Technologies to Improve Platform Security

Ernie Brickell
Intel Corporation

9/29/2011

Security is Intel's Third Value Pillar

Paul Otellini
Intel CEO

Intel is positioning itself to lead in three areas:

- *energy-efficient performance silicon,*
- *connectivity, and*
- *security.*

There's an urgent need for security innovation as people are spending more time online and the amount of data is growing.

Intel Security & Trust Pillars

Identity Protection & Fraud Deterrence

Detection & Prevention of Malware

Securing Data and Assets

Recovery and Enhanced Patching

Intel Security & Trust Pillars

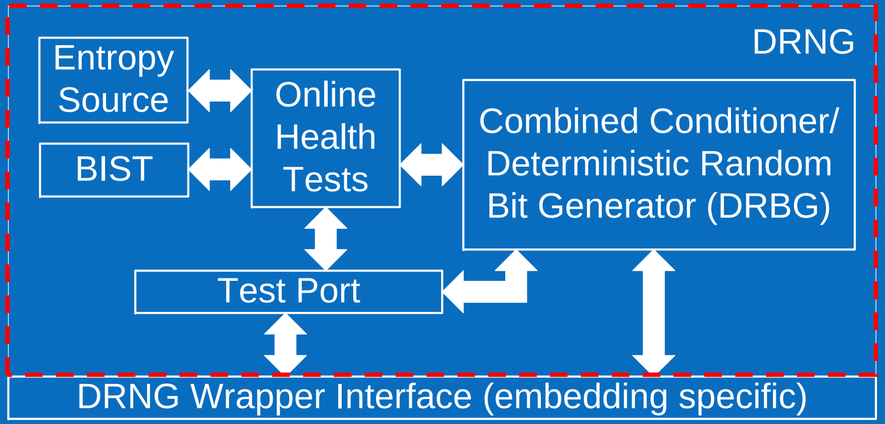
Identity Protection & Fraud Deterrence

Detection & Prevention of Malware

Securing Data and Assets

Recovery and Enhanced Patching

Digital Random Number Generator (DRNG)


DRNG
Entropy Source
BIST
Online Health Tests
Combined Conditioner/ Deterministic Random Bit Generator (DRBG)
Test Port
DRNG Wrapper Interface (embedding specific)

A reusable circuit that provides an autonomous/self contained, complete DRNG

Provides a hardware source of high quality, high performance entropy to be embedded across Intel products. It is composed of

– An all-digital Entropy Source, (3 Gbps, 90% Entropic)

– Runtime Entropy Source health measurement via Online Health Test,

– Conditioning (via AES CBC-MAC mode) and DRBGing (via AES CTR mode) post processing and

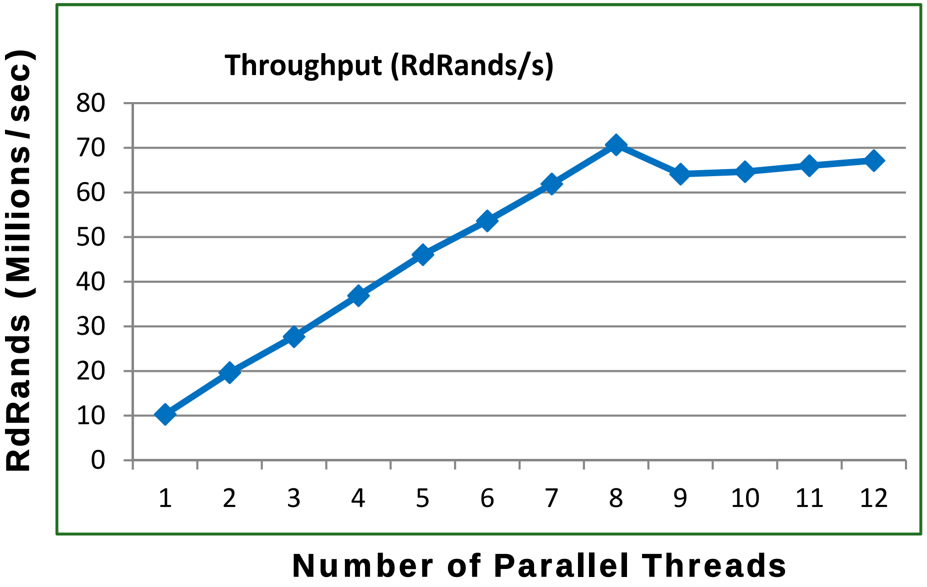
– Built In Self Test (BIST) and Test Port

