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

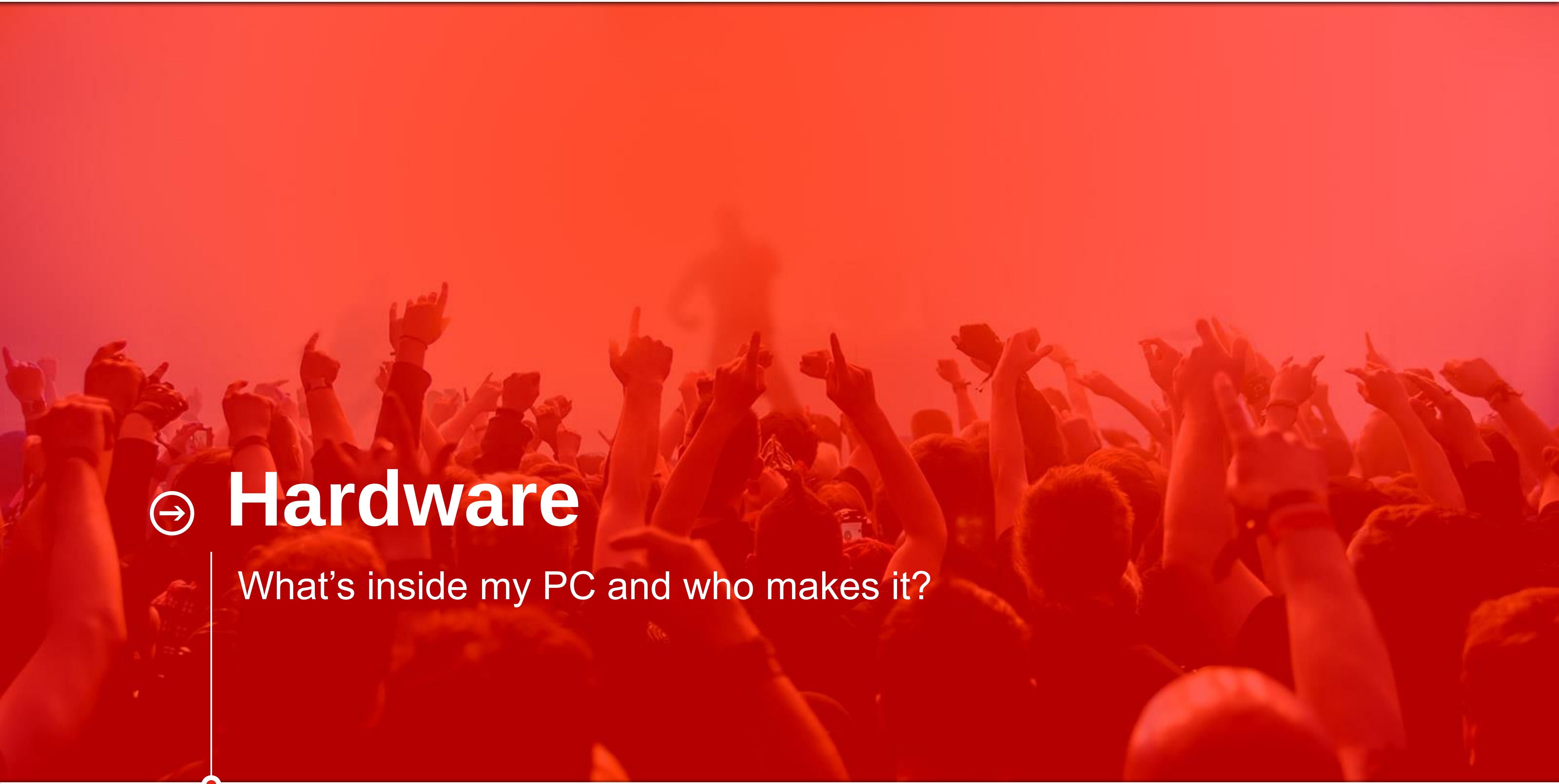
- Director, Security Architecture since February, 2014
- Founding member of Product Security Office
- Work with global product teams and industry partners to enhance product security
- Achieving company – and industry! – security “firsts”

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®

What’s Behind the Curtain?

Hardware	• What’s inside my PC and who makes it?
Firmware	• Who makes my PC’s firmware and why should I update it?
Software	• What are common security issues?
Tips	• What security things do I need to know when buying PCs?
Bonus!	• Factoids, definitions, and questions to ask your PC vendors



Hardware

What’s inside my PC and who makes it?

What’s Inside?

