Behind the Curtain: Insider Insights into PC Industry Security

Raleigh FIRST TC 2016

Bill Jaeger; Director, Security Architecture
bjaeger@lenovo.com
Bio: Bill Jaeger

**Lenovo**

- Director, Security Architecture since February, 2014
- Founding member of Product Security Office
- Work with global product teams and industry partners to enhance product security
- Achieving company – and industry! – security “firsts”

**Highlights**

- 20+ years solving complex security, operational, and technical challenges for commercial and government customers
- Built an award-winning Software-as-a-Service managed security offering
- Author, Inventor
- CISSP®
- CSSLP®
<table>
<thead>
<tr>
<th>Section</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>What’s inside my PC and who makes it?</td>
</tr>
<tr>
<td>Firmware</td>
<td>Who makes my PC’s firmware and why should I update it?</td>
</tr>
<tr>
<td>Software</td>
<td>What are common security issues?</td>
</tr>
<tr>
<td>Tips</td>
<td>What security things do I need to know when buying PCs?</td>
</tr>
<tr>
<td>Bonus!</td>
<td>Factoids, definitions, and questions to ask your PC vendors</td>
</tr>
</tbody>
</table>
Hardware

What’s inside my PC and who makes it?
- PCs are a commodity, w/ common technologies across brands
- Differentiators are design, specs, support, security, etc…

<table>
<thead>
<tr>
<th>What's Inside?</th>
<th>CPU</th>
<th>Memory</th>
<th>TPM</th>
<th>Disk</th>
<th>Video</th>
</tr>
</thead>
<tbody>
<tr>
<td>FACTOID</td>
<td>AMD, Intel</td>
<td>Micron, Samsung</td>
<td>Atmel, Infineon, Intel, NuvoTon, ST</td>
<td>HGST, Intel, Micron, Samsung, SanDisk, Seagate, WD</td>
<td>AMD, Intel, NVIDIA</td>
</tr>
</tbody>
</table>
Who Makes My PC?

Definition: **ODM**
- Original Design Manufacturer designs & manufactures product to spec or w/ own IP, for re-brand and re-sale by another company.

Definition: **OEM**
- Original Equipment Manufacturer is the manufacturer, spec originator, or performs final transformation (assembly).

---

**OEM Specifications**

- Lenovo
- NEC
- Acer
- ASUS
- Dell
- HP
- Microsoft
- Apple

**Suppliers**

- Intel
- Micron
- NVIDIA
- Samsung
- STI

**ODM**

- Compal
- Foxconn
- Inventec
- PEGATRON
- Wistron

**OEM**

- Lenovo
- NEC
- Acer
- ASUS
- Dell
- HP
- Microsoft
- Apple

Copyright © 2016
ODM Manufacturing

- PCs typically made in China, Taiwan, Mexico

- Australia
- Austria
- Brazil
- Canada
- China
- Czech Republic
- Germany
- Hungary
- India
- Indonesia
- Ireland
- Israel
- Italy
- Japan
- Malaysia
- Mexico
- Poland
- Romania
- Singapore
- South Korea
- Slovakia
- Sweden
- Taiwan
- Turkey
- Ukraine
- United States
- Vietnam

Note: Not all ODMs are in each country
Lenovo Manufacturing

- China
- India
- Mexico
- United States
Ask Your PC Vendors: Hardware Questions

How do you secure your supply chain?

How do you vet your suppliers?

Where will my PCs be manufactured?

Who will manufacture my PC – you or an ODM?
Firmware

Who makes my PC’s firmware and why should I update it?
Firmware is Everywhere

Definition: Firmware

• Embedded, non-volatile software for low-level hardware control, monitoring, and data manipulation
Definition: **UEFI**

- Unified Extensible Firmware Interface provides the interface between firmware and Operating System; the modern PC BIOS

**Introduction to UEFI**

- Developed EFI in ’90s to address legacy BIOS limitations
- Contributed EFI v1.10 to UEFI Forum in 2005
- TianoCore open source UEFI core implementation
- Consortium of interested parties
- Maintains UEFI specifications
**UEFI Origins**

**Definition: IBV**
- Independent BIOS Vendors are 3rd-party UEFI developers that sell value-added UEFI, toolkits, and custom development services.
UEFI By The Numbers

FACTOID

• OEMs typically originate <10% of the UEFI code in your computer

![Diagram showing the percentage of source code contributed by different vendors and IBV in three products: Product 1 (IBV A), Product 2 (IBV B), and Product 3 (No IBV).]

Copyright © 2016
IBV UEFI Development

Note: Not all IBVs are in each country

Copyright © 2016
Lenovo UEFI Development

Lenovo

- China
- Japan
- United States
Why Update?

