The Current State of Hardware Hacking
(even a 2-year-old can do it...)

Joe Grand, Grand Idea Studio
joe@grandideastudio.com
We Need to Open Our Eyes...

- Hardware hacks becoming more common
- Not many use new or novel techniques
- Most "security" has been a mere roadblock
We Are Part of the Problem

- Many attacks are so easy that we (engineers & vendors) should be blamed
- We are trained to think like engineers
- We are not trained to think like hackers
- We are constrained by budget and time-to-market
- Security is an afterthought (if at all)
- Our response to hardware attacks is antiquated
  - Knee-jerk reactions
  - Denial of any issue (and refusal to fix it)
Hardware Hacking Areas

- **Information Gathering**
  - Obtaining data about the target by any means necessary

- **Hardware Teardown**
  - Product disassembly, component/subsystem identification, modification

- **Firmware Reverse Engineering**
  - Extract/modify/reprogram code or data
  - OS exploitation/device jailbreaking

- **External Interface Analysis**
  - Communications monitoring, protocol decoding/emulation

- **Silicon Die Analysis**
  - Chip-level modification/data extraction
Common Attack Surfaces

• Memory & Firmware
• Exposed Buses & Interfaces
• Passwords & Cryptography
Memory & Firmware
Memory & Firmware

1993: Oki 900 Cellphone Cloning (8051)

www.hackcanada.com/blackcrawl/cell/oki/oki900.html
# Memory & Firmware

## 1998: NIC MAC Address Cloning (Serial EEPROM)

www.grandideastudio.com/portfolio/mac-address-cloning/

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
<th>EEPROM</th>
<th>MAC Address</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Semiconductor</td>
<td>NSC ?</td>
<td>93LC06</td>
<td>00:00:17:03:C0:E5</td>
<td>0008 0317 E5C0 0000 0500 010D 01DA 5757 4242 0000 0000 0000 0000 0020 0020</td>
</tr>
<tr>
<td>Ansel Communications</td>
<td>N2000 Plus 3</td>
<td>93C46</td>
<td>00:40:90:80:07:7E</td>
<td>4000 8090 7E07 FFFF FFFF FFFF 5757 4242 FFFF FFFF FFFF FFFF 0100 FF20</td>
</tr>
<tr>
<td>Microdyne</td>
<td>NE2000 Plus 3</td>
<td>93C06</td>
<td>00:80:29:E7:C2:9C</td>
<td>N/A</td>
</tr>
<tr>
<td>Linksys</td>
<td>Ether16</td>
<td>93C46</td>
<td>00:40:05:44:17:A7</td>
<td>4000 4405 A717 0108 020A 5464 00D8 0000 0000 0000 0000 0000 0000 0000</td>
</tr>
<tr>
<td>Genitus</td>
<td>GE2000 II</td>
<td>93C46</td>
<td>00:40:33:2A:82:82</td>
<td>4000 2A33 8283 5805 0000 0000 0000 5757 4242 0000 0000 0000 0000 2100 0020</td>
</tr>
<tr>
<td>Winbond</td>
<td>HT-2003CT</td>
<td>93C46</td>
<td>48:54:33:01:48:24</td>
<td>5448 0133 2448 0000 5448 0133 2448 5757 4242 0000 0000 0000 0000 4040 0020</td>
</tr>
</tbody>
</table>
Memory & Firmware

2000: Declawing the CueCat (Serial EEPROM)

www.sujal.net/tech/declaw/
Memory & Firmware

2006: IBM ThinkPad BIOS Password (Serial EEPROM)

http://sodoityourself.com/hacking-ibm-thinkpad-bios-password/
Memory & Firmware

2006: The Netherlands Electronic Voting Machines (68K)

www.wijvertrouwenstemcomputersniet.nl
Memory & Firmware

2010: India Electronic Voting Machines (Serial EEPROM)

www.indiaevm.org
Memory & Firmware

2011: HP LaserJet Printer (VxWorks)

http://ids.cs.columbia.edu/sites/default/files/CuiPrintMeIfYouDare.pdf
Exposed Buses & Interfaces
Exposed Buses & Interfaces