FACTOID

- PCs are a commodity, w/ common technologies across brands
- Differentiators are design, specs, support, security, etc…

CPU	AMD intel
Memory	Micron SAMSUNG
TPM	Atmel Infineon intel nuvoTon 新唐科技 ST life.augmented
Disk	HGST intel Micron SAMSUNG SanDisk SEAGATE WD Western Digital
Video	AMD intel NVIDIA

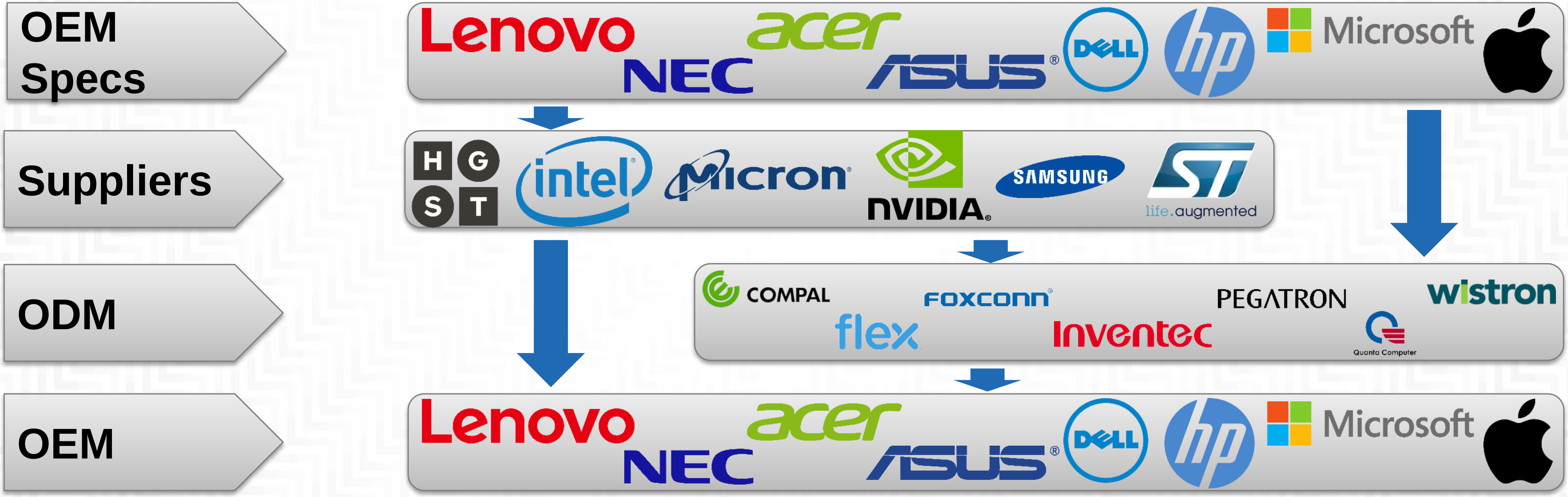
Who Makes My PC?

