ACSAC Case Study

ICT Supply Chain Risk Management

Austin, TX
Thursday, December 9, 2010
13:30-15:00
ICT products are assembled, built, and transported by multiple vendors around the world before they are acquired. The challenges range from poor acquirer practices to lack of transparency into the supply chain. Abundant opportunities exist for malicious actors to tamper with and sabotage products, ultimately compromising system integrity and operations. There are a substantial number of organizations or people who can “touch” an ICT product without being detected, however, there is no standardized methodology or lexicon for managing ICT supply chain risks. Over the last 5 years the awareness of the challenge and US Government and industry response have brought this problem to the forefront of cyber security.
From *The World Is Flat* by Thomas Friedman
Dell Inspiron 600m Notebook Key Components and Suppliers

<table>
<thead>
<tr>
<th>Part</th>
<th>Supplier or Potential Suppliers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel Microprocessor</td>
<td>Intel factory either in the Philippines, Costa Rica, Malaysia, or China</td>
</tr>
<tr>
<td>Memory</td>
<td>Korea (Samsung), Taiwan (Nanya), Germany (Infineon), or Japan (Elpida)</td>
</tr>
<tr>
<td>Graphics Card</td>
<td>Taiwanese-owned factory in China (MSI) or Chinese-owned factory in China (Foxconn)</td>
</tr>
<tr>
<td>Cooling fan</td>
<td>Taiwan (CCI or Auras)</td>
</tr>
<tr>
<td>Motherboard</td>
<td>Korean-owned factory in Shanghai (Samsung), a Taiwanese-owned factory in Shanghai (Quanta) or Taiwan (Compal or Wistron)</td>
</tr>
<tr>
<td>Keyboard</td>
<td>Japanese-owned company in Tianjin, China (Alps), Taiwanese-owned factory in Shenzhen, China (Sunrex) or a Taiwanese-owned factory in Suzhou, China (Darfon)</td>
</tr>
<tr>
<td>LCD</td>
<td>South Korea (Samsung, LG.Philips LCD), Japan (Toshiba or Sharp), or Taiwan (Chi Mei Optoelectronics, Hannstar Display, or AU Optronics)</td>
</tr>
<tr>
<td>Wireless Card</td>
<td>American-owned factory in China (Agere) or Malaysia (Arrow), Taiwanese-owned factory in Taiwan (Askey or Gemtek) or China (USI)</td>
</tr>
<tr>
<td>Modem</td>
<td>Taiwanese-owned company in China (Asustek or Liteon), or a Chinese-run company in China (Foxconn)</td>
</tr>
<tr>
<td>Battery</td>
<td>American-owned factory in Malaysia (Motorola), a Japanese-owned company in Mexico or Malaysia or China (Sanyo) or a South Korean or Taiwanese factory (SDI or Simplo)</td>
</tr>
<tr>
<td>Hard Disk Drive</td>
<td>American-owned factory in Singapore (Seagate), a Japanese-owned company in Thailand (Hitachi or Fujitsu), or a Japanese-owned company in the Philippines (Toshiba)</td>
</tr>
<tr>
<td>CD/DVD</td>
<td>South Korean-owned company with factories in Indonesia and the Philippines (Samsung), a Japanese-owned factory in China or Malaysia (NEC), a Japanese-owned factory in Indonesia, China, or Malaysia (Teac) or a Japanese-owned factory in China (Sony)</td>
</tr>
<tr>
<td>Notebook Carrying Bag</td>
<td>Irish-owned company in China (Tenba), or an American-owned company in China (Targus, Samsonite, or Pacific Design)</td>
</tr>
<tr>
<td>Power Adapter</td>
<td>Thai-owned factory in Thailand (Delta) or a Taiwanese-, Korean-, or American-owned factory in China (Liteon, Samsung, or Mobility)</td>
</tr>
<tr>
<td>Power Cord</td>
<td>British-owned company with factories in China, Malaysia, and India (Volex)</td>
</tr>
<tr>
<td>Removable Memory Stick</td>
<td>Israeli-owned company in Israel (M-System) or an American-owned company with a factory in Malaysia (Smart Modular)</td>
</tr>
</tbody>
</table>
What is the Problem and Gaps We Are Trying to Address?

- Information and Communication Technology (ICT) products are assembled, built, and transported by multiple vendors around the world before they are acquired \textit{without the knowledge of the acquirer}.

