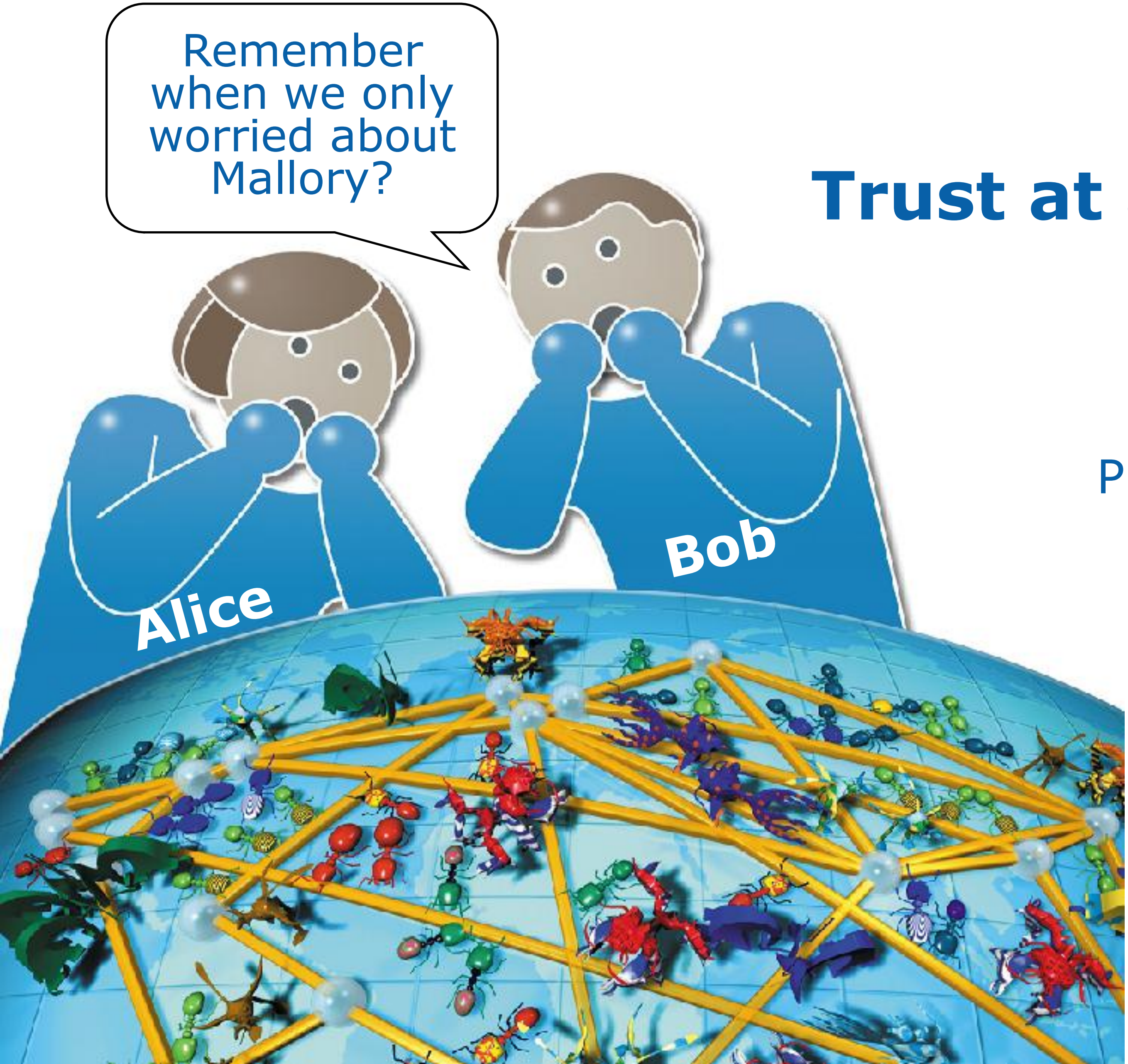


Trust at a Distance
The Vision

David Durham

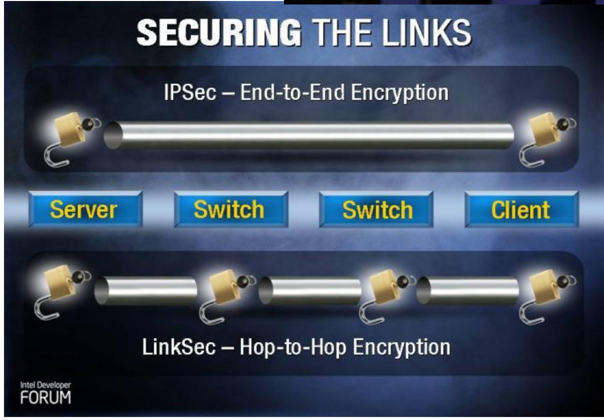
Principal Engineer

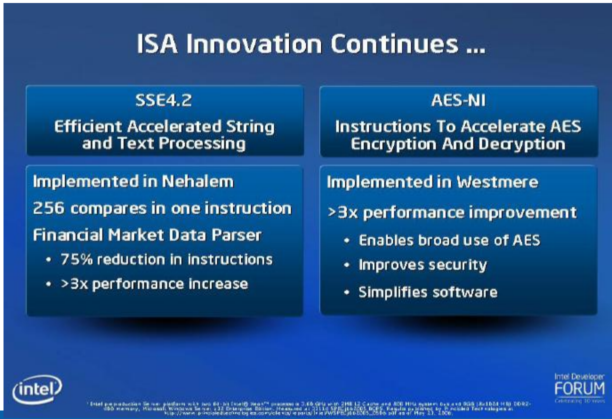
Intel Labs

June, 2009

From Research to Solutions

- Innovation flowing into products
  - Intel® vPro™ w/ AMT 1.0 ('05)
  - System Defense/Heuristics ('06)
  - Network Access Control ('07)
  - Link Layer Security (Linksec, 11i)
  - ISA Crypto Acceleration (soon)
- Industry influence
  - Standards, publications, patents…





ISA Innovation Continues …

SSE4.2 Efficient Accelerated String and Text Processing	AES-NI Instructions To Accelerate AES Encryption And Decryption
Implemented in Nehalem 256 compares in one instruction Financial Market Data Parser • 75% reduction in instructions • >3x performance increase	Implemented in Westmere >3x performance improvement • Enables broad use of AES • Improves security • Simplifies software

