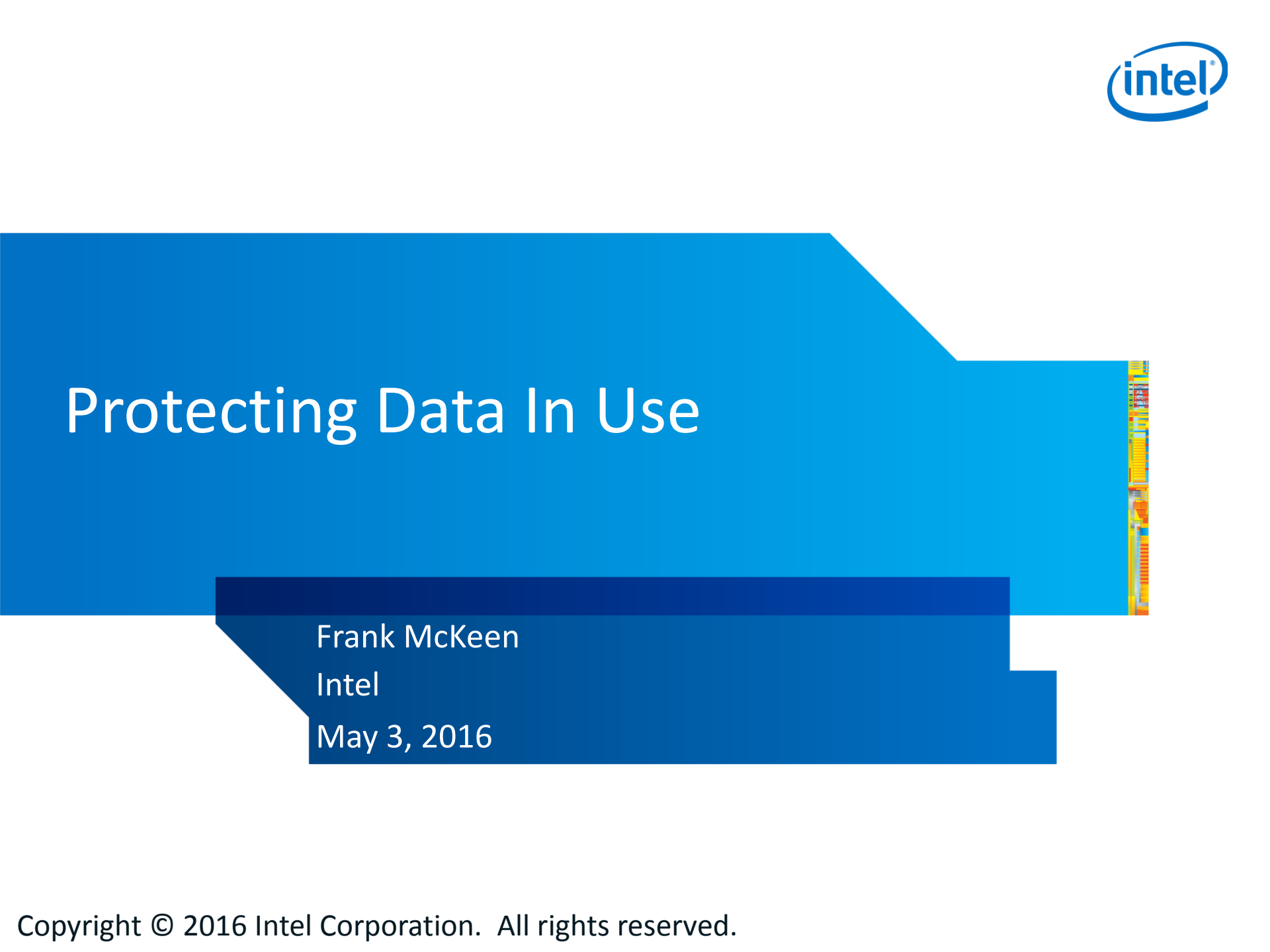


Protecting Data In Use

Frank McKeen
Intel
May 3, 2016

Legal Disclaimers

- The comments and statements are the presenter's and not necessarily Intel's

- Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com

- No computer system can be absolutely secure.