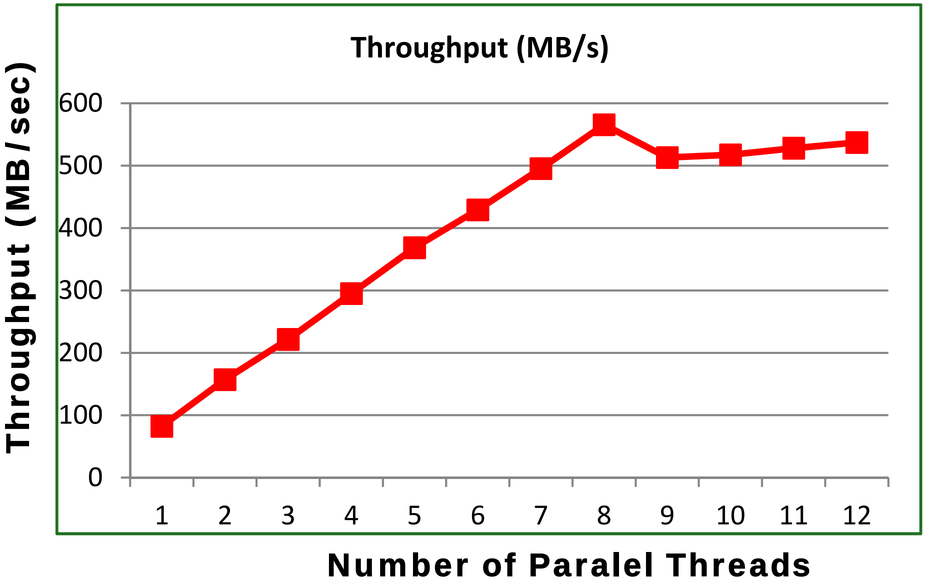
Standards compliant (NIST SP 800-90) and FIPS 140-2/3 Level 2 certifiable as such

RDRAND Performance

Preliminary data from pre-production Ivy Bridge sample[1]

- RdRand – new CPU instruction which provides access to DRNG
- Up to 70 million RdRand invocations per second
- 500+ Million Bytes of random data per second
- Throughput ceiling is insensitive to number of contending parallel threads
  - ❑ Steady state maintained at peak performance





[1] Data taken from Intel® processor codename Ivy Bridge early engineering sample board. Quad core, 4 GB memory, hyper-threading enabled. Software: LINUX* Fedora 14, gcc version 4.6.0 (experimental) with RdRand support, test uses pthreads kernel API

RdRand Response Time and Reseeding Frequency

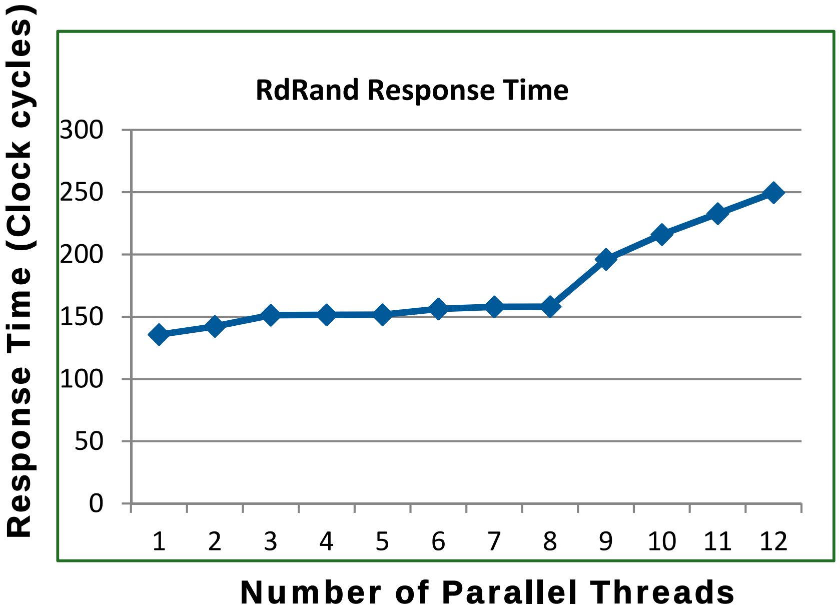
Preliminary data from pre-production Ivy Bridge sample[1]

