Bringing The Trust Back Into Cyber Space:

Extending Intel's commitment to Security

Steve Pawlowski

Intel Senior Fellow
GM, Central Architecture and Planning
CTO, Intel Architecture Group

Legal Disclaimer

Intel and the Intel logo are trademarks or registered trademarks of
Intel Corporation or its subsidiaries in the United States and other countries.

Other names and brands may be claimed as the property of others.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. All dates and product descriptions provided are subject to change without notice. This slide may contain certain forward-looking statements that are subject to known and unknown risks and uncertainties that could cause actual results to differ materially from those expressed or implied by such statements

The threats and attack examples provided in this presentation are intended as examples only. They are not functional and cannot be used to create security attacks. They are not be replicated and/or modified for use in any illegal or malicious activity.

Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license.

"Security" is a relative, not absolute, term. No product can provide complete security to the user as all security schemes have inherent limitations. However, some products provide more protection than others.

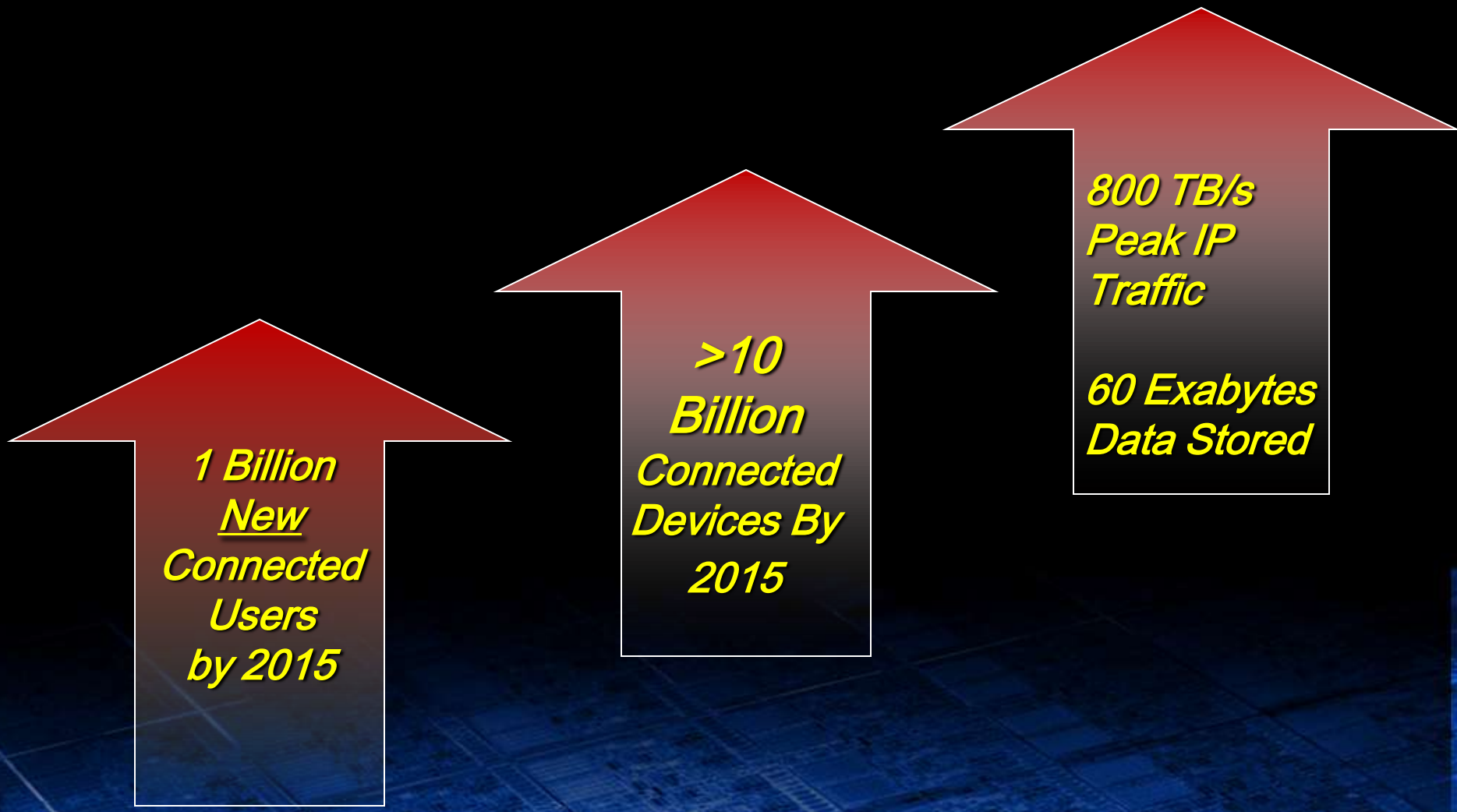
No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses.