System Level Security Features

System Level Security Features

Trusted Channels

System Level Security Features

User
Authentication

System Level Security Features

Protected Storage

System Level Security Features

Biometrics

System Level Security Features

Trusted Cloud Orchestration

System Level Security Features

Anti-Malware Software and Detection

System Level Security Features

Firewalls

System Level Security Features

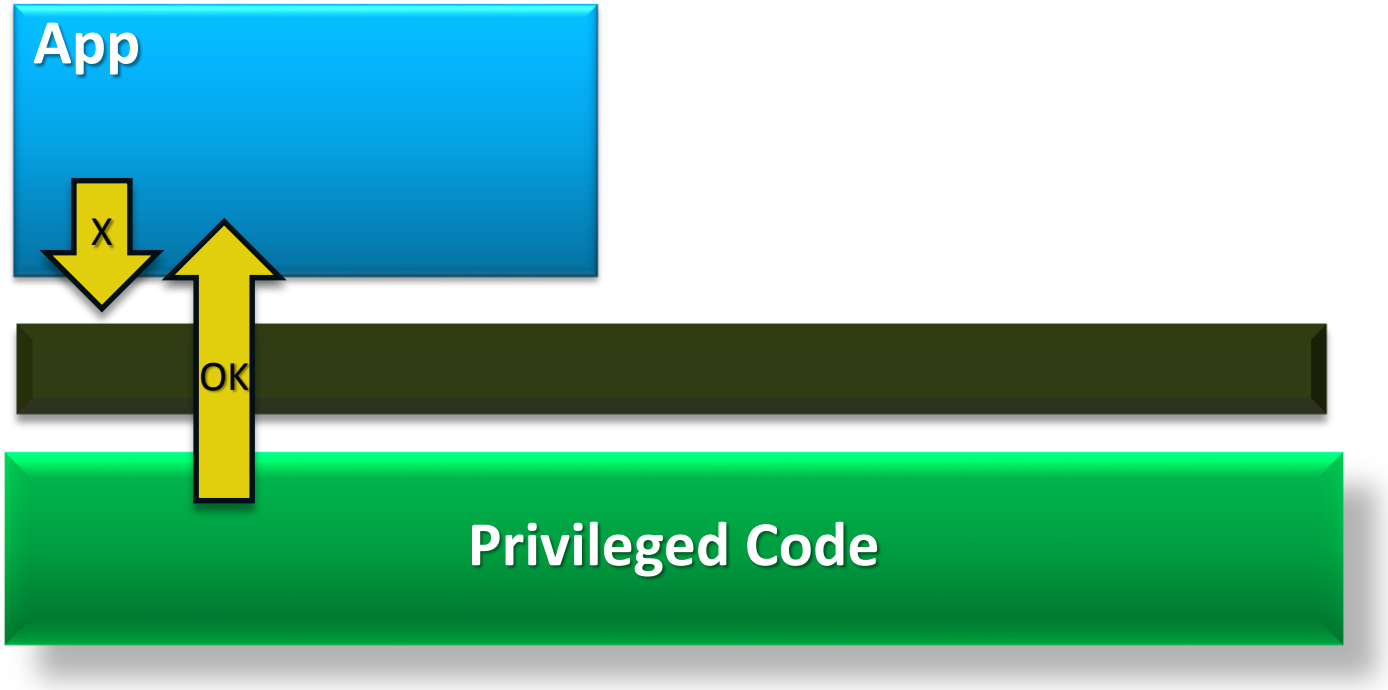
System Level Security Features

Architecture to Protect Application Secrets

Protecting Applications from Privileged Malware Attacks

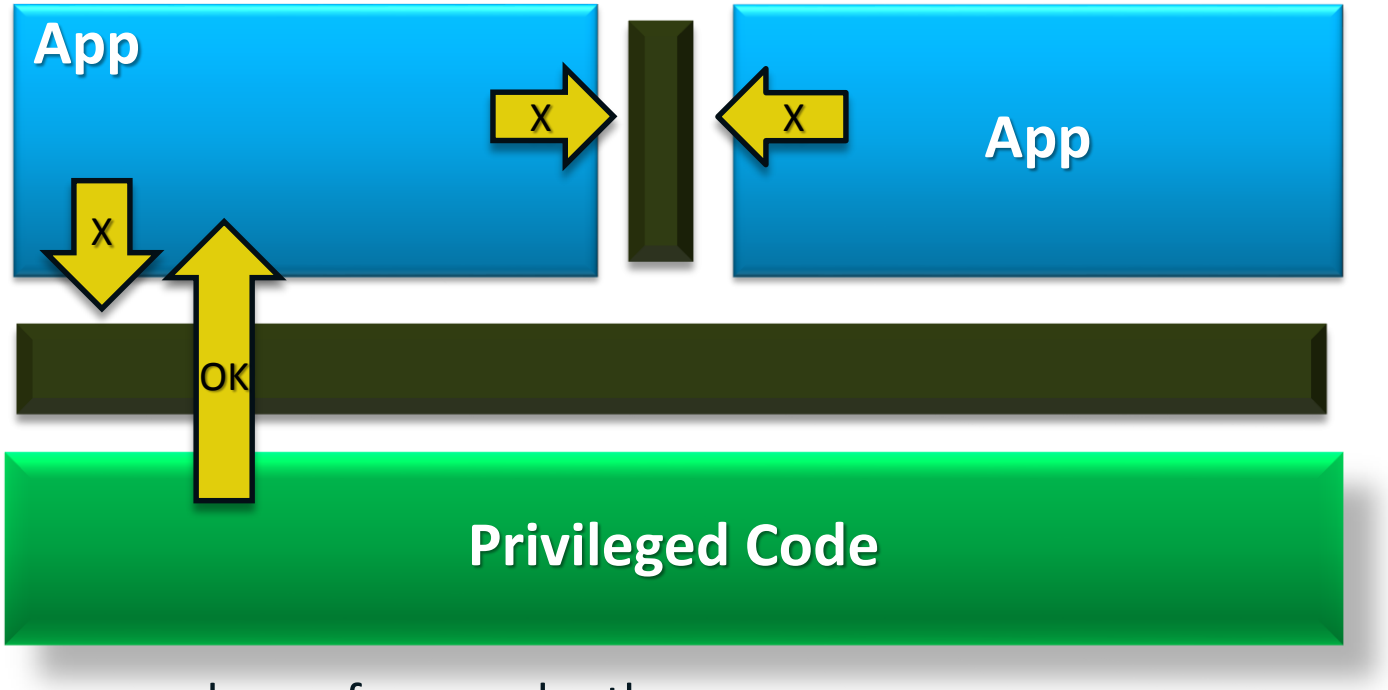
The Basic Issue: Vulnerabilities in Privileged Code

Protected Mode (rings) protects OS from apps …



The Basic Issue: Vulnerabilities in Privileged Code

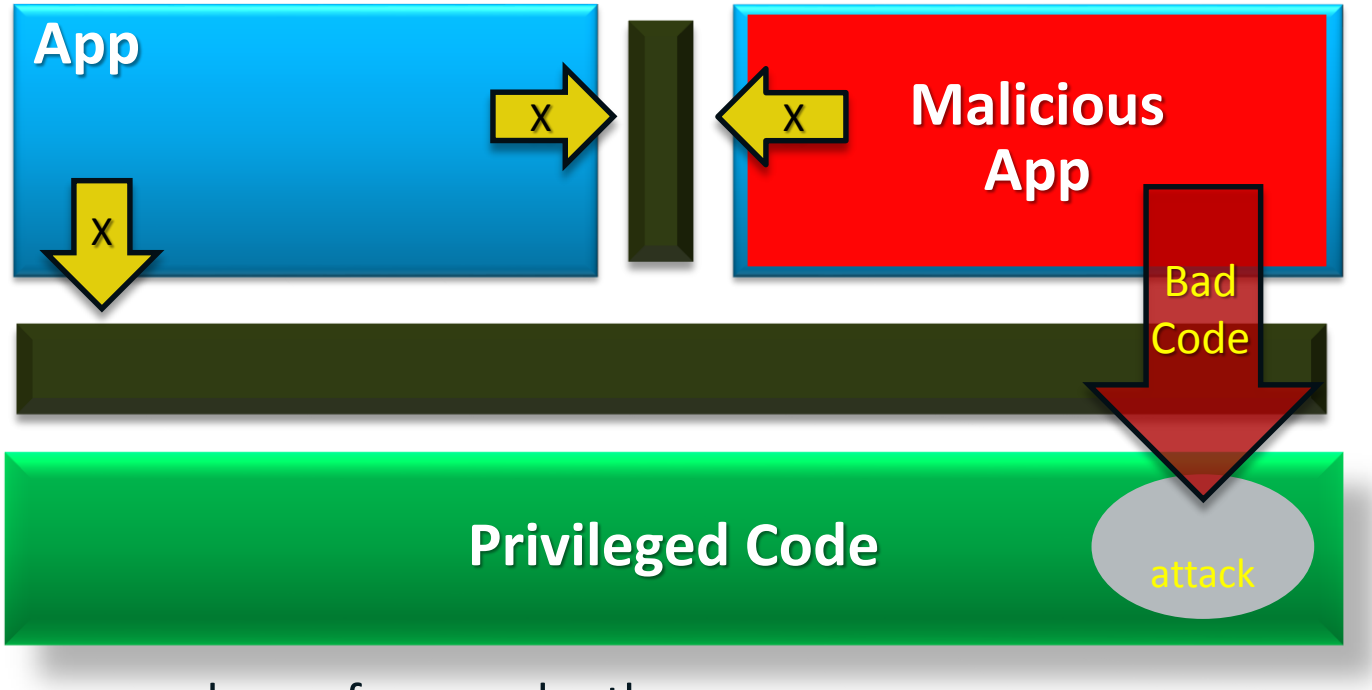
Protected Mode (rings) protects OS from apps …