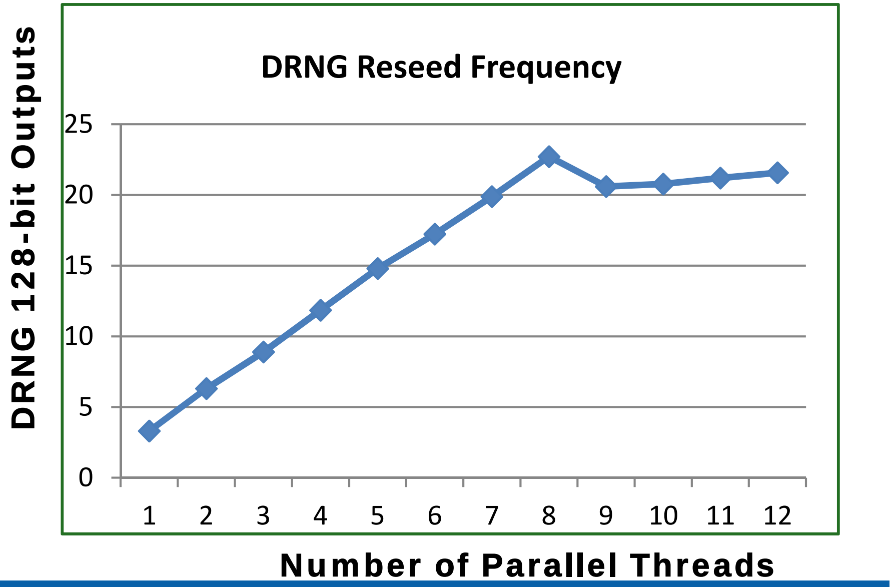
RdRand Response Time

- ~150 clocks per invocation
- Little contention until 8 threads
  - (or 4 threads on 2 core chip)
- Simple linear increase as additional threads are added

DRNG Reseed Frequency

- Single thread worst case: Reseeds every 4 RdRand invocations
- Multiple thread worst case: Reseeds every 23 RdRand invocations
- At slower invocation rate, can expect reseed before every 2 RdRand calls
  - ❑ NIST SP 800-90 recommends ≤ 2^{48}