The original equipment manufacturer must provide TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.

Enabling Execute Disable Bit functionality requires a PC with a processor with Execute Disable Bit capability and a supporting operating system. Check with your PC manufacturer on whether your system delivers Execute Disable Bit functionality.

- All information provided related to future Intel products and plans is preliminary and subject to change at any time, without notice.
- Intel, the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- * Other names and brands may be claimed as the property of others.

More Users, More Devices, More Data



Source: IDC "Server Workloads Forecast" 2009 and IDC "The Internet Reaches Late Adolescence" Dec 2009, extrapolation by Intel for 2015 , IDC Embedded Internet Project, 2009; Intel estimates Nov 2009, 8x Network: 800 Terabytes / second of IP traffic estimated on Internal Intel analysis "Network Supply/Demand 2010-2020" forecast . 16x Storage: 60 Exabytes of data stored from Barclays Capital "Storage Bits" Sept 2009, extrapolation by Intel for 2015; 20x Compute: Intel Internal LRP forecast. Extrapolated to 1 billion virtual servers using 1 vm/core,

New (Ecosystem = Vulnerabilities = Threats)

Television

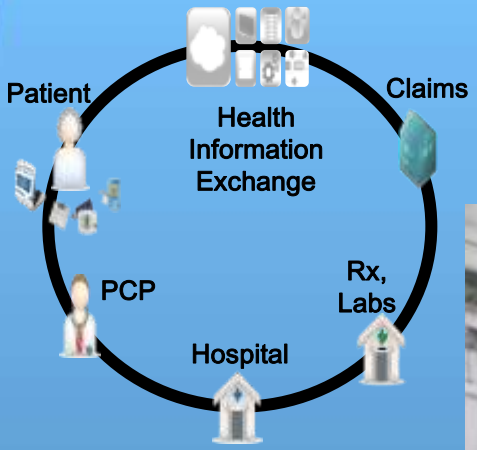
Embedded

Auto

PC Clients

Handhelds

Servers



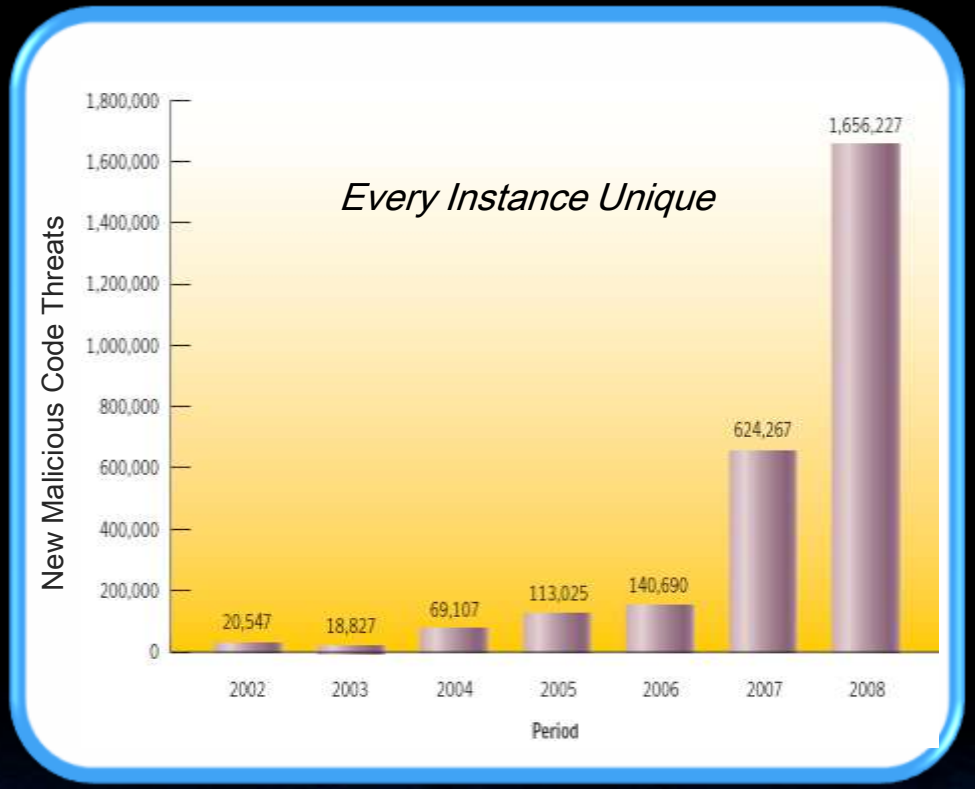
Intel Architecture Across All These Ecosystems