… and apps from each other …

The Basic Issue: Vulnerabilities in Privileged Code

Protected Mode (rings) protects OS from apps …



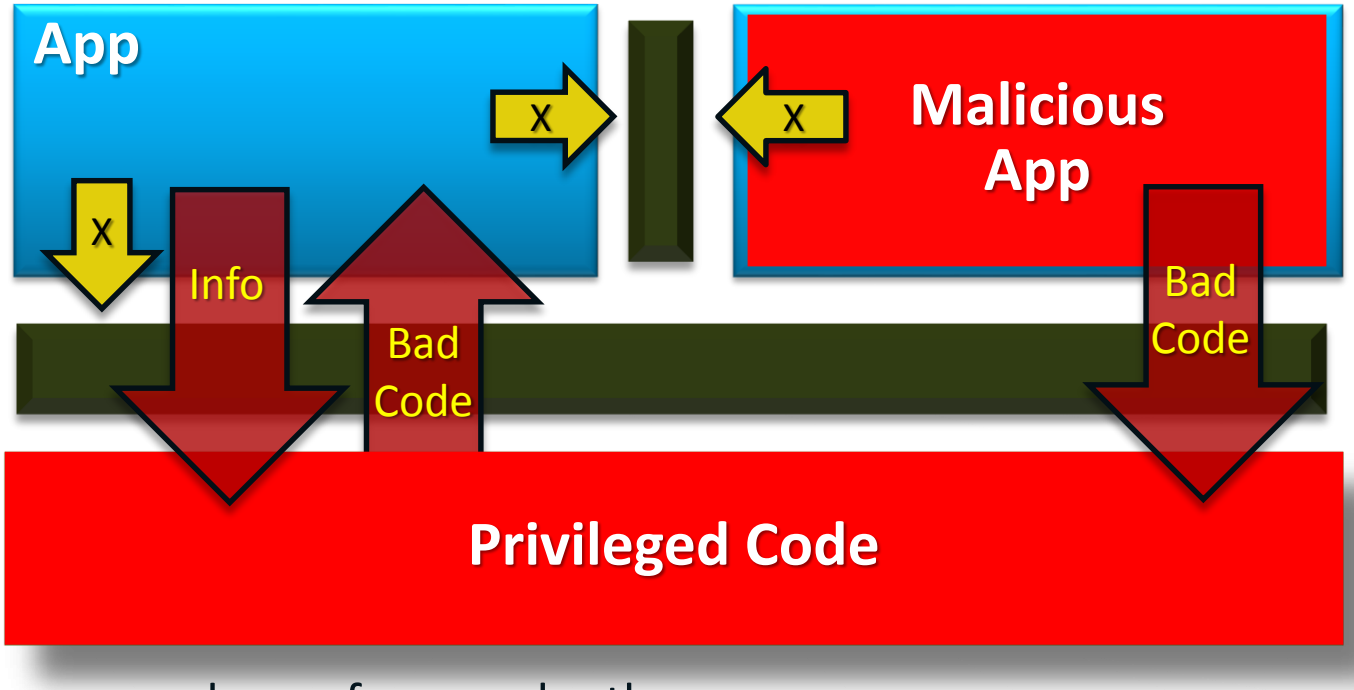
… and apps from each other …

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

Apps not protected from privileged code attacks

The Basic Issue: Vulnerabilities in Privileged Code

Protected Mode (rings) protects OS from apps …



… and apps from each other …

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

Apps not protected from privileged code attacks

A Place to Stand

A stable execution environment:

- Not susceptible to Privileged Software manipulation
- Provides confidentiality and integrity to data and code
- Can prove that it resides on protected hardware
- Can provide the details of hardware revision level
- Fits into the current eco-system

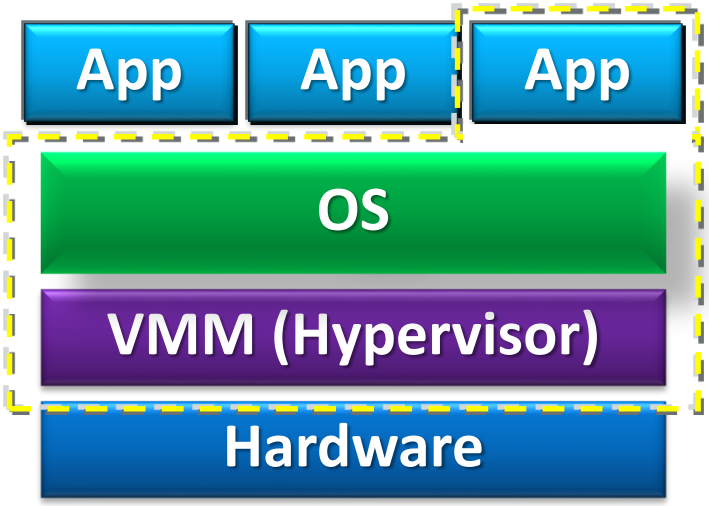
Desired Protections

Protection	Description
Protection from firmware attack	SMM, BIOS, Graphics card, etc
Protection from SW attacks	OS, VMM, Drivers, etc.
Operator Access	Operator can't access restricted data
Administrator Access	Admin can't access restricted data
Replay Attacks	Insert old data values in place of latest data value
Protection from translation changes	Privileged code should not be able to change address mappings
Understand platform type	Prove to external party what protection a platform offers
Correct entry and exit points	Only execute at allowed spots
Side Channels	External observers can't gleam data from timing, power, voltage, etc.

