Supply Chain Integrity Through Hardware Material Analysis

Mackenize Morris @ ZeroAltruism
Cyber Security Lead | Savannah River Nuclear Solutions
About Me

• PhD dropout in chemical engineering focusing on kinetics and catalysis research

• Team USA 2012 Modern Pentathlon

• Lived 18 years on a farm and refuse to live on one again

• Has a corgi named QWERTY
“This is a particularly pernicious threat... because it’s very difficult for the average citizen, company or government entity to understand every component that was put into a piece of equipment or network that they’ve purchased,” - Former Secretary of Homeland Security Kirstjen Nielsen.
What is the problem

320.4 MILLION
Personal Computers

That's 90.6% of all the personal computers produced in 2011.
Supply Chain Woes

• By definition your supply chain is not inhouse
• You can get in writing, but contracts are still trust based
• Outsourcing moves the supply chain overseas and out of country
• Out of sight = out of security
• Massive supply chain logistics is a necessary evil
There are so many problems with the supply chain.
Thinking Outside the Box

• Supply chain attacks intercept a valid product from a trusted vendor

• A company accepts products from a trusted business partner

• Hardware hacks bypass almost all cyber security controls because hardware has the highest level of privilege

• Trust but verify is not going to work moving forward
What do we know about microprocessors?

- They have a predictable atomic architecture
- Silicon-Silicon don’t really form in nature
- They are required on the motherboard
- The number of microcontrollers doesn’t vary
Maybe just look at it?

...with a high powered laser
A Brief Chemistry Lesson

<table>
<thead>
<tr>
<th>Group</th>
<th>Period</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1 H</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2 He</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3 Li</td>
<td>4 Be</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14 Si</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>11 Na</td>
<td>12 Mg</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14 Si</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>19 K</td>
<td>20 Ca</td>
<td>21 Sc</td>
<td>22 Ti</td>
<td>23 V</td>
<td>24 Cr</td>
<td>25 Mn</td>
<td>26 Fe</td>
<td>27 Co</td>
<td>28 Ni</td>
<td>29 Cu</td>
<td>30 Zn</td>
<td>31 Ga</td>
<td>32 Ge</td>
<td>33 As</td>
<td>34 Se</td>
<td>35 Br</td>
<td>36 Kr</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>37 Rb</td>
<td>38 Sr</td>
<td>39 Y</td>
<td>40 Zr</td>
<td>41 Nb</td>
<td>42 Mo</td>
<td>43 Tc</td>
<td>44 Ru</td>
<td>45 Rh</td>
<td>46 Pd</td>
<td>47 Ag</td>
<td>48 Cd</td>
<td>49 In</td>
<td>50 Sn</td>
<td>51 Sb</td>
<td>52 Te</td>
<td>53 I</td>
<td>54 Xe</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>55 Cs</td>
<td>56 Ba</td>
<td>57 La</td>
<td>58 Ce</td>
<td>59 Pr</td>
<td>60 Nd</td>
<td>61 Pm</td>
<td>62 Sm</td>
<td>63 Eu</td>
<td>64 Gd</td>
<td>65 Tb</td>
<td>66 Dy</td>
<td>67 Ho</td>
<td>68 Er</td>
<td>69 Tm</td>
<td>70 Yb</td>
<td>71 Lu</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>87 Fr</td>
<td>88 Ra</td>
<td>89 Ac</td>
<td>90 Th</td>
<td>91 Pa</td>
<td>92 U</td>
<td>93 Np</td>
<td>94 Pu</td>
<td>95 Am</td>
<td>96 Cm</td>
<td>97 Bk</td>
<td>98 Cf</td>
<td>99 Es</td>
<td>100 Fm</td>
<td>101 Md</td>
<td>102 No</td>
<td>103 Lr</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Elements with incomplete electron shells
A Brief Chemistry Lesson

The diagram illustrates the energy transitions in Raman and Hyper-Raman spectroscopy. The upper electronic state is shown at the top, with transitions labeled as follows:

