Intel® SGX Technology:

Trusted Execution Environment for DRMs, CA Systems, and other applications.

June 2015

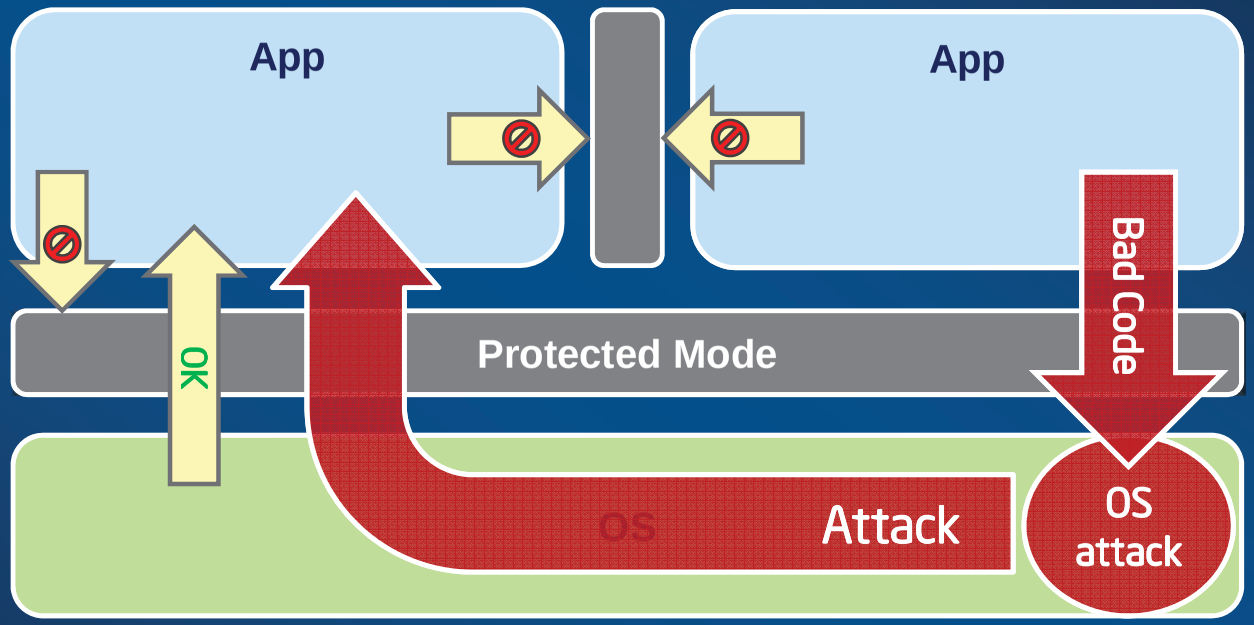
Intel® Software Guard Extensions (SGX)

- A CPU feature for upcoming Intel processors
- Provides "Enclaves," where apps can protect critical code and data
- Allows any app to keep a secret, within a standard OS environment
  - No dependency on OS (or underlying SW) correctness or configuration
  - Developers use standard and familiar development tools
  - Execution utilizing full power of main Intel CPU
- Provides confidentiality and integrity
  - Protects against software attacks, incl. privileged malware, malicious BIOS, etc.
  - Protects against hardware attacks such as bus analyzers or cold-boot
- Includes functionality to attest enclave state (incl. to a remote / 3rd party)
  - Enables secure provisioning of credentials to otherwise untrusted platforms
- "Hardware" level robust trusted execution environment

Build

Why Aren't Platforms Trustworthy?