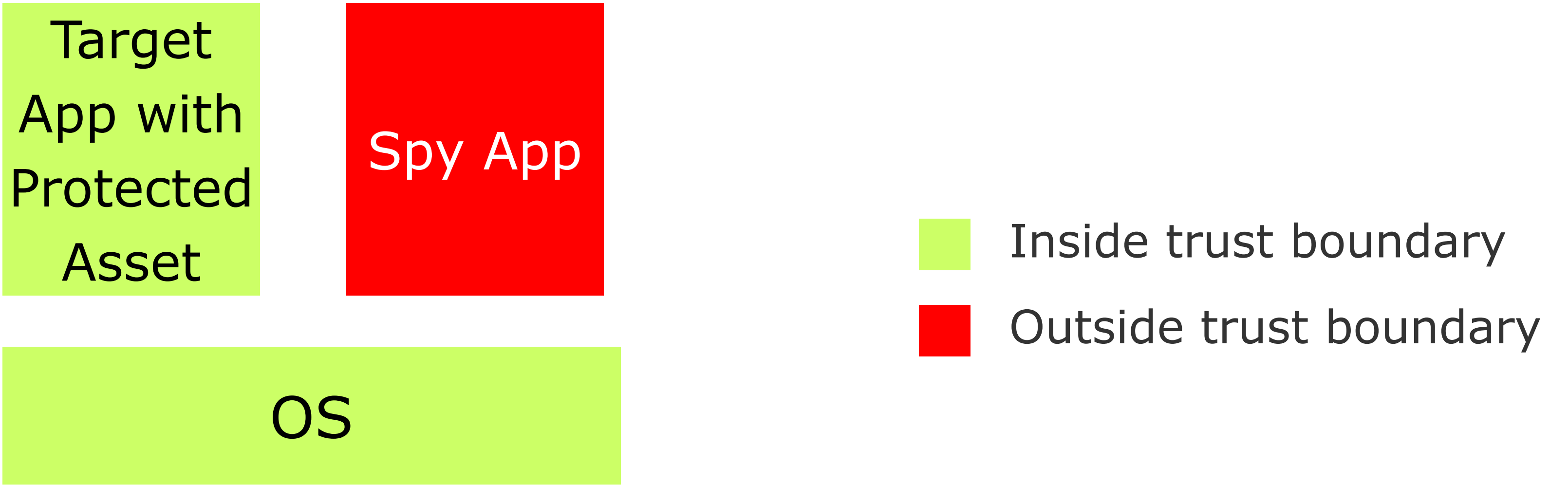




[1] Data taken from Intel® processor codename Ivy Bridge early engineering sample board. Quad core, 4 GB memory, hyper-threading enabled. Software: LINUX* Fedora 14, gcc version 4.6.0 (experimental) with RdRand support, test uses pthreads kernel API

Software Side Channels

- Not Hardware Side Channel where adversary has physical access.
- Not Software Covert Channel where adversary has malware in a high security partition and a low security partition
- Software Side Channel – Adversary has malware executing in a spy process, and tries to obtain information about an uncompromised target process executing on same platform.