- **A**: Lower to upper state transition
- **B**: Stokes transition, $h(v_o - v_k)$
- **C**: Anti-Stokes transition, $h(2v_o - v_k)$
- **D**: Resonance Raman, $h(v_o + v_k)$
- **E**: Resonance Hyper-Raman, $h(2v_o - v_k)$

The lower electronic state is at the bottom, with transitions labeled as:

- **Raman**: $h(v_o)$
- **Hyper-Raman**: $h(2v_o - v_k)$

The transitions are indicated with arrows, showing the energy differences and the photons involved in each transition.
\[
\frac{m_1 m_2}{m_1 + m_2} \left( \frac{d^2 x_1}{dt^2} + \frac{d^2 x_2}{dt^2} \right) = -K(x_1 + x_2), \quad \mu \frac{d^2 q}{dt^2} = -Kq, \quad \sigma_R \propto \frac{1}{\lambda^4},
\]

\[
q_o E_o \left( \frac{\partial \alpha}{\partial t} \right)_{q=0} \left[ \cos(2\pi \{v_o - v_m\} t) + \cos(2\pi \{v_o + v_m\} t) \right],
\]

\[
P = a_0 E_o \cos(2\pi v_o t) + q_o \cos(2\pi v_m t) E_o \cos(2\pi v_o t) \left( \frac{\partial \alpha}{\partial t} \right)_{q=0},
\]

\[
\alpha = a_o + q \left( \frac{\partial \alpha}{\partial t} \right)_{q=0} + \ldots,
\]

\[
P = \alpha E_o \cos(2\pi v_o t),
\]

\[
q = q_o \cos(2\pi v_m t),
\]

\[
\nu_m = \frac{1}{2\pi} \sqrt{\frac{K}{\mu}}.
\]
X-Rays Material analysis techniques

- X-Ray Ptychography
- X-Ray Photoelectron Spectroscopy
- X-Ray Computed Tomography
- X-Ray Fluorescence
X-Ray Ptychography
X-Ray Ptychography

• Hilariously expensive
• Requires a synchrotron (<100 in the world)
• Gives visibility down to 14 nanometers in 3D space
• Currently in use by AMD to reverse engineer Intel’s chips
• Takes a 24 hours to scan a computer and has 10000x more resolution than needed
• Proves an initial proof of concept
X-Ray Photoelectron Spectroscopy
X-Ray Photoelectron Spectroscopy

*Photo-Emitted Electrons* (< 1.5 kV) escape only from the very top surface (70 - 110Å) of the sample.

*Electron Energy Analyzer* (0-1.5kV) (measures kinetic energy of electrons)

*Electron Detector* (counts the electrons)

*Beam of X-rays* (1.5 kV)

Electron Collection Lens

SiO₂ / Si Sample

Samples are usually solid because XPS requires ultra-high vacuum (<10⁻⁶ torr)

Si (2p) XPS signals from a Silicon Wafer
X-Ray Photoelectron Spectroscopy

• More feasible, high capital cost for detectors and vacuum containers

• Surface phenomenon and will have difficulty seeing under objects

• Provides clear definition of differences between Si and SiO$_2$
X-Ray Computed Tomography
X-Ray Computed Tomography
X-Ray Computed Tomography

• Provides 3-D material analysis by looking at “slices” of an object
• Relatively cheap compared to other solutions, already a common technology that can be readapted
• Microprocessors stand out from other components and can be counted
• Possible to automate for large number of PCBs and machine learning
X-Ray Fluorescence
Gold images and Baselines

- CIS and DISA STIG are example of industry baseline guidance
- Create a baseline for your configuration and measure yourself
- Hardware baselines could be created from validated “good” units
- Programs can compare scans of hardware to golden image files
- Validating your hardware from supply chain interdiction
What can we Learn?

• Does not stop a malicious manufacturer whom is compromised from the beginning, although every part they produce would have to be malicious
• This is an expensive process for a low risk attack
• Put your money toward the best solution
• Validating high risk assets (HVA)
Supply Chain Integrity Through Hardware Material Analysis

Mackenize Morris @ ZeroAltruism
Mackenize.Morris@srs.gov
Cyber Security Lead | Savannah River Nuclear Solutions