Protected Mode (rings) protects OS from apps …



… and apps from each other …

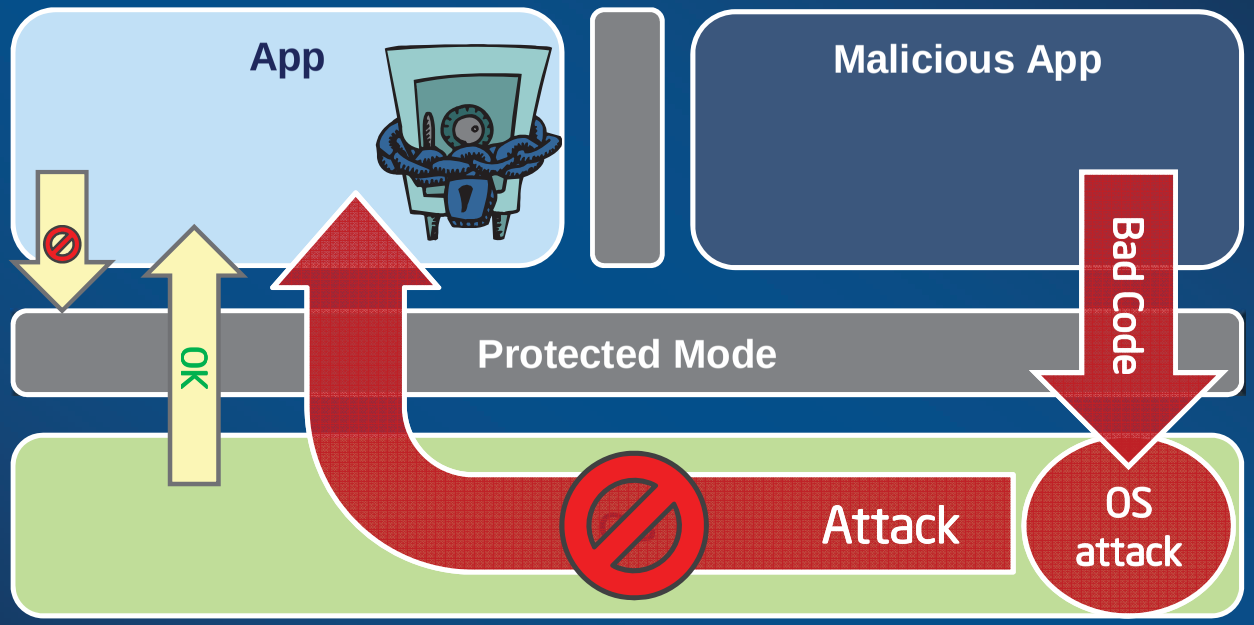
… UNTIL a malicious app exploits an OS flaw to gain full privileges and then tampers with the OS or other apps