*Third party marks and brands are the property of their respective owners

Internet Full of Promise – Also Peril

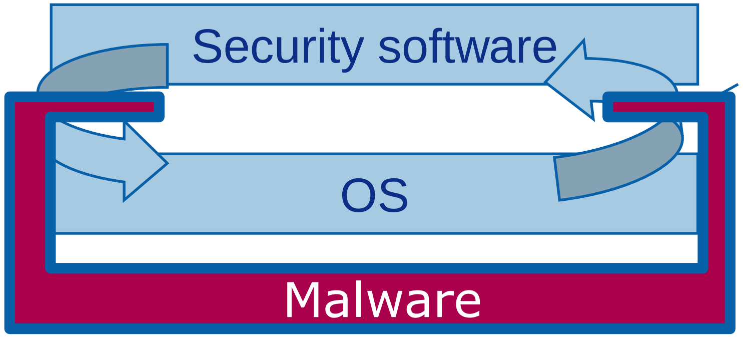
As commerce, content & personal information moves online – *malice follows*

- Cybercriminals profit from your information
  - Phishing/Social Engineering
  - Identity Theft
  - Espionage/Extortion

> **"We estimate consumer losses to phishing scams at almost a half-billion dollars during the past two years.."[1]**

> **"In 2008, we created 1.6M new malicious code signatures – That's more than we created in the past 17 years.."[2]**

- Evolving attack sophistication
  - Combining spam, spyware, viruses and other malware in the attacks
  - Arms race between good and bad guys