Intel® Software Guard Extensions (Intel® SGX): Principles of Operation

Reduced attack surface with Intel ® SGX

Attack surface today

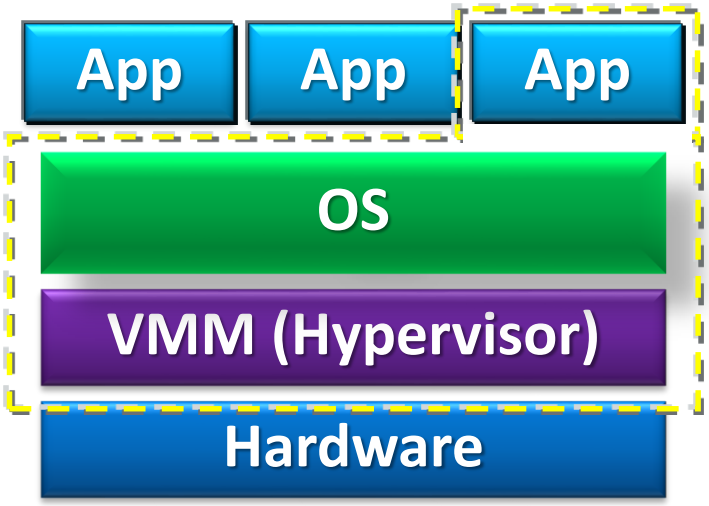


Attack Surface

Reduced attack surface with Intel ® SGX

Application gains ability to defend its own secrets

Attack surface today



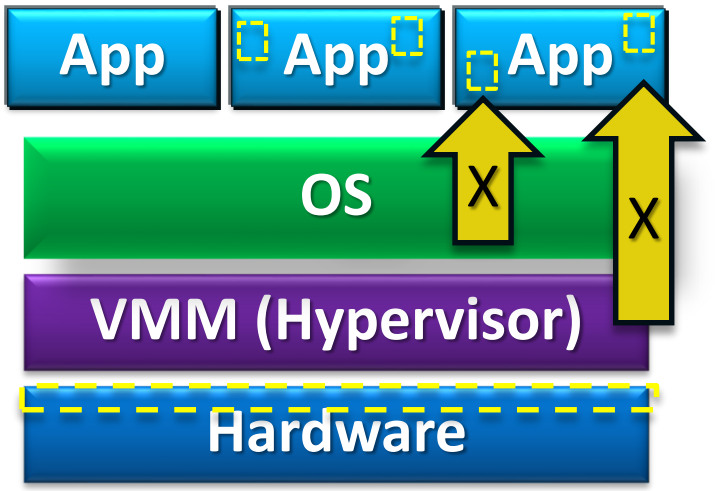
Attack Surface

Reduced attack surface with Intel ® SGX

Application gains ability to defend its own secrets

- Smallest attack surface (app + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

Attack surface with Enclaves



Attack Surface

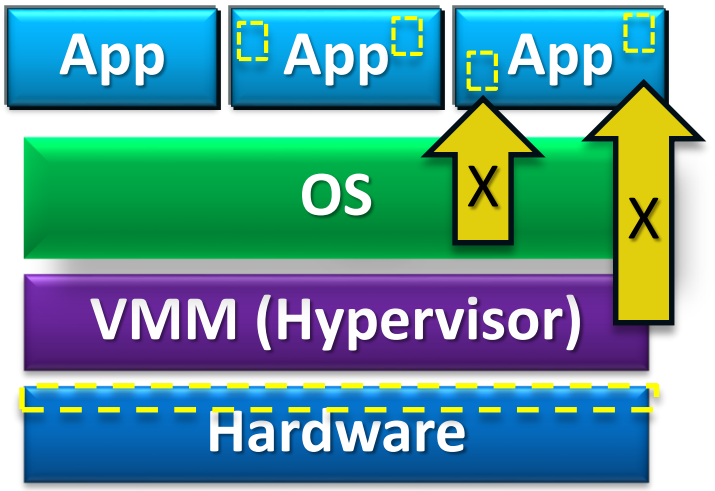
Reduced attack surface with Intel ® SGX

Application gains ability to defend its own secrets

- Smallest attack surface (app + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

Familiar development/debug

Attack surface with Enclaves



Attack Surface

Reduced attack surface with Intel ® SGX

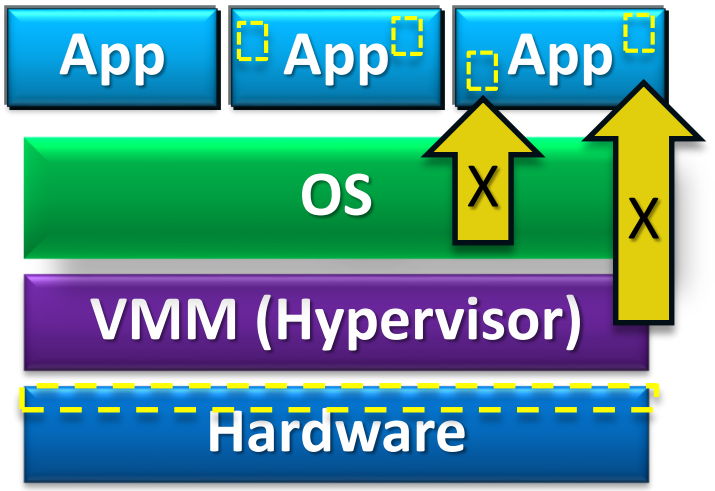
Application gains ability to defend its own secrets

- Smallest attack surface (app + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

Familiar development/debug

- Single application environment

Attack surface with Enclaves



Attack Surface

Reduced attack surface with Intel ® SGX

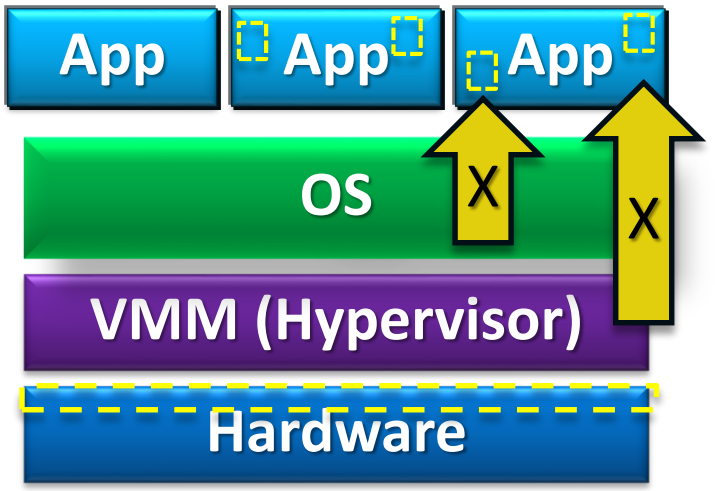
Application gains ability to defend its own secrets

- Smallest attack surface (app + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

Familiar development/debug

- Single application environment
- Build on existing ecosystem expertise

Attack surface with Enclaves



Attack Surface

Reduced attack surface with Intel ® SGX

Application gains ability to defend its own secrets

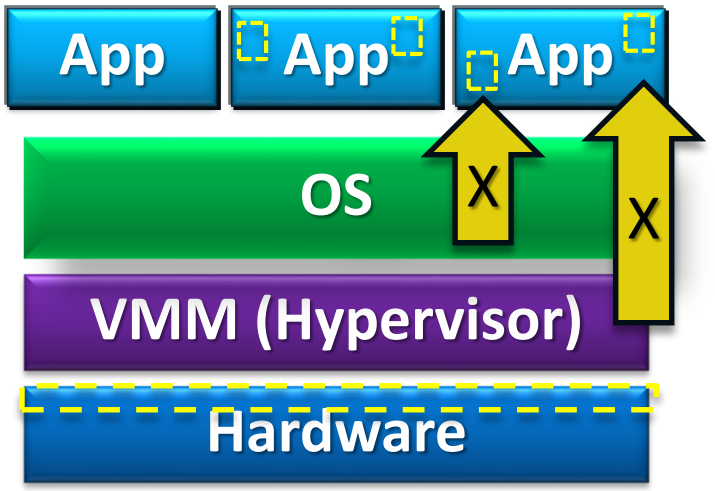
- Smallest attack surface (app + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