Applications not protected from privileged code attacks

Build

Allowing App Developers to Secure Data

Intel® SGX provides a safe place for code and data in the application



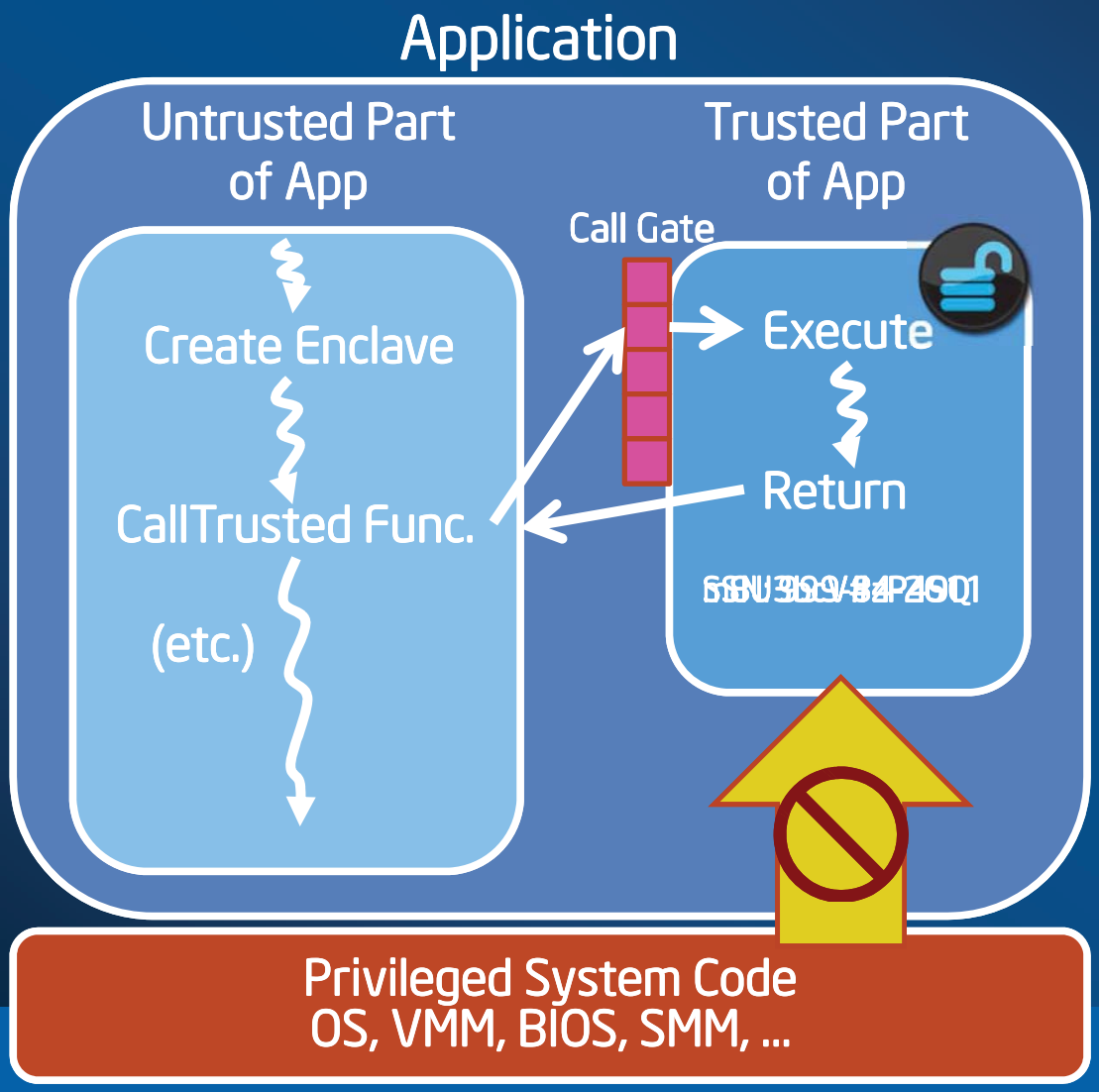
Undetected malicious software cannot access secrets

