Pulseview / Sigrok Hardware

Pulseview is foss [https://sigrok.org/wiki/PulseView]
• Universal Asynchronous Receiver/Transmitter

• Handles the details
  – Signaling
  – Power requirements

Signal levels of ±5 V, ±10 V, ±12 V, and ±15 V are all commonly seen depending on the voltages available to the line driver circuit.

Valid signals are either in the range of +3 to +15 volts or the range −3 to −15 volts with respect to the "Common Ground" (GND) pin.

The range between −3 to +3 volts is not a valid RS-232 level

The Trick

+ -15V will fry a microcontroller

Atmel Zero Cross Application note for 110 Vac

- Don’t want additional UART chip
- (Ab)use the protection Diodes instead

Protection Diodes are rated <1mA
@15 volts that means a 15K ohm input resistor
Hmm 5.1K maybe close enough :)

Test Equipment Evolution 1

- Arduino Mega
- Cisco Serial Cable
Attack Hardware Selection

• ATTINY10
  – Not just tiny, miniscule

• ATTINY85
  – EEPROM for timing and other storage
  – Easier Programming
    • Existing software
    • Existing board
DigiSpark

https://www.amazon.com/DAOKI-Digispark-Kickstarter-ATTINY85-Development/dp/B01MDUHSWO

https://www.amazon.com/s?k=digispark&ref=nb_sb_noss_2

B01MDUHSWO

1-48 of 740 results for "digispark"

DAOKI 5 PCS Digispark Kickstarter ATTINY85 Micro USB Development Board For Arduino

$10.98

FREE Delivery for Prime members
Only 19 left in stock - order soon.

Avg. Customer Review
• DigiSpark board for testing ATTINY85
After Programming the ATTINY85

- Hot Air Rework Tool $150

- Magnifying Microscope $40

- Tweezers $2

- Bluetack Poster Putty $3
  https://www.amazon.com/Loctite-Fun-Tak-Mounting-2-Ounce-1865809/dp/B018A3AG0W
• Originally 4 wires
  - +5V, GND, TX, RX
• Place anywhere with 3 Bodge wires
• Bodge wires are ugly

https://techobsessed.net/2015/09/new-to-me-edc-521-dc-voltagecurrent-source/img_8627/

https://hackaday.io/project/160754-puredata-portable-synth/
3 Wire Solution

- Changing pins and careful positioning allowed all signals to be connected without wire.
What is its value?
• Used 2 surface mount resistors
• Success!

• And failure :(
The 5V Puzzle

MICREL Dual channel power distribution switch

Pin Configuration

Pin Description

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Pin Name</th>
<th>Pin Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ENA</td>
<td>Switch A Enable (Input): Logic-compatible, enable input. Active high (-1) or active low (-2).</td>
</tr>
<tr>
<td>2</td>
<td>FLGA</td>
<td>Fault Flag A (Output): Active-low, open-drain output. Indicates overcurrent or thermal shutdown conditions. Overcurrent conditions must last longer than t0 in order to assert FLGA.</td>
</tr>
<tr>
<td>3</td>
<td>FLGB</td>
<td>Fault Flag B (Output): Active-low, open-drain output. Low indicates overcurrent or thermal shutdown conditions. Overcurrent conditions must last longer than t0 in order to assert FLGB.</td>
</tr>
<tr>
<td>4</td>
<td>ENB</td>
<td>Switch B Enable (Input): Logic-compatible enable input. Active-high (-1) or active-low (-2).</td>
</tr>
<tr>
<td>5</td>
<td>OUTB</td>
<td>Switch B (Output)</td>
</tr>
<tr>
<td>6</td>
<td>GND</td>
<td>Ground</td>
</tr>
<tr>
<td>7</td>
<td>IN</td>
<td>Input: Switch and logic supply input.</td>
</tr>
<tr>
<td>8</td>
<td>OUTA</td>
<td>Switch A (Output)</td>
</tr>
</tbody>
</table>
Solder Bridging as an Attack

Two “accidental” solder bridges solve my 5V problem without ugly bodge wires :)

TDI Technologies, LLC
https://www.tditechnologies.com/
Can you Find it?
Hiding the Payload

- On the motherboard
- On the bottom of the motherboard
  - Means removing 14 screws to see it
- Other hiding, in the can
- Hiding Jumpers as solder bridges
Warranty Void if Removed Stickers
• Normal Serial Connection
• Review After Admin Setup at Serial Console
CISCO Attack

- Escape Characters, confreg 0x41
- Boot, Enable
- copy startup-config running-config
- Enable SSH, Add account, Add routing
- no config-register
- ping attack address as notification

• Without Serial Adapter Connection
  – Using Sigrok to read serial signals
  – High Input Impedance 8 Channel Analyzer
Chipping Implications

- Impossible to detect via traditional software methods until after the attack is executed
- Will survive re-imaging the device
- Attack is invisible
- Consider the debug cycle
Enhancements

- Trigger based on reset line
- “Expect” script style delivery
- Store password changes
  - Allows better timed accesses
  - May allow exfil over network
- RF exfil

Thanks to these colleagues for their input
- Derek Kolakowski
- Roger Rademacher
- Steven Wirt
Defenses

- Carefully review mainboard
- Configuration baselining
- Firmware hash and baselining
- RF baselining
- “no service password-recovery”
  - partial
What I Learned

• It’s pretty easy to build
• A bit hard to insert in supply chain
  – Ebay
  – Social Engineering
  – Component Suppliers
  – Nation State Level Resources
• Typically for targeted attacks
• Probably not your top priority
  – Why?
Factory Original Schmoo
• Monta Elkins
  - Pronounced “Montay”
  - Monta.sans@geekslunch.com
  - @MontaElkins Twitter
  - linkedin.com/in/montaelkins

• Sponsor: TDI Technologies
  - https://www.tditechnologies.com/