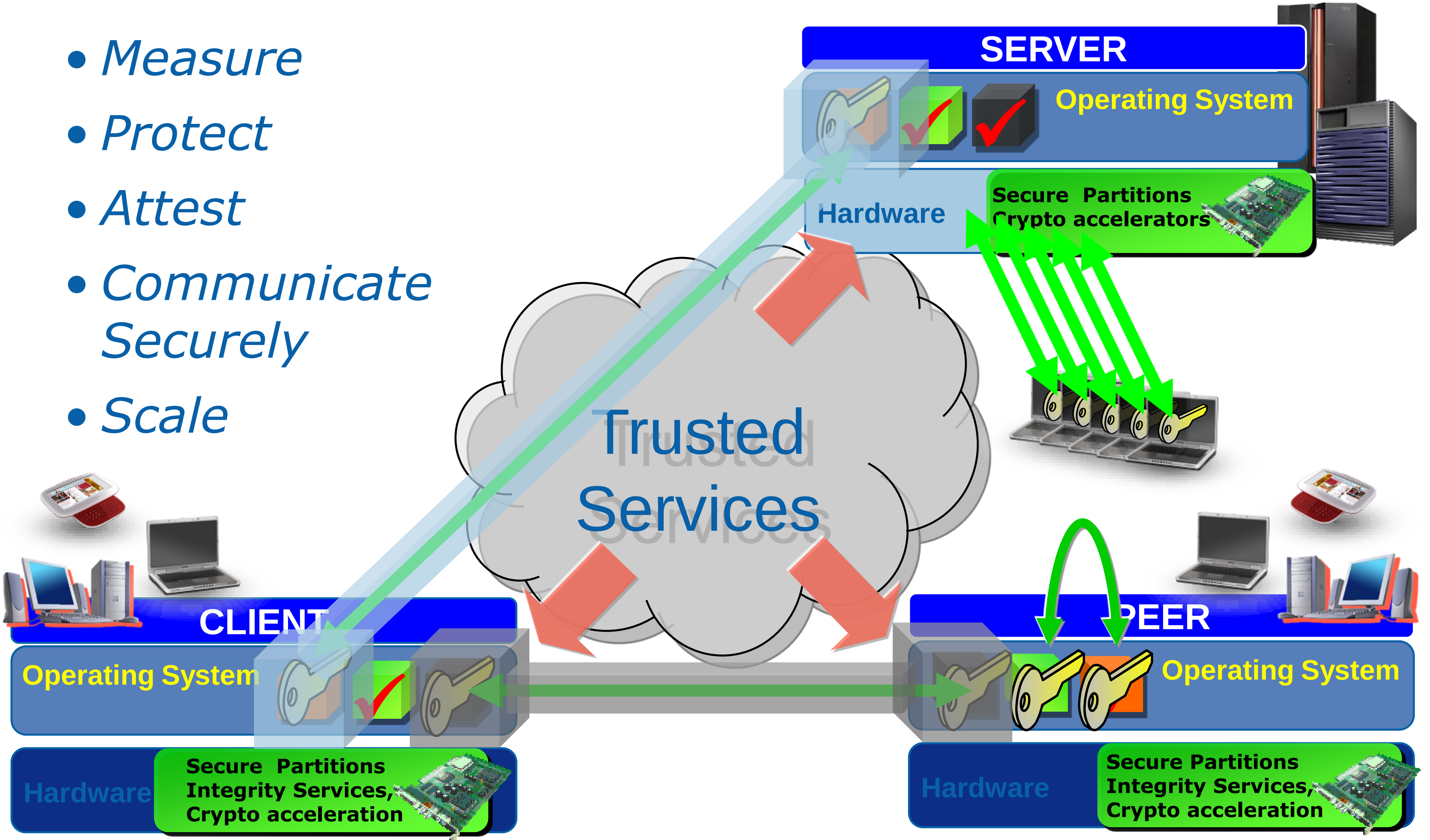
New Approaches Warranted To Preserve Trust

[1] Cost of Phishing – Consumer Reports, June 2009
[2] Enrique Salem – CEO Symantec, 2009 RSA Keynote