Secrets are protected from bad actors with platform access

Need a safe as well as guards

Build

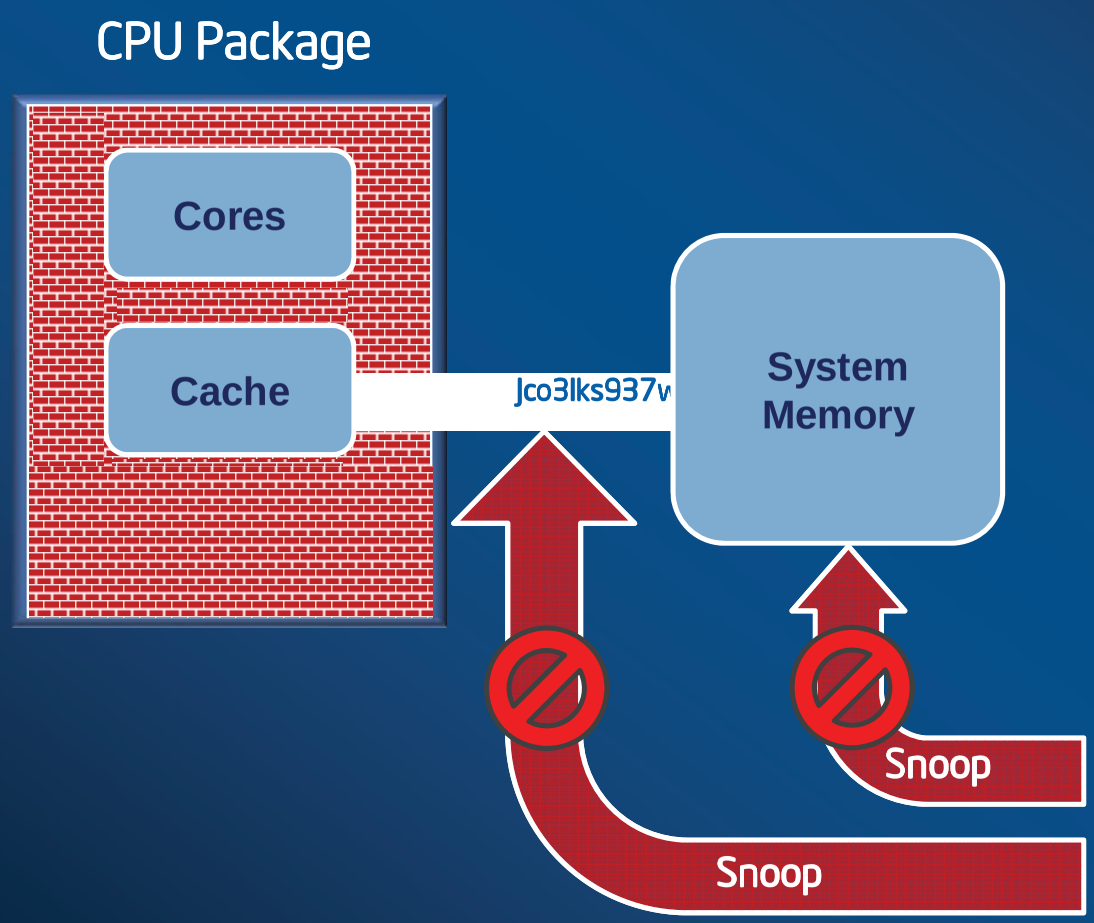
Protects Against Software Attack



1. App is built with trusted and untrusted parts
2. App runs & creates enclave which is placed in trusted memory
3. Trusted function is called; code running inside enclave sees data in clear; external access to data is denied
4. Function returns; enclave data remains in trusted memory