- Abundant opportunities exist for malicious actors to tamper with and sabotage products, ultimately compromising system integrity and operations \textit{evidenced by multiple recently publicized incidents} (counterfeit hardware sold to government agencies).

- Organizations acquiring hardware, software, and services are not able to understand and manage the security risks associated with the use of these products and services.

- Challenges range from poor acquirer practices to lack of transparency into the supply chain:
  - Substantial number of organizations or people can “touch” an ICT product without being identified.
  - No standardized methodology or lexicon exists for managing ICT supply chain risks.
  - Poor ICT products and services acquisition practices contribute to acquirers’ lack of understanding what is in their supply chain.
  - Counterfeit hardware and software proliferate.
  - Acquirers do not have a framework to help enforce security and assurance compliance for vendors.
What is this thing we are trying to do?

- ICT Supply Chain assurance, (risk management, security, trust, trustworthiness) intersects with many disciplines

- However, it focuses on a core group of practices that are specific to protecting ICT from security risks caused by the global/international supply chain
How did US Government become aware of the challenge?

- **10+ years of awareness-raising**
  - 2005: GAO, Offshoring of Services: An Overview of the Issues
  - 2007: European Commission, Availability and Robustness of Electronic Communications Infrastructures
  - 2010: Department of Commerce Bureau of Industry and Security, Defense Industrial Base Assessment: Counterfeit Electronics

- **CNCI Initiative 11 “Develop Multi-Pronged Approach for Global Supply Chain Risk Management”**
ICT SCRM Initiatives

Government and Industry

- Multi-faceted initiatives
- Strategy, methodology, and guidance initiatives
- Policy initiatives
- Acquisition initiatives
- Product assurance initiatives
- Anti-counterfeiting and anti-piracy initiatives
- Intelligence and counterintelligence initiatives
- Foreign supplier risk identification initiatives
- Efforts to hold suppliers legally liable for product assurance lapses
- Standards initiatives
- Supply chain collaboration and data flow security initiatives
- Post-acquisition product risk mitigation initiatives
- SCRM education initiatives
- Supply chain risk avoidance through custom ICT production

“Semiconductor counterfeiting is fraud, pure and simple. Given the potential for catastrophic injury and damage from failure of a counterfeit microchip, vigorous enforcement actions are necessary to deter this type of illegal activity.”

— George Scalise
President
Semiconductor Industry Association
The Research Landscape

- ICT SCRM Process
- HW Assurance
- SW Assurance
- Secure Use of OTS SW

Number of Projects:
- SCRM Methodologies
- SCM Data Flow Security
- Secure SW Distribution
- HW Trustworthiness
- HW Tamperproof
- HW IP Protect/Anti-Reverse
- HW Anti-Counterfeit
- HW Trojan Detection
- SW Integrity/IP Protect
- SW Anti-Pracy
- SW Security Analysis
- SW Anti-Malicious Logic
- Secure System Engineering
- HW to Harden SW Environment
- SW to Harden SW Environment

Booz | Allen | Hamilton
Resistance is futile...

- The ICT supply chain is unavoidably global (see Friedman’s *The World is Flat*)
- Pedigree and provenance are often untraceable, even by suppliers themselves
- Basing risk assessment on national origins is impractical for all but the most critical/trusted ICT components/parts (maybe not even then)

**Table 6-2  National Origins of Components Used in Leading Personal Computer**

<table>
<thead>
<tr>
<th></th>
<th>Dell</th>
<th>HP</th>
<th>Lenovo</th>
</tr>
</thead>
<tbody>
<tr>
<td>System design</td>
<td>China, India, Singapore, Taiwan, US</td>
<td>India, US</td>
<td>China, Japan, Taiwan, US</td>
</tr>
<tr>
<td>Motherboard assembly</td>
<td>China</td>
<td>China</td>
<td>China</td>
</tr>
<tr>
<td>System assembly</td>
<td>Brazil, China, Ireland, Malaysia, US</td>
<td>Australia, Canada, China, Czech Republic, India, US</td>
<td>Brazil, China, Czech Republic, Hungary, India, Japan, Mexico</td>
</tr>
<tr>
<td>BIOS design</td>
<td>China, India, US</td>
<td>China, India, US</td>
<td>China, Japan, US</td>
</tr>
</tbody>
</table>

Source: Verizon [360]
Over the last 5 years US industry and government have begun addressing this challenge

- DoD – Don Davidson
- NIST – Marianne Swanson (Nadya Bartol)
- NSA – Larry Wagoner
- SEI CERT – Carol Woody
- SAFECode – Dan Reddy