Protection from software side channels

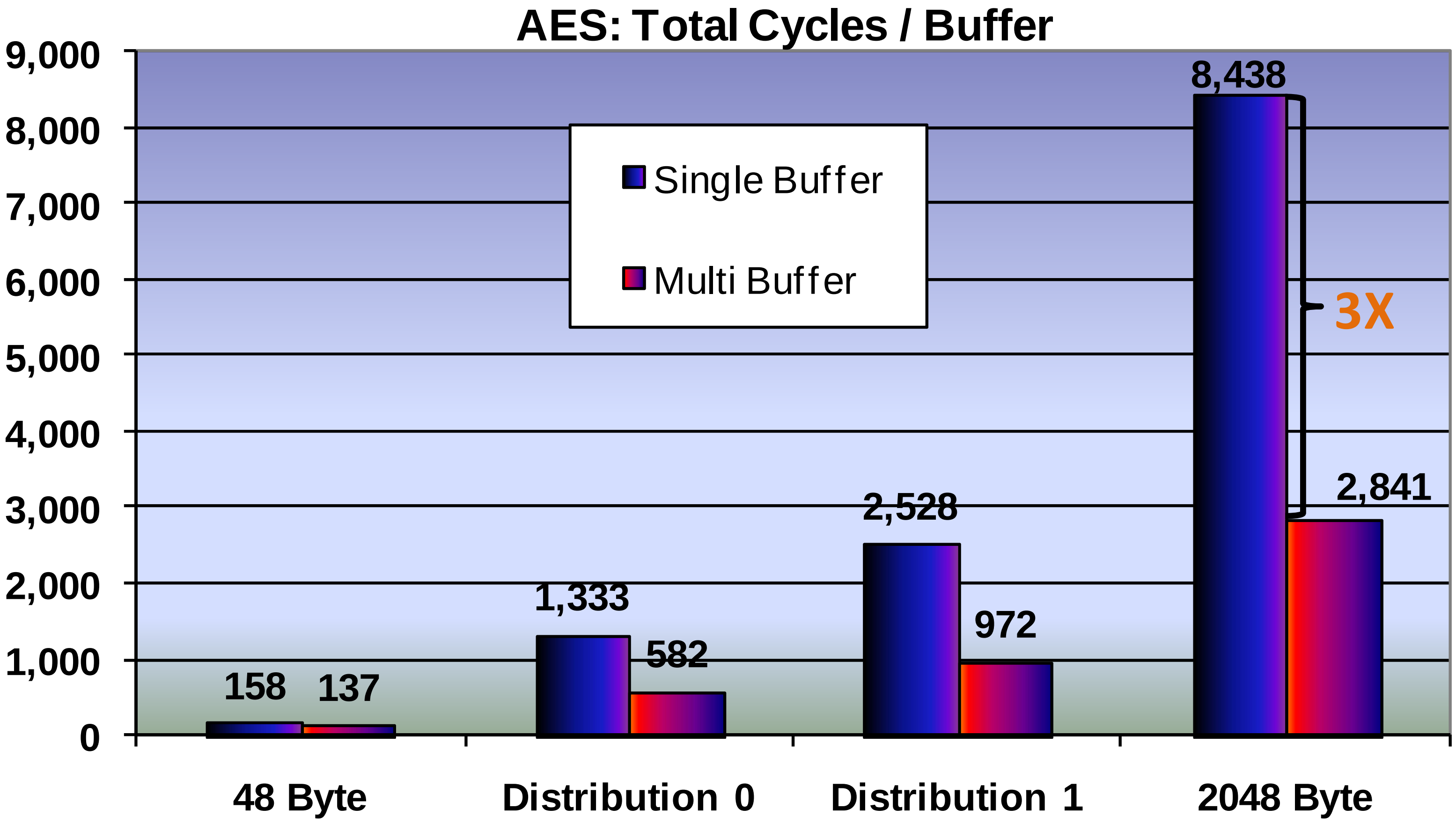
- Platform approach for software side channels
  - AES-NI: CPU instructions for a round of AES
  - PCLMULQDQ: CPU instructions for GF(2) Multiplication
  - Recommend side channel mitigated implementations of other crypto algorithms
    - No secret key or data dependent
      - memory access (at coarser than cache line granularity)
      - code branching
    - Ex: RSA implemented with <6% performance reduction in OpenSSL

Crypto Performance

- Software improvements
  - Multi-buffer
  - Function Stitching
- Hardware improvements
  - AES-NI
  - PCLMULQDQ
  - Microarchitecture improvements