Malware Threats are Outracing Solutions

Goals of Malware have changed – It is a business today

Asset Protection is Vital

Increasing number of zero day attacks



No Silver Bullet Solution Today

intel

Areas of Vulnerability

Firmware - A New Target for Attack

"Trusted" third-party Websites
Susceptible to Exploitation Code

Vulnerabilities in Popular Applications
Buffer Overflows Due to Programming Errors

Fragmented Security Solutions

http://www.sans.org/top-cyber-security-risks/

Cyber Attacks -
It's more than Worms, Hacking, & Phishing

Cyber Attacks Are
Holistic, Coordinated, & Smarter

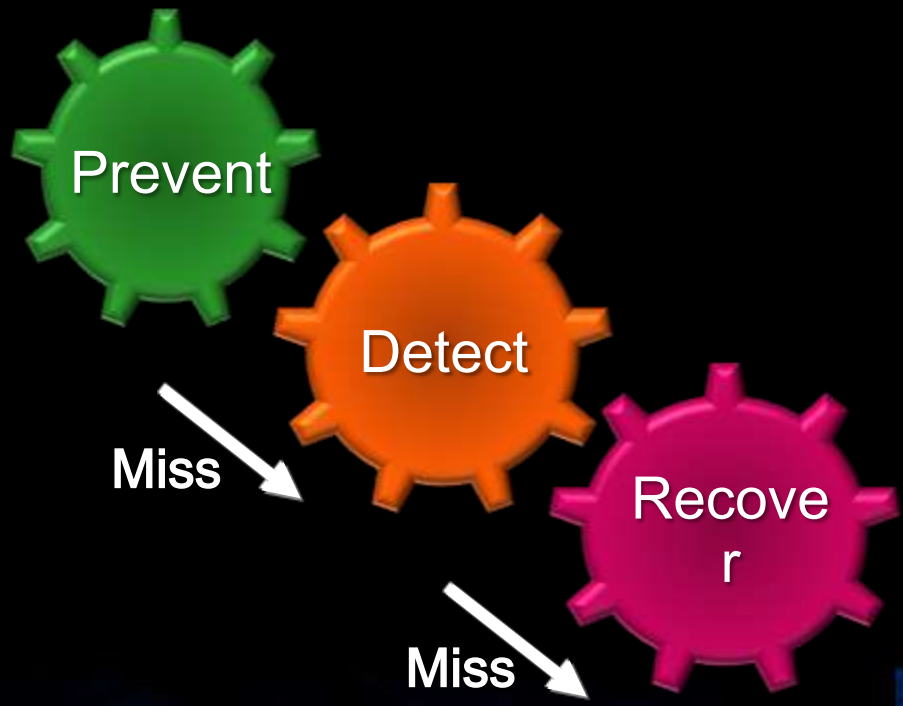
intel

More Unknown Than Known Out There
Predict – But Learn To Recover

Prevent the Security & Trust Infractions

Detect the Security & Trust Infractions

Recover *quickly* *and* *gracefully* from the Security & Trust Infractions



Intel's Security Vision

Deliver the Foundation for Trustworthy Platforms

Trust Establishment

Detection & Protection from Malware

Asset & Data Protection

Architectural Leadership

Handheld

Notebook

Desktop

Server

Improving Platform Security
From Handhelds to Data Centers

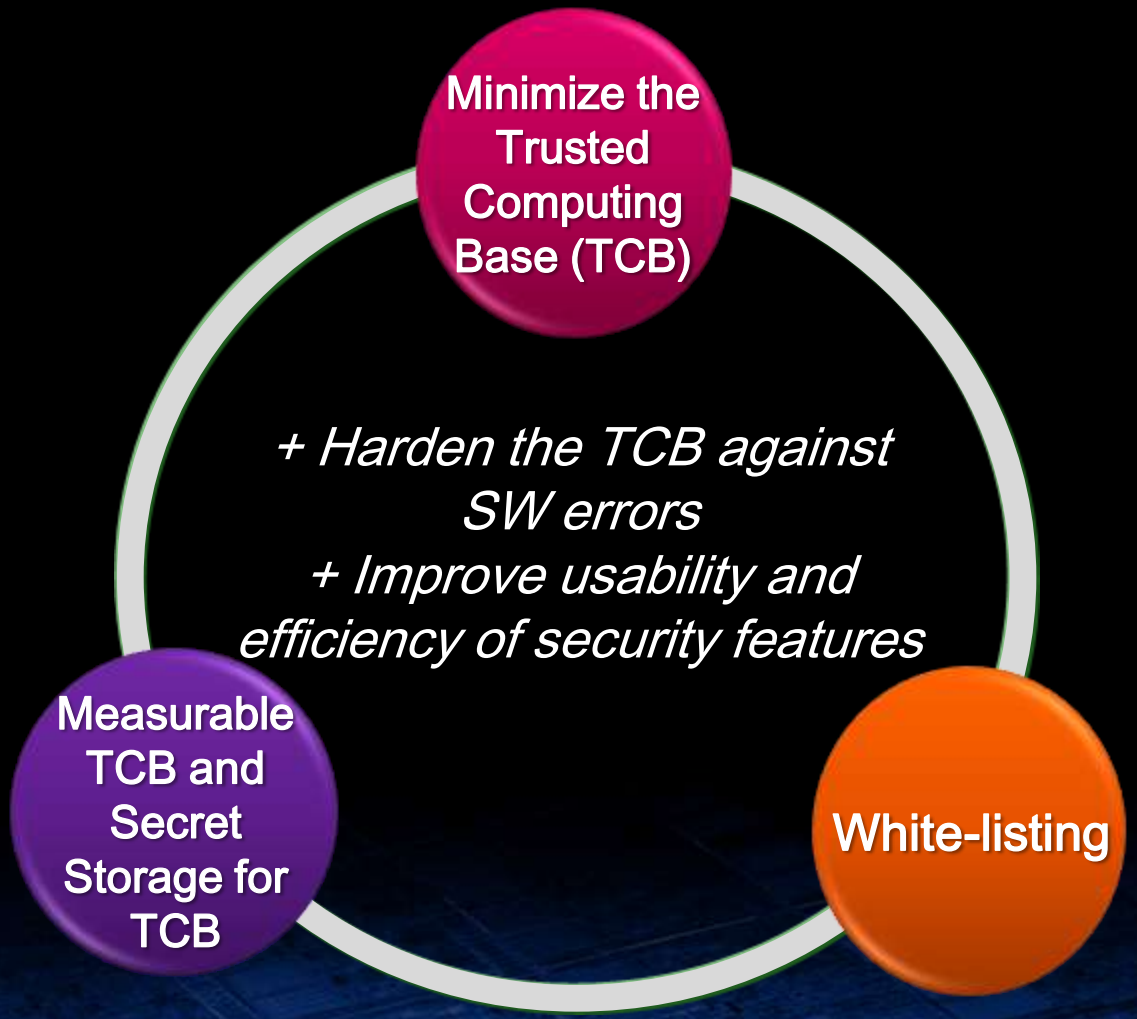
A “Three Prong Attack” to Combat Malware