FACTOID

- Common UEFI / IBV code leads to common vulns across OEMs
- OEM UEFI updates often bundle other firmware updates

Industry UEFI Vulnerabilities Exist – Past Year Highlights

<table>
<thead>
<tr>
<th>AMT Config via USB</th>
<th>Insertion of specially prepared USB drive</th>
<th>Surreptitious access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Sinkhole</td>
<td>Legacy CPU feature abuse</td>
<td>Privilege escalation</td>
</tr>
<tr>
<td>Speed Racer</td>
<td>Protection race condition</td>
<td>Privilege escalation</td>
</tr>
<tr>
<td>SMM Incursion</td>
<td>Unchecked function calls</td>
<td>Privilege escalation</td>
</tr>
<tr>
<td>S3 Boot Script</td>
<td>Protections cleared on resume</td>
<td>Privilege escalation</td>
</tr>
<tr>
<td>UEFI Variables</td>
<td>UEFI security feature bypass</td>
<td>Privilege escalation, DoS</td>
</tr>
<tr>
<td>Capsule Update</td>
<td>Buffer overflow</td>
<td>Privilege escalation</td>
</tr>
</tbody>
</table>

Most (All?) PCs are Vulnerable

- Firmware updates are “scary”, so firmware is rarely – if ever – updated

Copyright © 2016
What measures do you take to provide secure code?

How do you document security issues and distribute fixes?

How do customers report security issues?
Software

What are common security issues?
Lenovo’s Cleaner and Safer Initiative

**FACTOID**
- 100% of software had at least 1 security finding, regardless of supplier – writing secure software is an industry-wide challenge

- **Industry First – Wholesale Application Security Security Reviews**
  - Covers Windows 10 pre-loaded applications

- **Methodology**
  - ✔ Questionnaire
  - ✔ Risk ranking
  - ✔ Risk-based security review

- **Results**
  - ✔ 100+ questionnaires reviewed and ranked
  - ✔ 50+ hands-on 1st and 3rd-party security reviews
  - ✔ 160+ potential security vulnerabilities remediated

Copyright © 2016
Common Software Security Issues

FACTOID
• Software from vendors of all sizes and reputations had findings

- Privilege Escalation
- Excessive Attack Surface / Known Vulns / Insecure Config
- Privacy Exposure
- Insecure Auto-Update / Network Downloads
- Certificate Installation
- Dirty Uninstallation

See backup slides for additional detail.
Ask Your PC Vendors: Software Questions
(Firmware Questions apply, too!)

How do you assess software security?

How do you hold suppliers accountable?

Have you ever not shipped software due to security issues?
Tips

What security things do I need to know when buying PCs?
<table>
<thead>
<tr>
<th>Security-Related PC Purchasing Tips</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Speak with Product Security Team</strong></td>
</tr>
<tr>
<td>• Ask questions – like those in this presentation</td>
</tr>
<tr>
<td>• No security team? Find another vendor…</td>
</tr>
<tr>
<td><strong>Seek “More Local” Product Origins</strong></td>
</tr>
<tr>
<td>• US or Trade Agreement Act (TAA)-compliant manufacturing may be an option</td>
</tr>
<tr>
<td><strong>Seek Custom Pre-load Images</strong></td>
</tr>
<tr>
<td>• Custom pre-loaded disk images, built to your corporate standards, may be an option</td>
</tr>
<tr>
<td><strong>Communicate Requirements, Desires, Concerns</strong></td>
</tr>
<tr>
<td>• The market drives OEMs; large OEMs can drive industry change</td>
</tr>
</tbody>
</table>
THANK YOU

DAKUJEM  DANK  BEDANKT  MERCI  TAKK  谢谢
ありがとう  СПАСИБО  GRACIAS  DZIĘKUJĘ  DANKE
OBRIGADO  БЛАГОДАРЯ  GRAZIE  תודה  GRACIAS

Bill Jaeger
bjaeger@lenovo.com
**Common Software Security Issues** (1/3)

**Privilege Escalation**
- Insufficient input validation, particularly between user and kernel processes
- Excessive file permissions for files executed by privileged processes
- User-influenced temporary files executed by privileged processes
- Permissive directories inserted into PATH + PATH-based DLL invocation

**Excessive Attack Surface / Known Vulns / Insecure Config**
- Runs with excessive permissions
- Listens unnecessarily to network interfaces
- Unnecessarily or permissively modifies Windows firewall rules
- Dependent software or libraries have known vulnerabilities
- Uses a known insecure configuration
Common Software Security Issues (2/3)

Privacy Exposure
- Transmission of PII, disallowed data, or not covered by Privacy Policy
- Transmission of allowable data via HTTP
- Invasive or overly persistent mechanisms to collect and report data
- Use of weak “custom” encryption mechanisms or use of encoding (i.e., BASE64) without encryption

Insecure Auto-Update / Network Download
- Improper download signature validation
- Susceptible to MITM attack
  - Insecure downloads via HTTP
  - Improper TLS certificate validation
Certificate Installation
• Reinstallation of Microsoft-provided CA certificates
• Installation of self-signed certificates

Dirty Uninstallation
• Residual services, tasks, firewall rules, files, registry keys, certificates, etc. left upon uninstall