Multi Buffer Performance – 1 WSM Core

Multi-buffer: Perform the same function on multiple independent data buffers

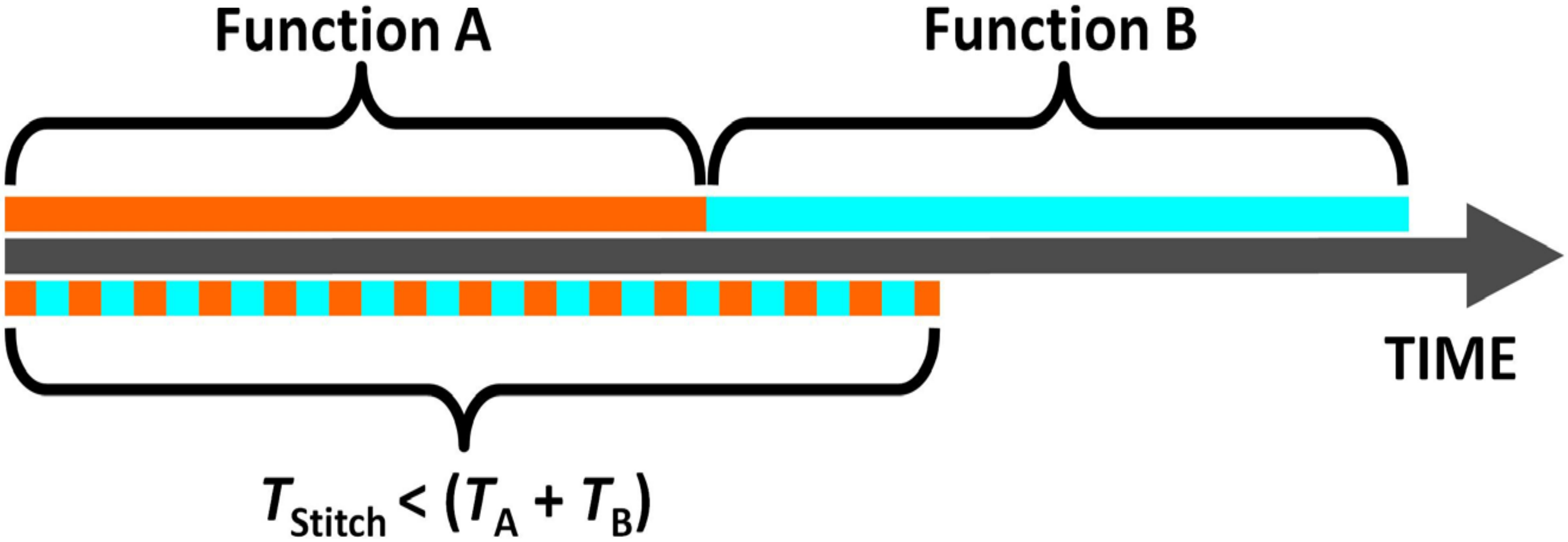


Excellent performance on AES CBC Encrypt

** See Intel technical papers for full description of methodology and results.*

Function Stitching

- Protocols such as SSL/TLS and IPsec apply two functions, confidentiality and integrity
- Improved performance by using multiple execution units more efficiently
- Fine grain integration achieves higher performance
- 1.4X Speedup on AES128 CBC-Encrypt with SHA1 (Cycles/Byte)



Method to speedup combined Encrypt/Authenticate

Sandy Bridge Performance

- SNB 2nd Generation Intel® Core™ improves:
  - AES-NI Throughput
  - SIMD Processing via AVX ISA extensions
  - Large-integer processing (public-key crypto)
- Multi Buffer Performance (Cycles/byte)

Algorithm	i5-650	i7-2600	i7-2600 Gain
MD5	1.46	**1.27**	**1.15**
SHA1	2.96	**2.2**	**1.35**
SHA256	6.96	**5.27**	**1.32**
AES128-CBC-Encrypt	1.52	**0.83**	**1.83**

- Modular Exponentiation Performance (Cycles)

Algorithm	i5-650	i7-2600	i7-2600 Gain
512-bit Modular Exponentiation	360,880	**246,899**	**1.46**
1024-bit Modular Exponentiation	2,722,590	**1,906,555**	**1.43**

1.2-1.8X additional performance gain on SNB!

Summary of reduction in trust boundary by virtualization and measured launch

Component in Trust Boundary	Mitigation with virtualization and measured launch
OS with kernel additions	Use VT-x and Require fewer kernel additions and device drivers in some VMs
Devices that can DMA	Restrict DMA to a single VM through VT-d
Apps installed by user	Restrict apps in protected VM, and sandbox suspect code
Virtualization layer underneath the OS	Allow only acceptable VMMs to launch using TXT launch control policy
BIOS, including SMM	Remove some or all of the BIOS from trust boundary using TXT and/or STM capability
Option ROMS	Remove Option ROMS from trust boundary using TXT