Definition:
ODM

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

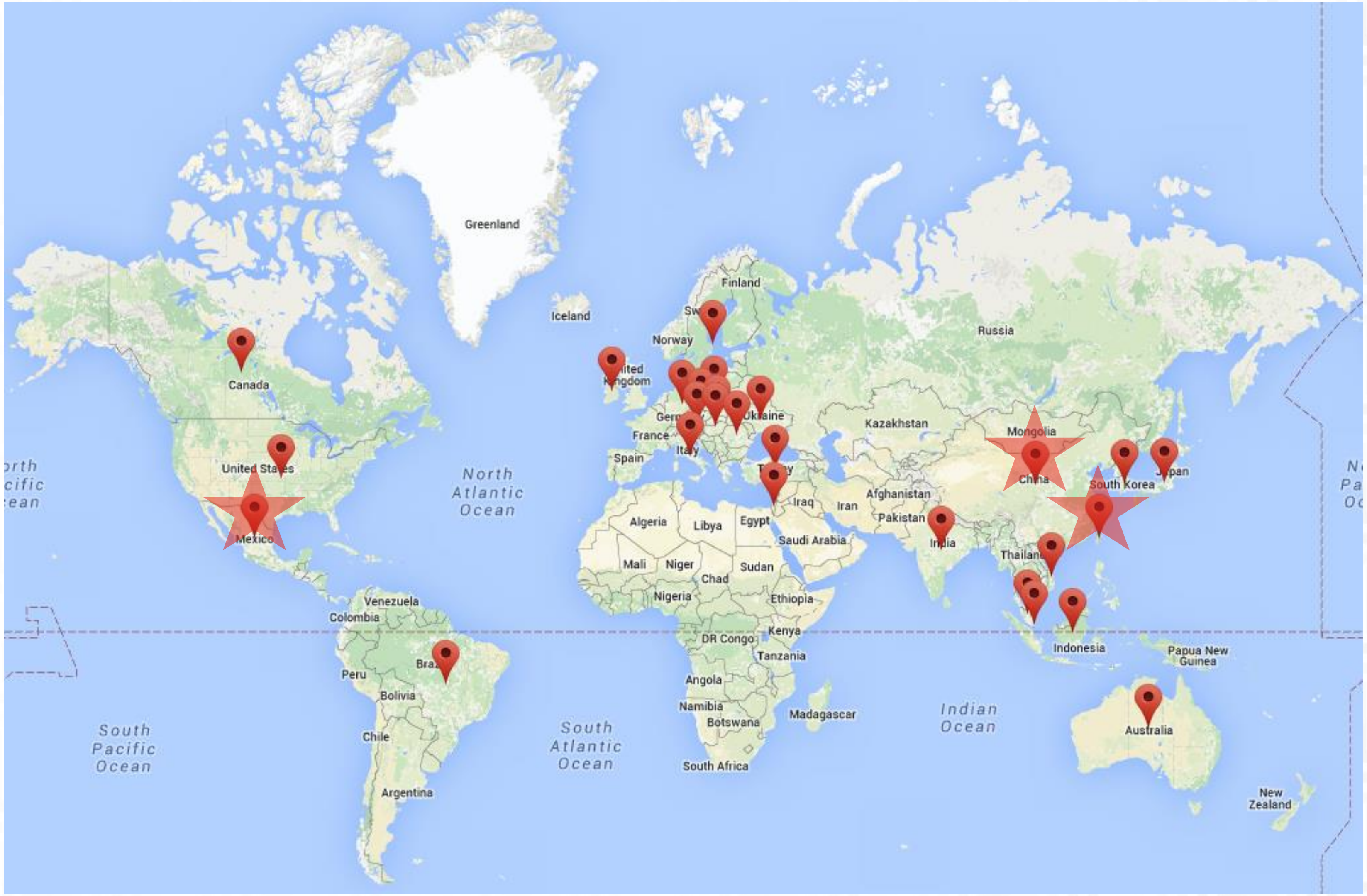
Definition:
OEM

- Original Equipment Manufacturer is the manufacturer, spec originator, or performs final transformation (assembly)



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

Greenland
Iceland
Finland
Sweden
Norway
Russia
United Kingdom
Canada
Poland
Germany
Ukraine
France
Kazakhstan
Mongolia
Italy
Spain
Turkey
United States
North Atlantic Ocean
North Pacific Ocean
Japan
China
South Korea
Iraq
Iran
Afghanistan
Pakistan
Algeria
Libya
Egypt
Saudi Arabia
India
Mexico
Thailand
Mali
Niger
Sudan
Chad
Nigeria
Ethiopia
Venezuela
Colombia
Kenya
DR Congo
Tanzania
Indonesia
Papua New Guinea
Brazil
Peru
Angola
Bolivia
Namibia
Botswana
Madagascar
Indian Ocean
South Pacific Ocean
Chile
South Atlantic Ocean
Australia
South Africa
Argentina
New Zealand