Build

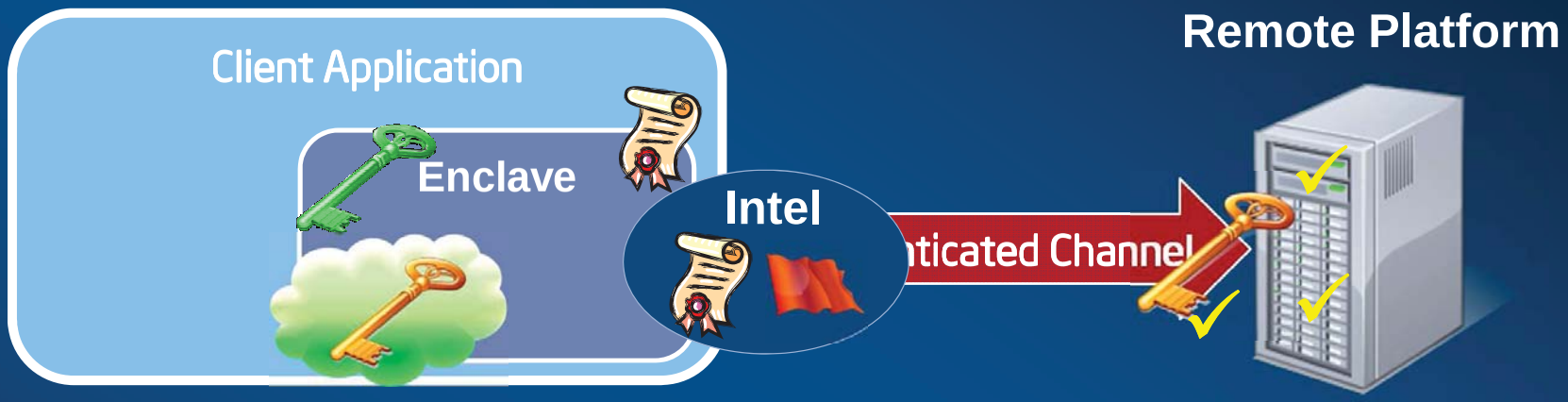
Protects Against Hardware Attack

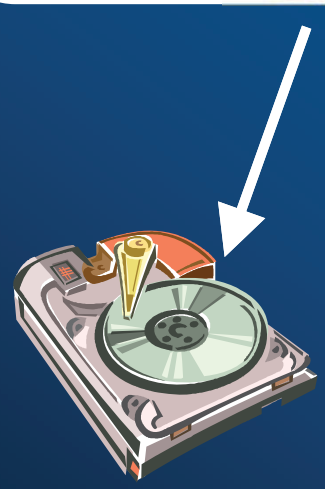


1. Security perimeter is the CPU package boundary
2. Data and code unencrypted inside CPU package
3. Data and code outside CPU package is encrypted and integrity checked
4. External memory reads and bus snoops see only encrypted data