Intel Security & Trust Pillars

Identity Protection & Fraud Deterrence

Detection & Prevention of Malware

Securing Data and Assets

Recovery and Enhanced Patching

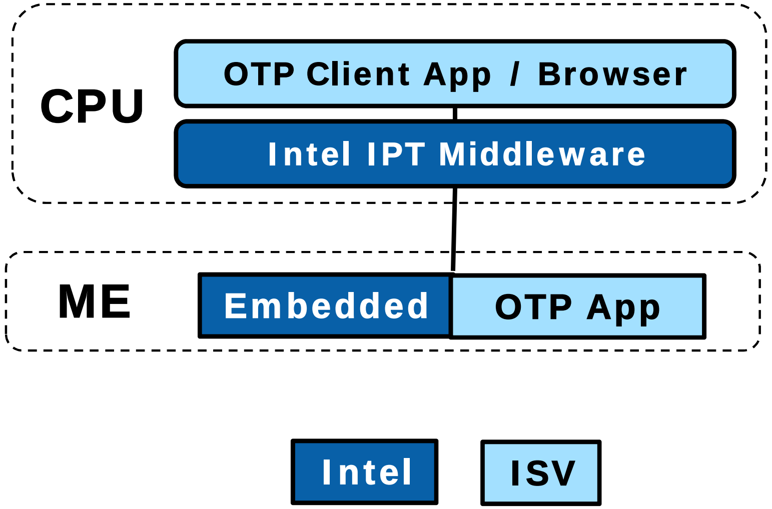
IPT 1.0: One Time Password (OTP)

The first generation of Intel® IPT is a dynamic code generated on 2nd generation Intel® Core™ processor-based PCs that is protected from malware in the OS.

- Single use, (i.e. 30 second, time-limited code → OTP)
- A hardware level 2nd factor of authentication
- Works with leading OTP Solutions from Symantec & Vasco

Traditional hardware token

Now embedded into your PC



No system can provide absolute security under all conditions. Requires an Intel IPT enabled system, including a 2nd generation Intel Core processor, enabled chipset, firmware and software. Available only on participating websites. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit [http://ipt.intel.com].

Intel Security & Trust Pillars

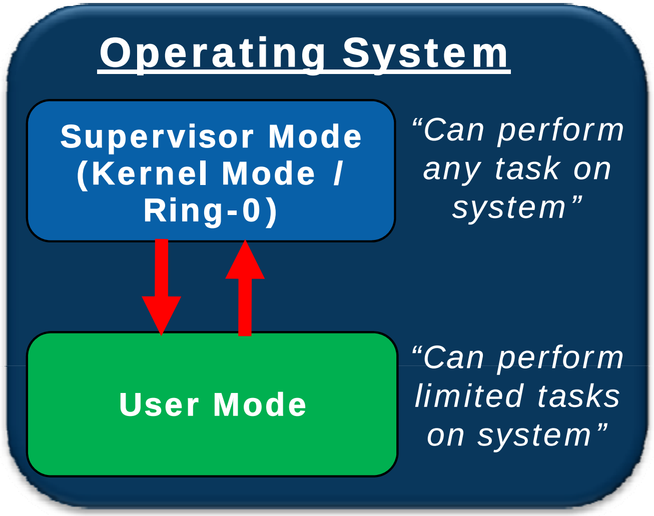
Identity Protection & Fraud Deterrence

Detection & Prevention of Malware

Securing Data and Assets

Recovery and Enhanced Patching

Supervisor Mode Execution Protection (SMEP)



Operating System

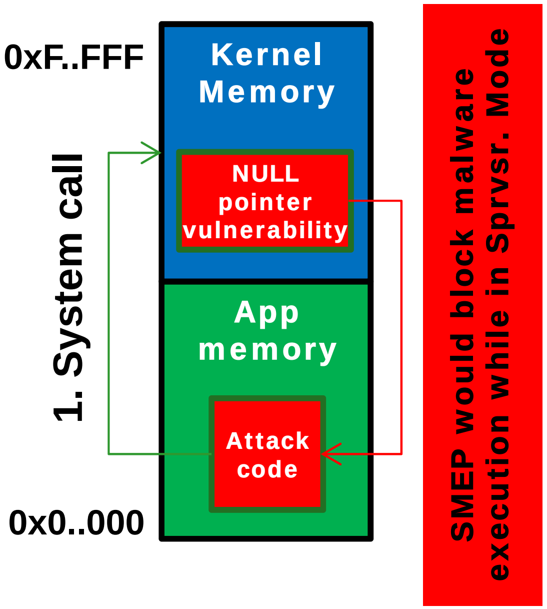
Supervisor Mode (Kernel Mode / Ring-0)

"Can perform any task on system"

User Mode

"Can perform limited tasks on system"

How does SMEP work?