Familiar development/debug

- Single application environment
- Build on existing ecosystem expertise

Familiar deployment model

Attack surface with Enclaves



Attack Surface

Reduced attack surface with Intel ® SGX

Application gains ability to defend its own secrets

- Smallest attack surface (app + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

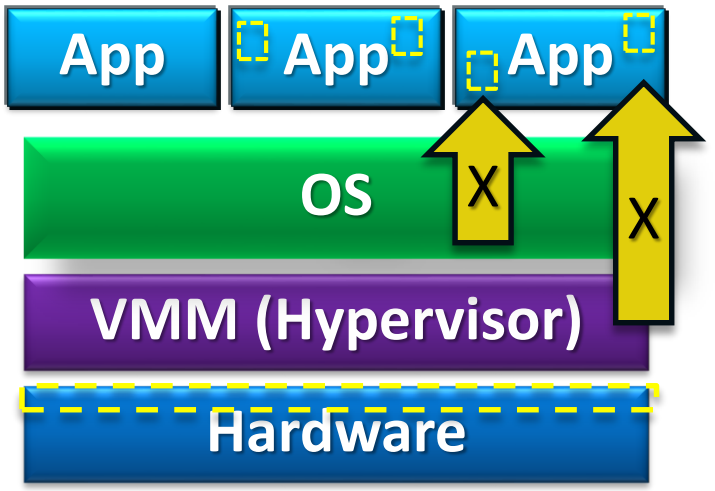
Familiar development/debug

- Single application environment
- Build on existing ecosystem expertise

Familiar deployment model

- Platform integration not a bottleneck to deployment of trusted apps

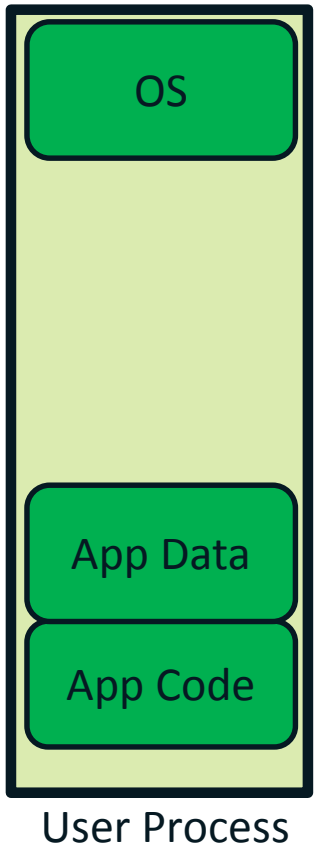
Attack surface with Enclaves



Attack Surface

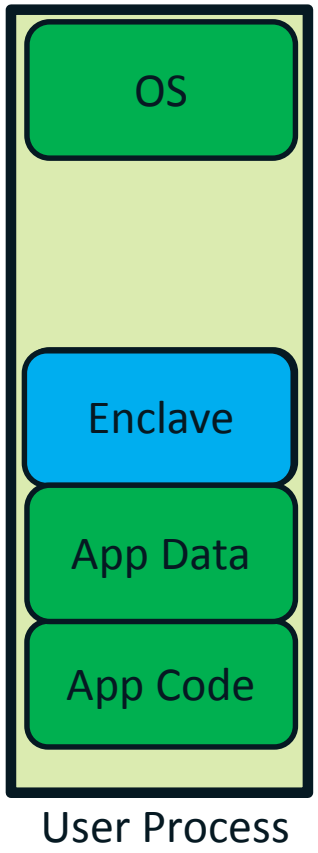
Scalable security within mainstream environment

What is an Enclave?



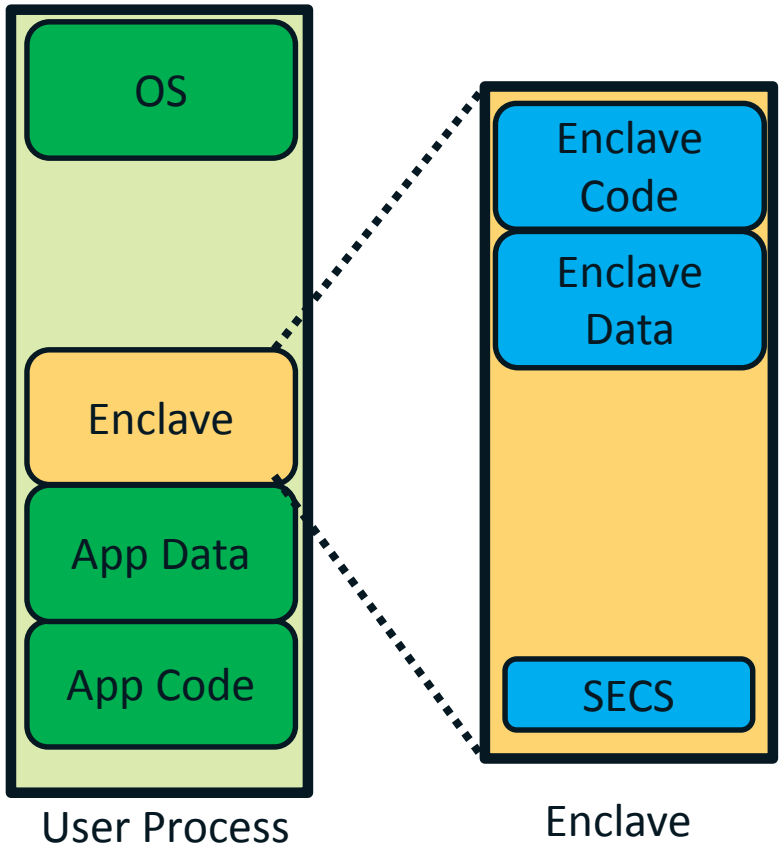
What is an Enclave?

Enclave: trusted execution environment embedded in a process



What is an Enclave?