Build

Critical Feature: Attestation and Sealing

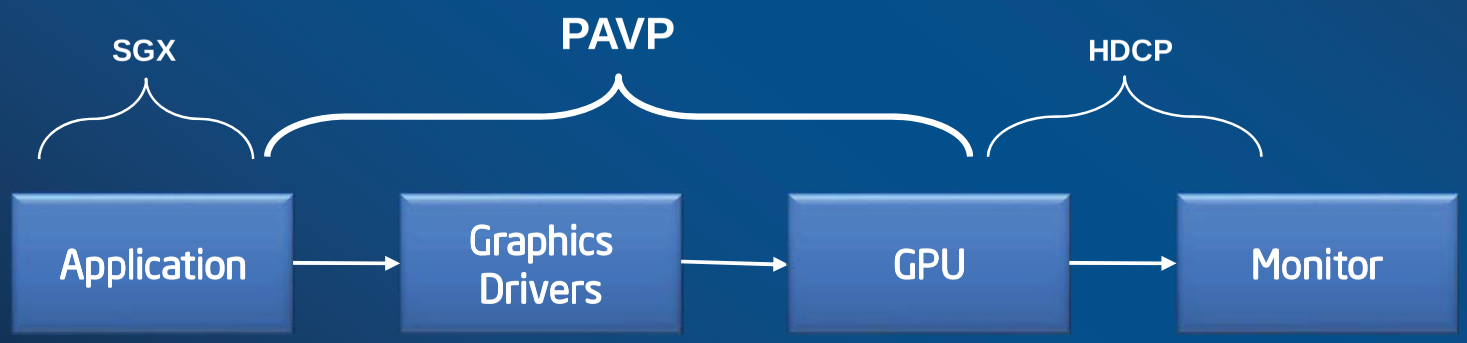




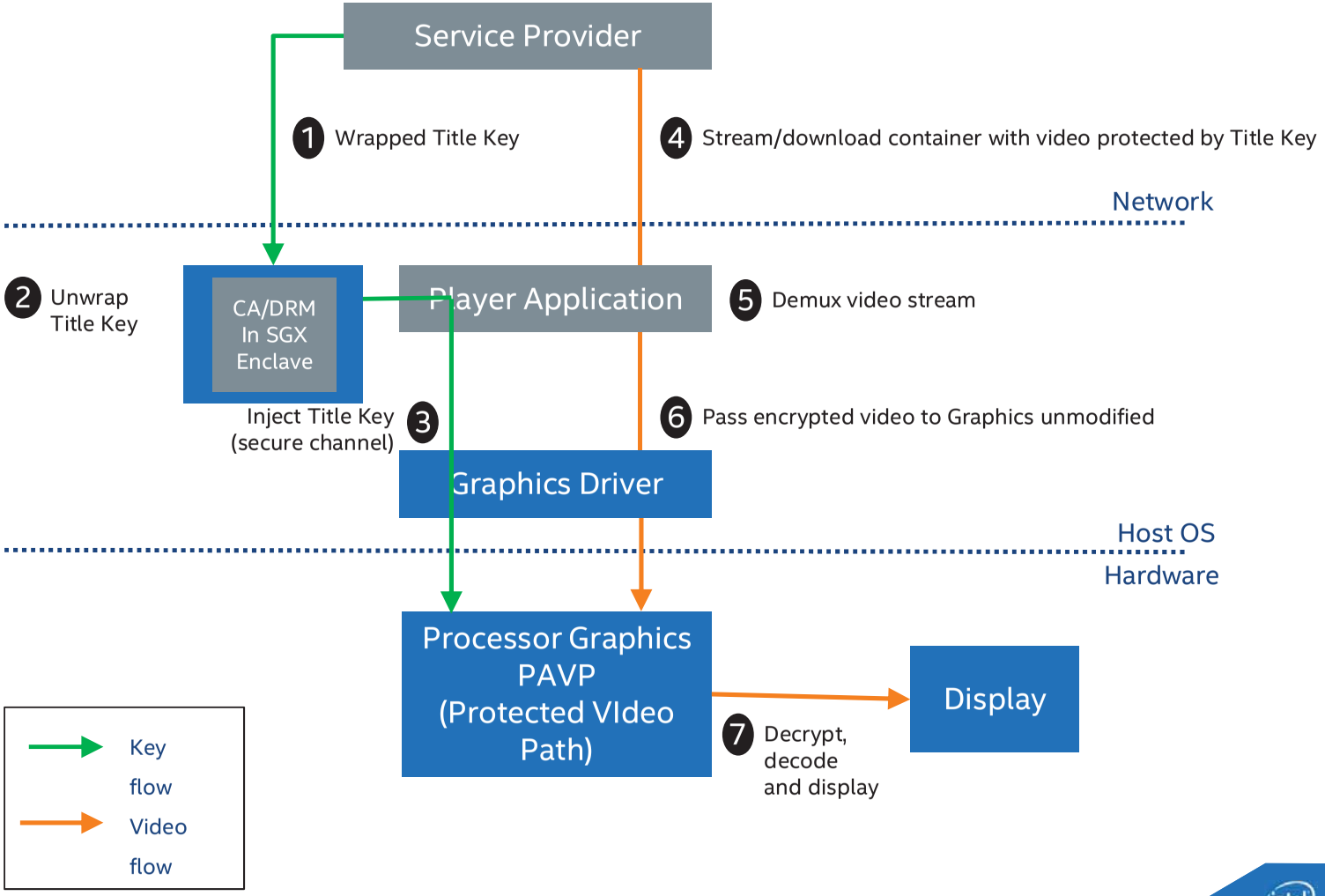
1. Enclave built & measured (initially no secrets)
2. Enclave requests REPORT (HW-signed blob that includes enclave identity information)
3. REPORT sent to server & verified
4. Application Key sent to enclave, first secret provisioned
5. Enclave-platform-specific Sealing Key generated
6. Application Key encrypted via Sealing Key & stored for later (offline) use

Protected Video Play back

- SGX use Intel® graphics for protected video playback
  - Secure key exchange
  - Video bitstream decryption
  - Memory protection



CA/DRM Example Block Diagram



SGX References

https://software.intel.com/en-us/isa-extensions/intel-sgx

- See the link above for published:
  - Overviews
  - White Papers
  - Detailed Programming reference

Legal Disclaimer

This document contains information on products in the design phase of development

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.
A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.
Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel.

Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice.

Copyright © Intel Corporation 2009, 2010, 2011, 2012, 2013, 2014. All rights reserved.