0xF..FFF

Kernel Memory

NULL pointer vulnerability

App memory

Attack code

0x0..000

1. System call

SMEP would block malware execution while in Sprvsr. Mode

- **Prevents attacks when executing user-mode code in ring-0**
  - Extends Intel eXecute Disable capability

- **Available on Intel CPUs starting 2012**

- **Example where SMEP benefits: 'Stuxnet' worm**
  - SMEP would have prevented one method of attack by 'Stuxnet' –> Escalation of Privilege attack

SMEP can prevent malware exploiting EoP vulnerabilities from executing

McAfee DeepSAFE

- Technology platform co-developed with Intel
  - Not a product, the foundation for new solutions
- Hardware-assisted, security-focused, system monitor
- Sits below the OS to provide a new vantage point for security
- Solutions to be announced soon.
- Announcement from McAfee: http://www.mcafee.com/us/solutions/mcafee-deepsafe.aspx

Intel Security & Trust Pillars

Identity Protection & Fraud Deterrence

Detection & Prevention of Malware

Securing Data and Assets

Recovery and Enhanced Patching

Recommend BIOS Hygiene

- NIST SP800-147 – BIOS protection Guidelines
  - Use digital signatures to verify the authenticity of BIOS updates.
  - BIOS updates verified using a Root of Trust for Update which includes:
    - The key store used to verify signatures on updates.
    - The digital signature verification algorithm.
  - Use of NIST-approved crypto algorithms.
  - Recommend rollback protection.
  - http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf
- Minimize TCB for system boot

Intel Security & Trust Pillars

Identity Protection & Fraud Deterrence

Detection & Prevention of Malware

Securing Data and Assets

Recovery and Enhanced Patching

Stay tuned for future improvements in all pillars

Feedback

- What else should Intel be doing?
- Are we on the right track?

Technical Papers - 1

Breakthrough AES performance with Intel AES New Instructions
http://software.intel.com/file/26898

Processing Multiple buffers in parallel
http://download.intel.com/design/intarch/papers/324101.pdf

Fast Cryptographic computation on IA processors via Function Stitching
http://download.intel.com/design/intarch/PAPERS/323686.pdf

Fast and Constant-time Implementation of Modular Exponentiation
http://www.cse.buffalo.edu/srds2009/escs2009_submission_Gopal.pdf

Fast CRC Computation for iSCSI Polynomial using CRC32 Instruction
http://download.intel.com/design/intarch/papers/323405.pdf

Optimized Galois-Counter-Mode Implementation on IA Processors
http://download.intel.com/design/intarch/PAPERS/324194.pdf

High Performance Storage Encryption on Intel® Architecture Processors

http://download.intel.com/design/intarch/PAPERS/324310.pdf

Technical Papers - 2

Fast CRC Computation for Generic Polynomials using PCLMULQDQ Instruction http://download.intel.com/design/intarch/papers/323102.pdf

High Performance DEFLATE Decompression on Intel® Architecture Processors http://edc.intel.com/Link.aspx?id=3972

Cryptographic Performance on the 2nd Generation Intel Core Processor http://download.intel.com/design/intarch/PAPERS/324952.pdf

Fast Parallel CRC Computation using the Nehalem CRC32 instruction http://drdobbs.com/cpp/229401411

Using Intel® AES New Instructions and PCLMULQDQ to Significantly Improve IPSec Performance on Linux http://download.intel.com/design/intarch/papers/324238.pdf

IDF 2010 Presentation with Voice: Examining the Performance of Intel AES New Instructions on Intel Core i7 Processor http://intelstudios.edgesuite.net/idf/2010/sf/aep/SFTS012/SFTS012.html intel®