Lenovo

- China
- India
- Mexico
- United States

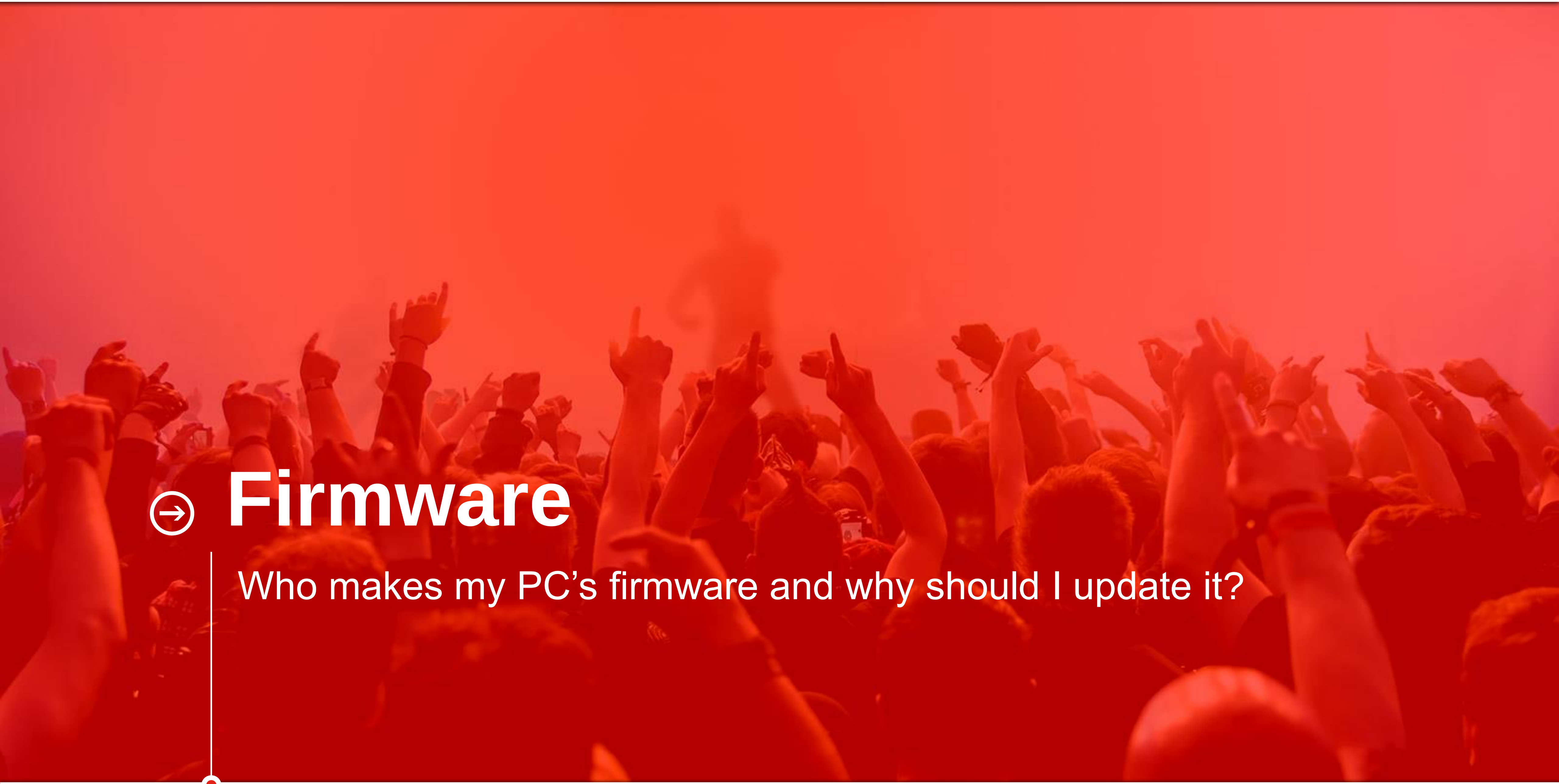
Ask Your PC Vendors: Hardware Questions

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?



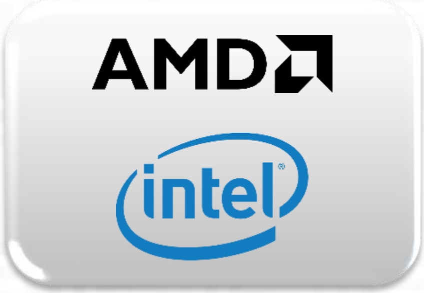
Firmware

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

Firmware is Everywhere

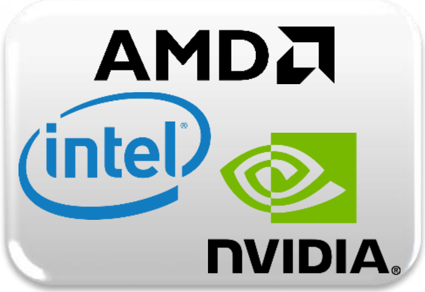
Definition:
Firmware

- Embedded, non-volatile software for low-level hardware control, monitoring, and data manipulation



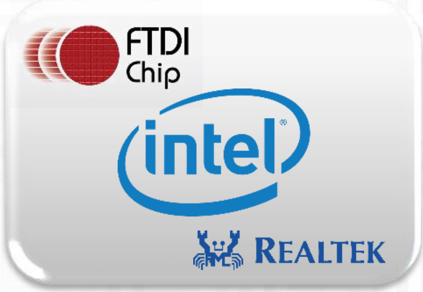
CPU Microcode

UEFI (BIOS)