1997: BlackBerry RIM 950/957 (RF)

www.grandideastudio.com/portfolio/decoding-mobitex/

Radio Oriented Synchronous Information (ROSI) Header

- Mobitex Access Number (MAN): 16589672
- Frame ID: 129
- Sequence Number: 184
- Data Blocks: 8

Mobitex Packet (MPAK) Header

- Sender MAN: 16589672
- Addressee MAN: 100031
- Flags: None
- Traffic State: N/A
- Packet Type: Data
- Time Stamp: N/A
- Packet ID: 37

Mobitex Packet (MPAK) Body

- Destination MAN: G101101
- Message Type: E-Mail Original (MIME)
- To: kingpin@atstake.com
- From: 16589672
- Subject: Foo
- Body: Sell the farm.
Exposed Buses & Interfaces

2002: Hacking the Xbox (HyperTransport bus)

www.xenatera.com/bunnie/proj/anatak/xboxmod.html
Exposed Buses & Interfaces

2008: MBTA CharlieTicket (Magnetic Stripe)

http://web.mit.edu/zacka/www/mbta.html

<table>
<thead>
<tr>
<th>const</th>
<th>ticket #</th>
<th>ticket type</th>
<th>value (in cents)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0150342</td>
<td>248</td>
<td>A84EBD</td>
<td>132</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>time</th>
<th>const</th>
<th>time</th>
<th>last reader</th>
<th>last station</th>
<th>const (approx)</th>
</tr>
</thead>
<tbody>
<tr>
<td>028</td>
<td>0002</td>
<td>00000000002025D0000</td>
<td>FC90</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>last trans</th>
<th># of uses</th>
<th>const (approx)</th>
<th>checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>(in nickels)</td>
<td>uses</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Exposed Buses & Interfaces

2009: San Francisco Smart Parking Meter (Smartcard)

www.grandideastudio.com/portfolio/smart-parking-meters/
Exposed Buses & Interfaces

2011: Medtronic Implantable Insulin Pump (RF)

Passwords & Cryptography
Passwords & Crypto


www.grandideastudio.com/portfolio/answering-machine-advisory/
Passwords & Crypto

1994: Universal Garage Door Opener

www.grandideastudio.com/portfolio/universal-garage-door-opener/
Passwords & Crypto

2000: Rainbow iKey 1000 Password Decoding

www.grandideastudio.com/portfolio/attacks-on-usb-tokens/

A, Hashed MKEY value, \text{md5}("rainbow") = CD13 B6A6 AF66 FB77
B, Obfuscated MKEY value in EEPROM = D2DD B960 B0D0 F499

\begin{align*}
B_1 &= A_1 \text{ XOR } 0x1F \\
B_2 &= A_2 \text{ XOR } (A_1 + 0x01) \\
B_3 &= A_3 \text{ XOR } 0x0F \\
B_4 &= A_4 \text{ XOR } (A_3 + 0x10) \\
B_5 &= A_5 \text{ XOR } 0x1F \\
B_6 &= A_6 \text{ XOR } (A_5 + 0x07) \\
B_7 &= A_7 \text{ XOR } 0x0F \\
B_8 &= A_8 \text{ XOR } (A_7 + 0xF3)
\end{align*}

Example: \begin{align*}
0xD2 &= 0xCD \text{ XOR } 0x1F \\
0xDD &= 0x13 \text{ XOR } (0xCD + 0x01)
\end{align*} ...
Passwords & Crypto

2005: Mobil SpeedPass (TI Digital Signature Transponder RFID)

http://static.usenix.org/event/sec05/tech/bono/bono.pdf
Passwords & Crypto

2008: Mifare Classic (RFID)

www.cs.virginia.edu/~evans/pubs/usenix08/usenix08.pdf
What Can Be Done?

- **Acceptance**
  - Admit that security needs to get better
  - Acknowledge that someone might be out to get you

- **Education**
  - Learn from history...don't repeat the same mistakes

- **Awareness**
  - Think like a hacker during the design phase

- **Dedication**
  - Security should be another tool in our toolbox
  - All facets of the organization need to put forth the effort to make products better