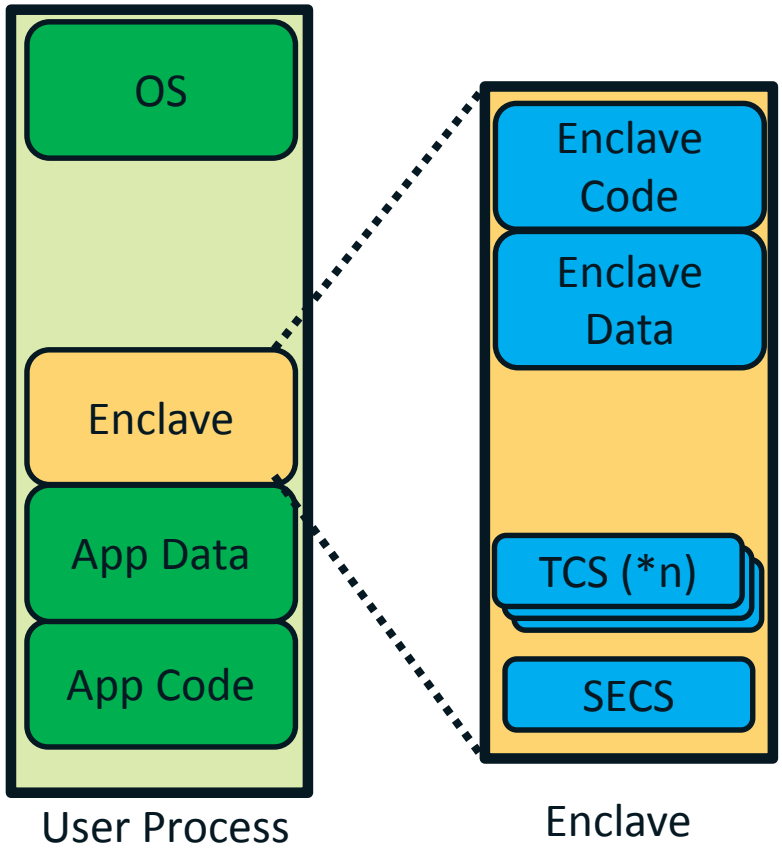
Enclave: trusted execution environment embedded in a process



- Own code and data
- Provides Confidentiality
- Provides integrity
- Controlled entry points

What is an Enclave?

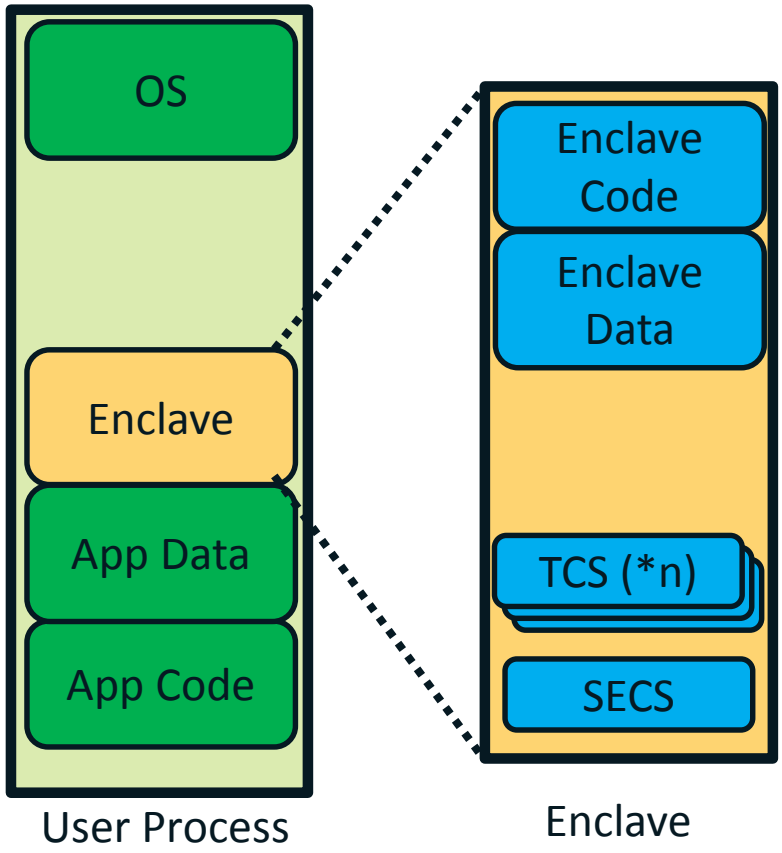
Enclave: trusted execution environment embedded in a process



- Own code and data
- Provides Confidentiality
- Provides integrity
- Controlled entry points
- Supporting multiple threads

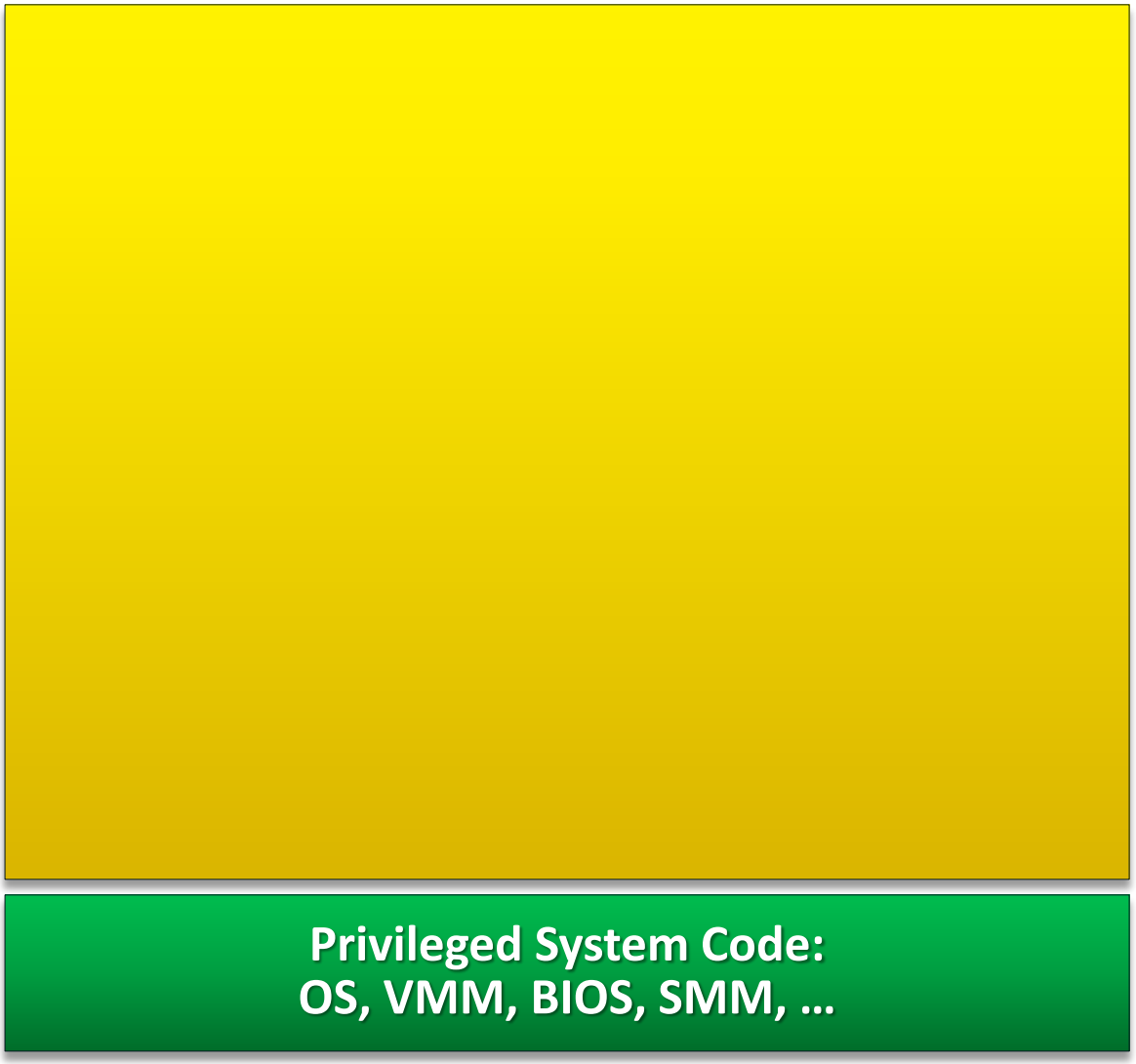
What is an Enclave?