Video

Disk and Controller



USB

Management Engine, vPro

SuperIO, System Management

Trusted Platform Module

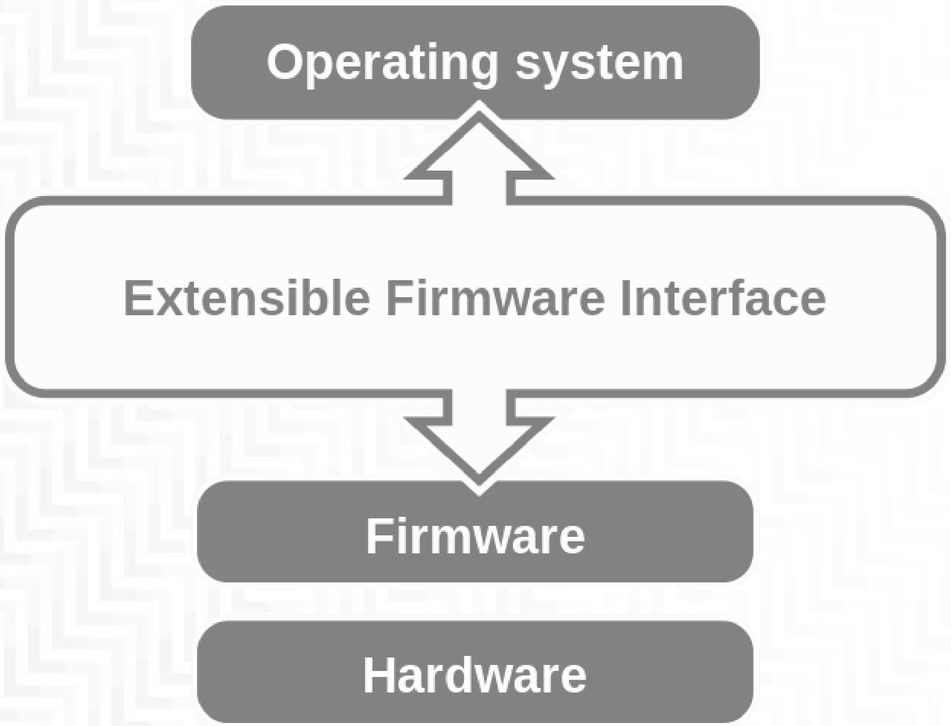
Ethernet, Wi-Fi

More...

Introduction to UEFI

Definition:
UEFI

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



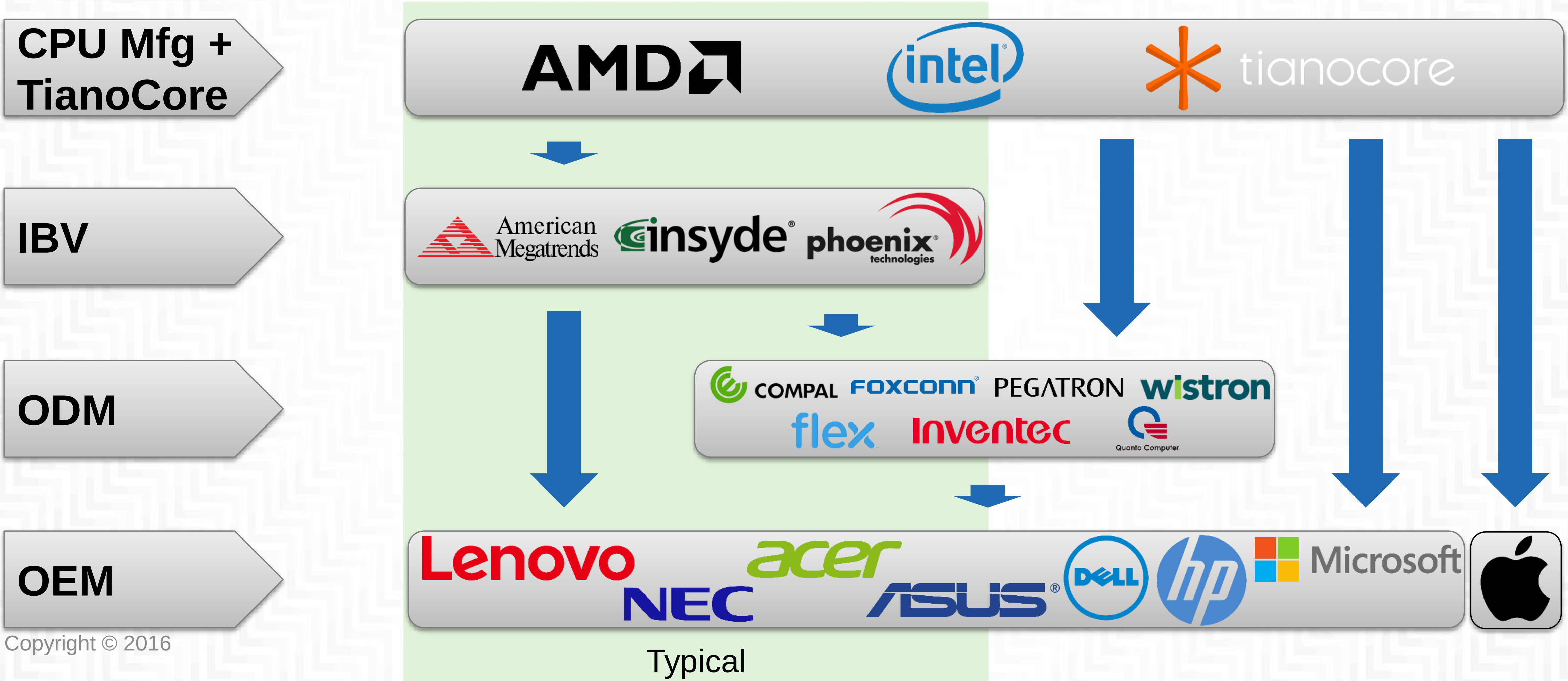
- Developed EFI in ’90s to address legacy BIOS limitations
- Contributed EFI v1.10 to UEFI Forum in 2005
- TianoCore open source UEFI core implementation