BUILD

The Vision: Establish Trust at a Distance

- *Measure*
- *Protect*
- *Attest*
- *Communicate Securely*
- *Scale*



*Third party marks and brands are the property of their respective owners

Three Focus Areas for a Trustworthy Cloud

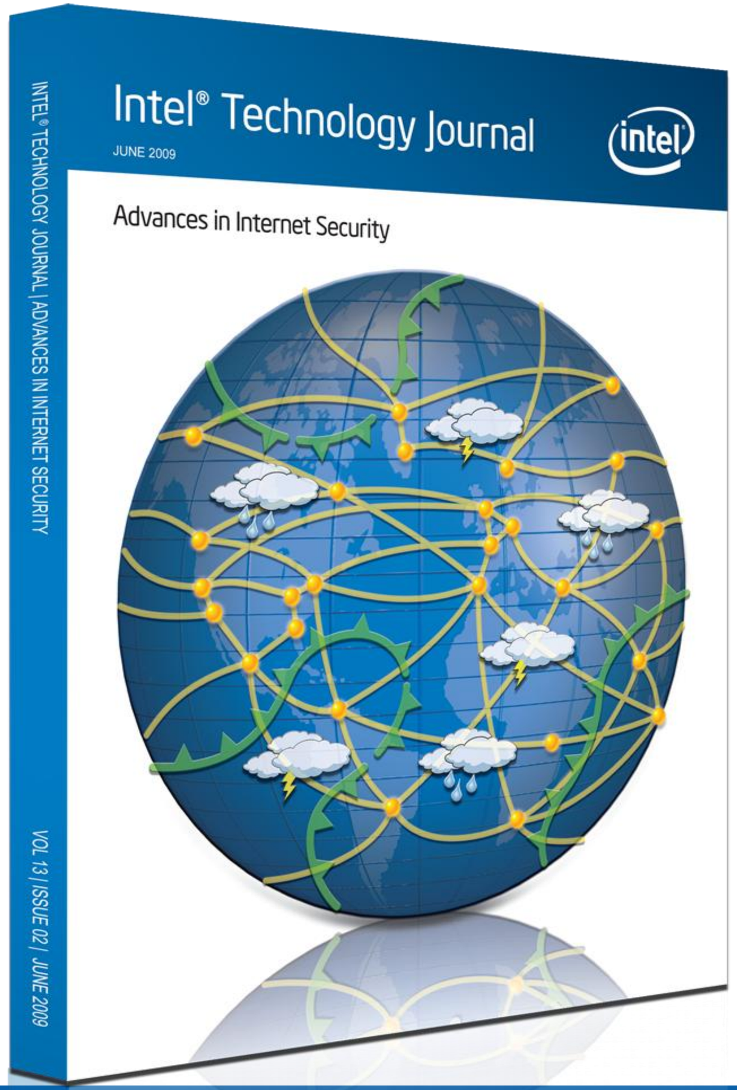
- Endpoint Integrity (redefine the network endpoint)
  - Minimize the Trusted Computing Base (exclude OS, Drivers, etc.)
  - Enable multiple peer TCBs with hw protection boundaries
  - Measurement to attest to true endpoint characteristics
- Cryptographic Acceleration (remove roadblocks)
  - Improve power/performance of cryptographic primitives
  - New focus on expensive asymmetric crypto algorithms
- Distributed Trust
  - Scalability, billions of independent secure connections
  - Automation (Environmental sensing to derive identity)
  - Attestation Services, privacy preserving functional identity

Deliver Trust-at-a-Distance via Intel Platforms and Services

*Third party marks and brands are the property of their respective owners

Intel® Technology Journal-Advances in Internet Security

- Enhanced Detection of Malware
- Protecting Critical Applications on Mobile Platforms
- Providing a Safe Execution Environment
- New Processor Instructions for Accelerating Encryption and Authentication Algorithms
- https://everywhere! Encrypting the Internet
- Recent Contributions to Cryptographic Hash Functions
- Enhanced Privacy ID: A Remote Anonymous Attestation Scheme for Hardware Devices
- Network Security: Challenges and Solutions
- The Dark Cloud: Understanding and Defending against Botnets and Stealthy Malware
- Decentralized Trust Management for Securing Community Networks


Intel® Technology Journal
JUNE 2009
intel
Advances in Internet Security
INTEL® TECHNOLOGY JOURNAL | ADVANCES IN INTERNET SECURITY
VOL 13 | ISSUE 02 | JUNE 2009