Enclave: trusted execution environment embedded in a process

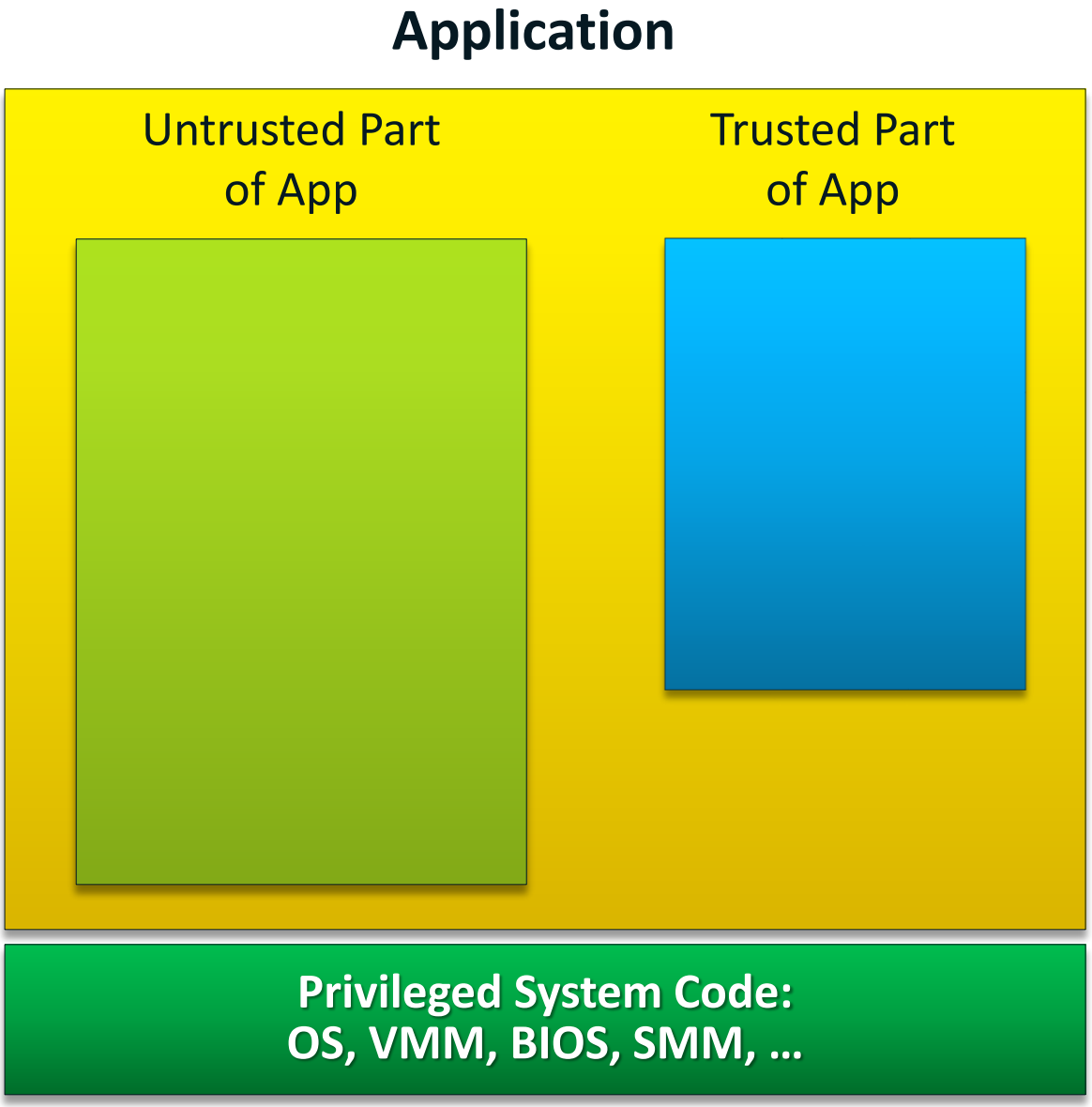


- Own code and data
- Provides Confidentiality
- Provides integrity
- Controlled entry points
- Supporting multiple threads
- Full access to app memory