- 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



CPU Mfg + TianoCore

IBV

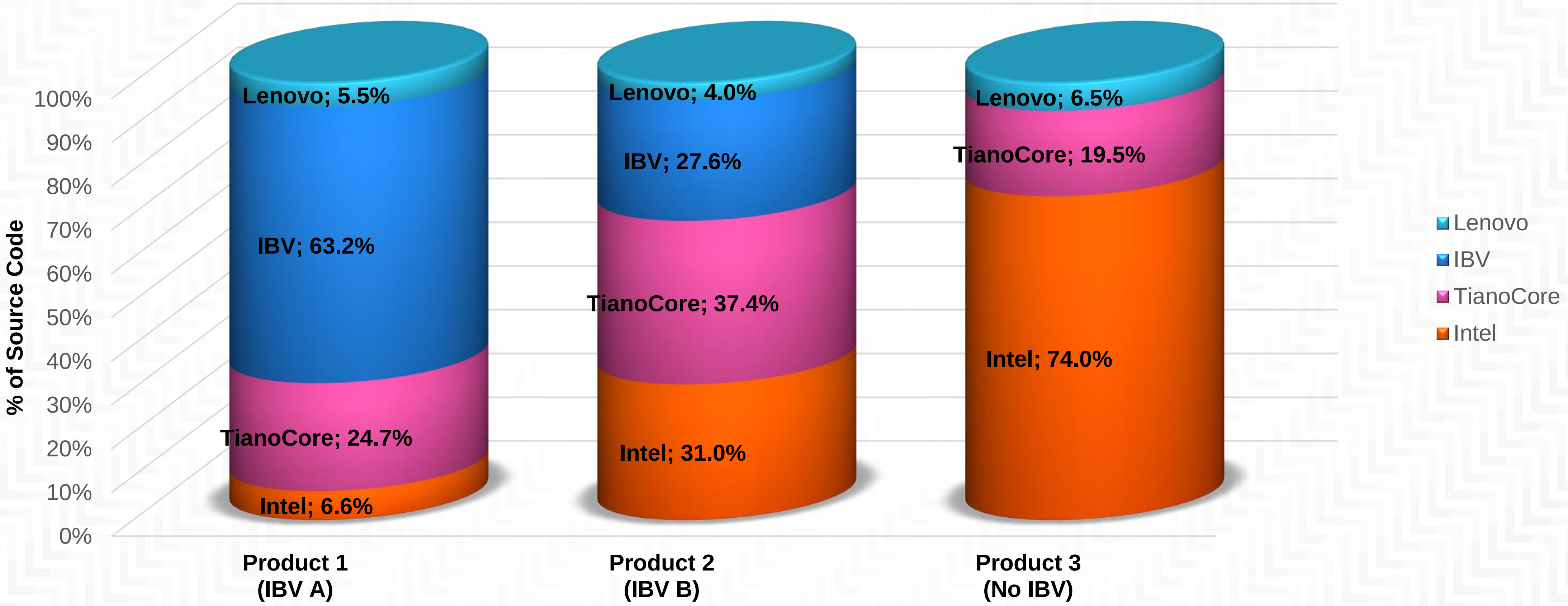
ODM

OEM

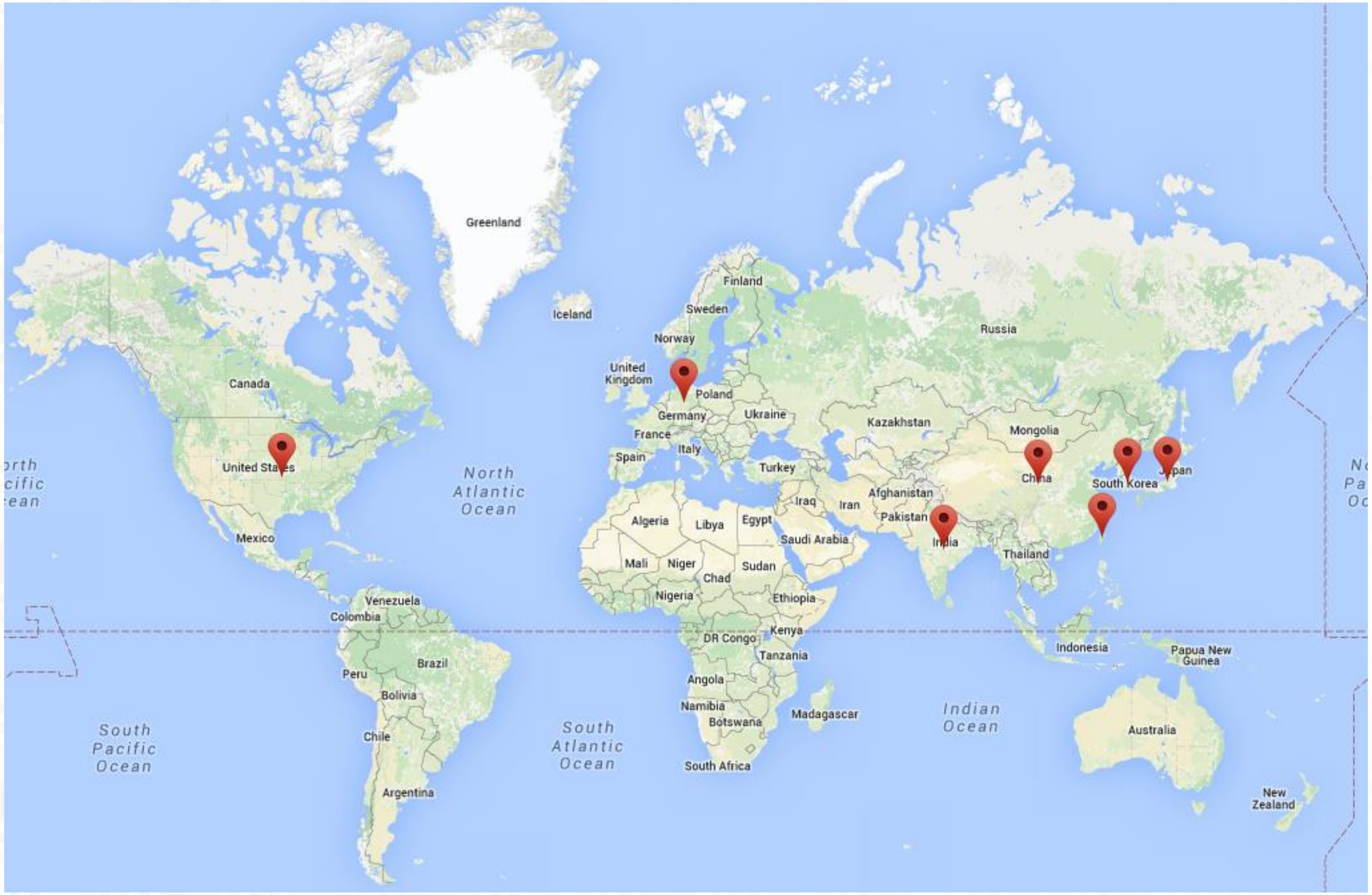
UEFI By The Numbers

FACTOID

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



IBV UEFI Development



Note: Not all IBVs are in each country

American Megatrends

- China
- Germany
- India
- Japan
- Taiwan
- South Korea
- United States

insyde®

- China
- Japan
- Taiwan
- South Korea
- United States

phoenix® technologies

- Japan
- Taiwan
- South Korea
- United States

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**

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

- **Most (All?) PCs are Vulnerable**
  - Firmware updates are “scary”, so firmware is rarely – if ever – updated

Ask Your PC Vendors: Firmware Questions

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 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

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?