Continue to harden the base architecture

Deliver a robust silicon-based defense

Deliver a silicon-based trust solution

Our Vision on Minimizing the Threat

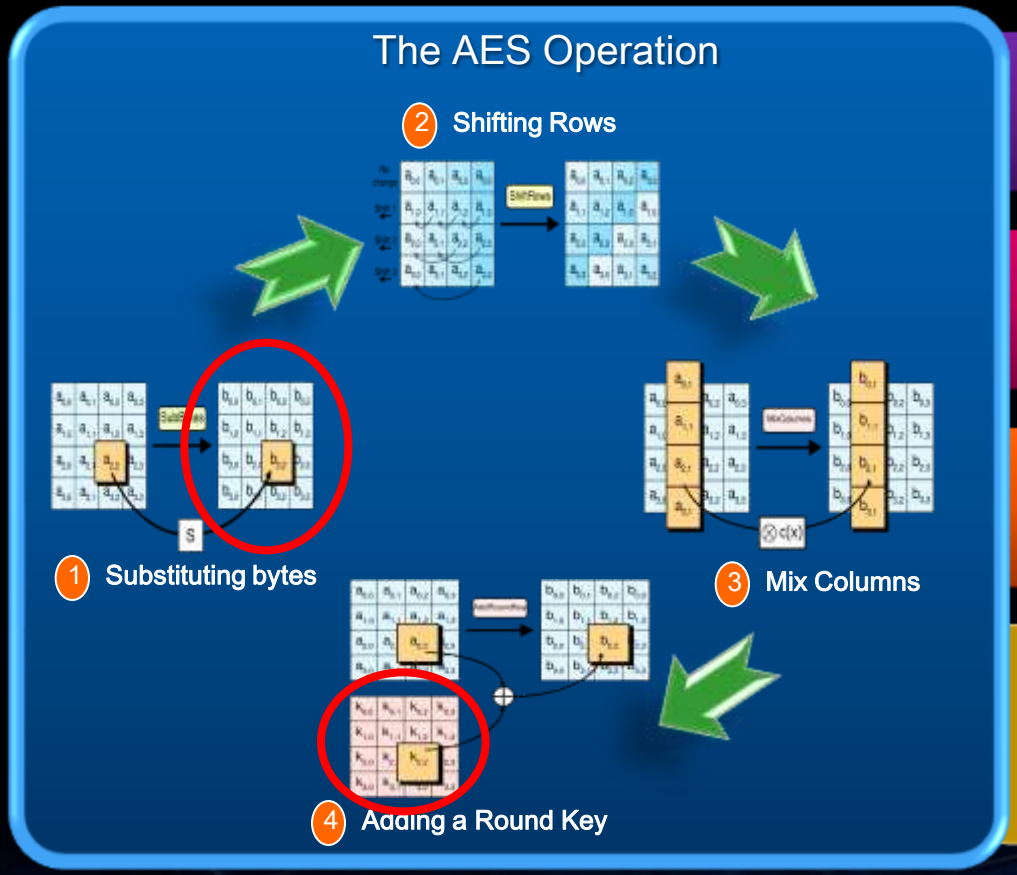


Minimizing the Trusted Computing Base

1 **Use Virtualization Techniques to Isolate**
- Protected or Suspect Files
- VMs from every IO device

2 **Reduce FW and SW in the Trust Boundary**
- Use digital signed code for FW/SW verification
- Launch only know good VMMs (White listing)

Securing Against Side Channel Attacks



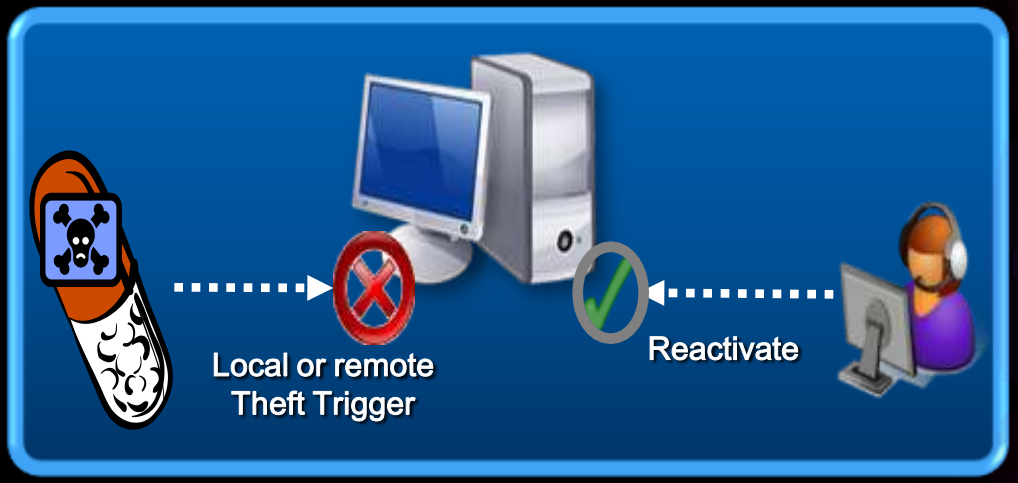
What the attacker wants -
The cipher key

The vulnerability today –
Substitution using look up tables

How the attacker works-
Measure latency of cache lookup

How do we make it more secure –
Operations done in HW with fixed latency

Securing Against Device Theft



Theft Detection

- *Login failures*
- *Timer Expiration*
- *PC hardware / firmware tampering*

"Poison Pill"

- *PC disable*
- *Data access disable*

Recovery

- *Local passphrase / recovery token*
- *Remote unlock*

Looking Over the Horizon

As We Continue Our Focus On Security

Defend Against Firmware Attacks

Keep Data Secure *and* Identity Private

Ensure Application Security

Overcome Programming Errors

Holistic Security Solution

Across the Entire Hardware-Software Stack

Across All IA Architectures from Embedded to Enterprise

Balance Security With Usability

Hardware-Software Co-Design Is Key

Thank You!