Security-Related PC Purchasing Tips

Speak with Product Security Team

- Ask questions – like those in this presentation
- No security team? Find another vendor…

Seek “More Local” Product Origins

- US or Trade Agreement Act (TAA)-compliant manufacturing may be an option

Seek Custom Pre-load Images

- Custom pre-loaded disk images, built to your corporate standards, may be an option

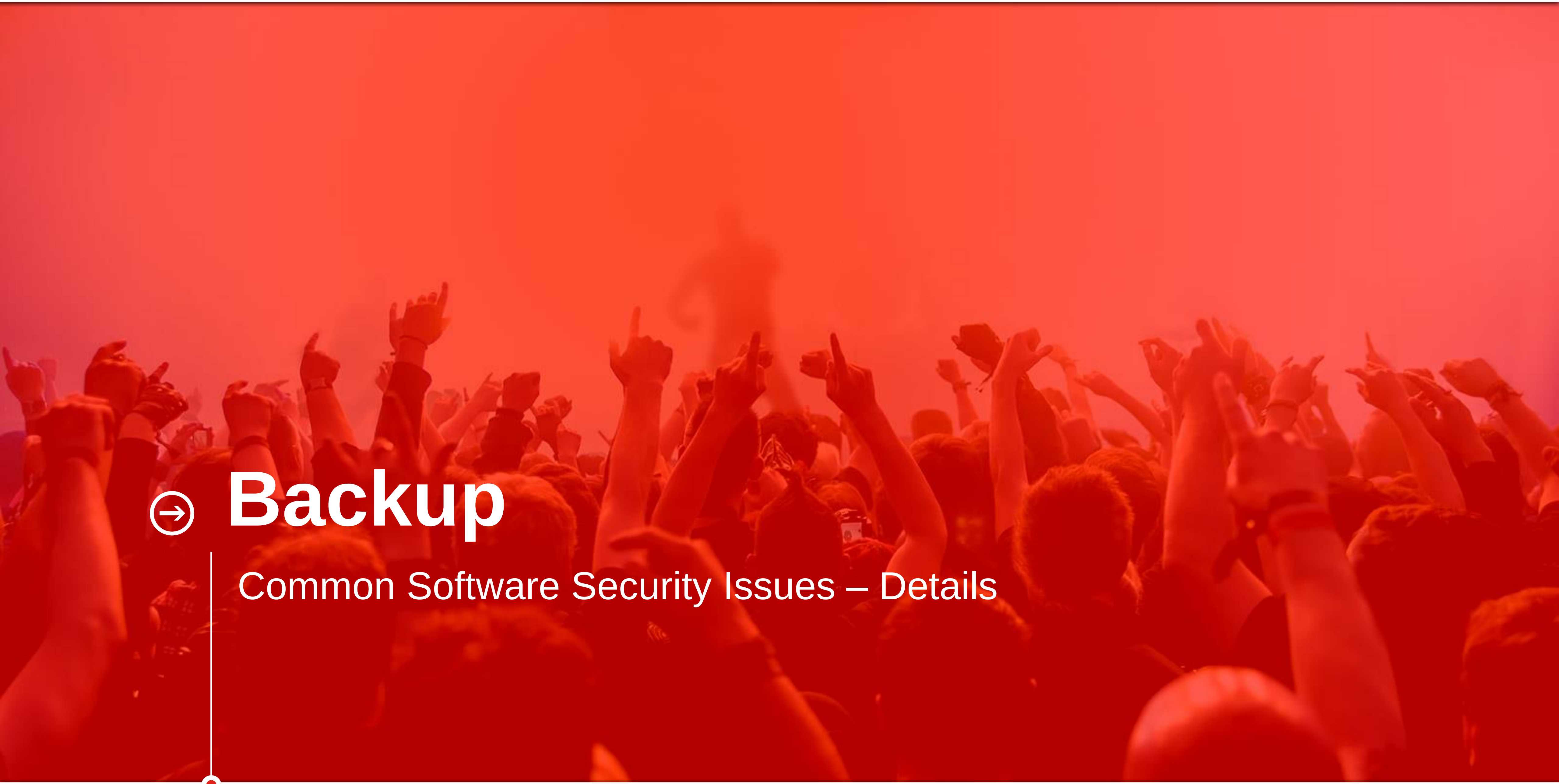
Communicate Requirements, Desires, Concerns

- The market drives OEMs; large OEMs can drive industry change

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



Backup

Common Software Security Issues – Details

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

Common Software Security Issues (3/3)

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