How Intel ® SGX Works: Protection vs. Software Attack

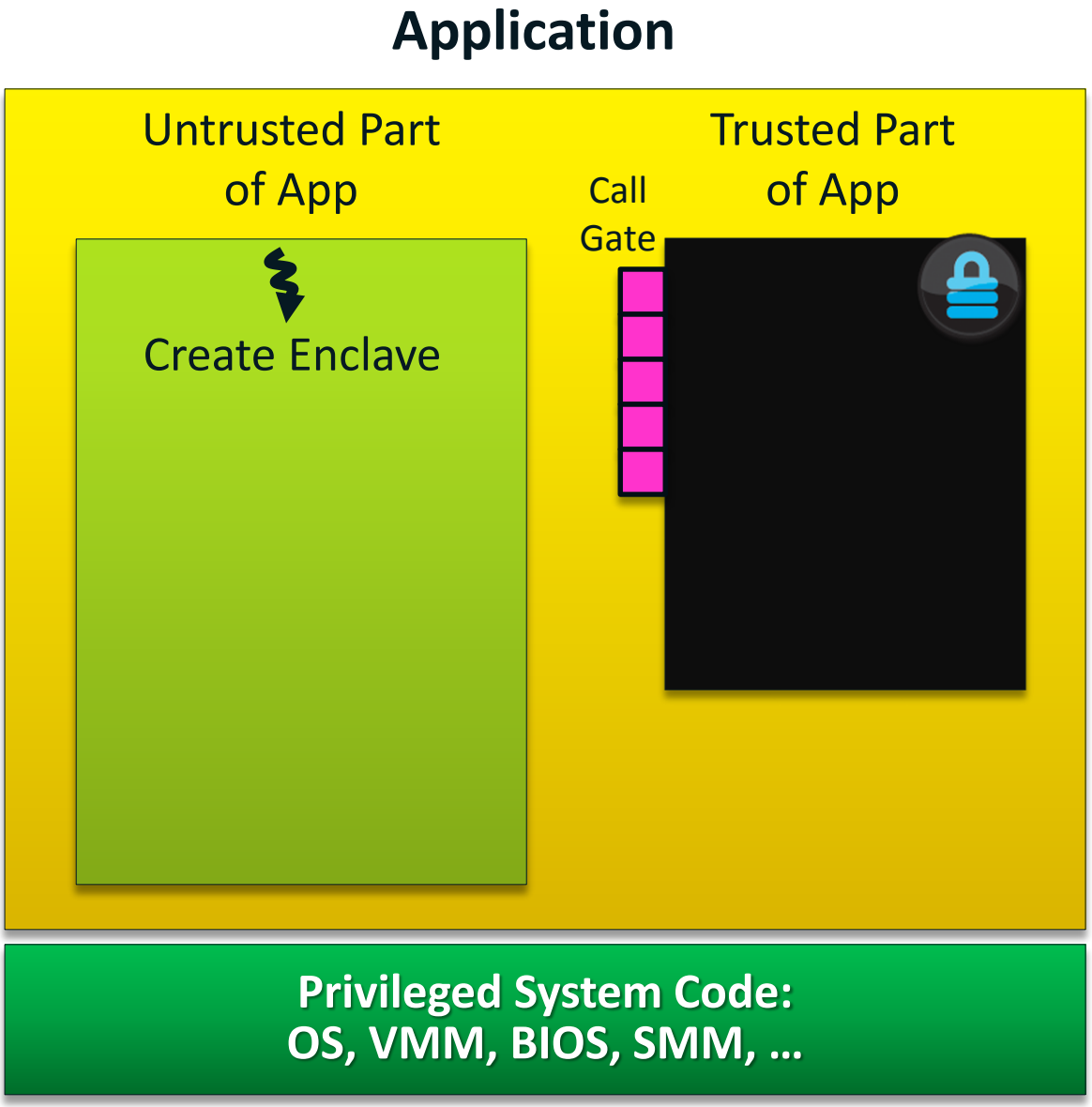


How Intel ® SGX Works: Protection vs. Software Attack



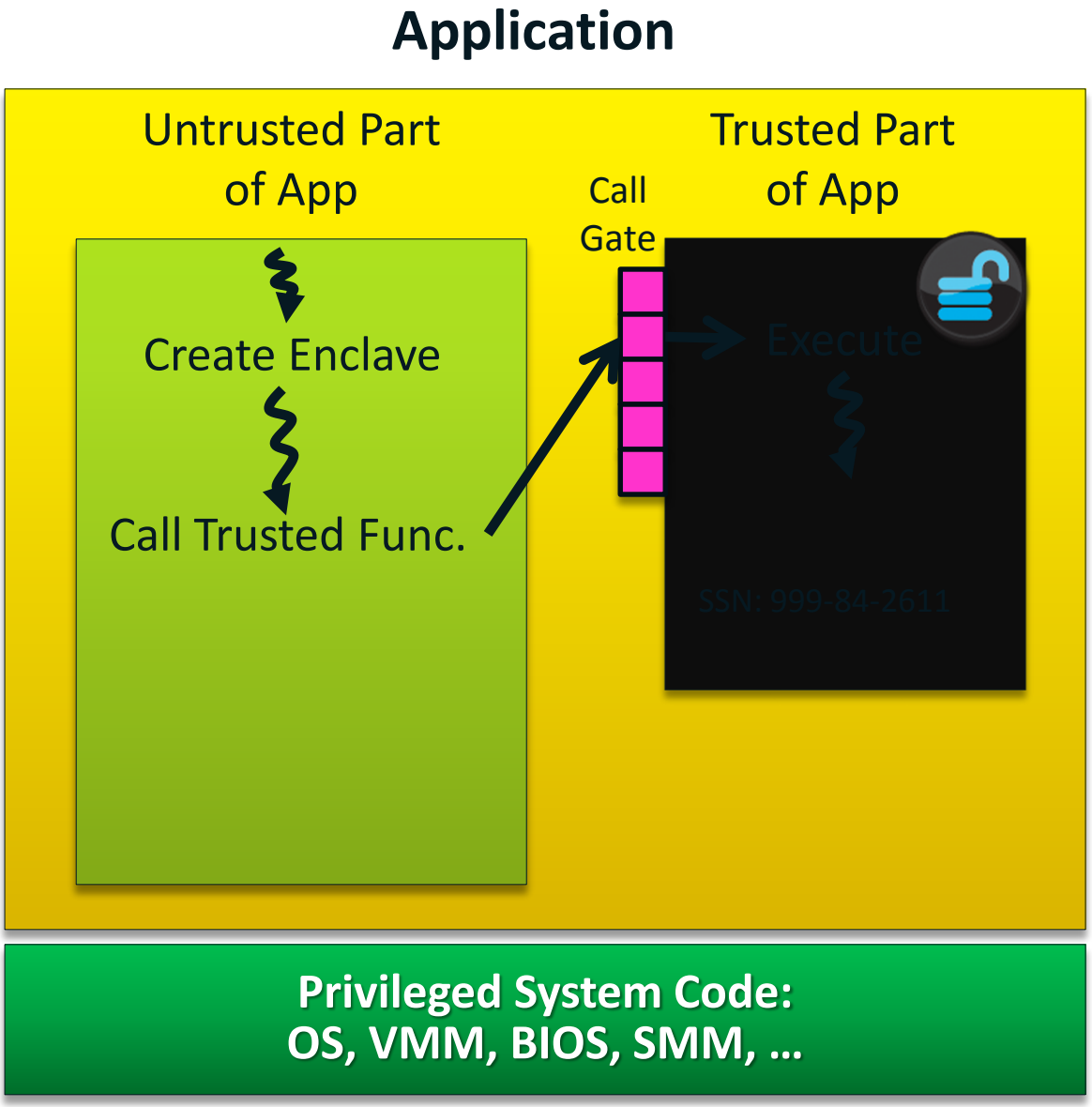
1. App is built with trusted and untrusted parts

How Intel ® SGX Works: Protection vs. Software Attack



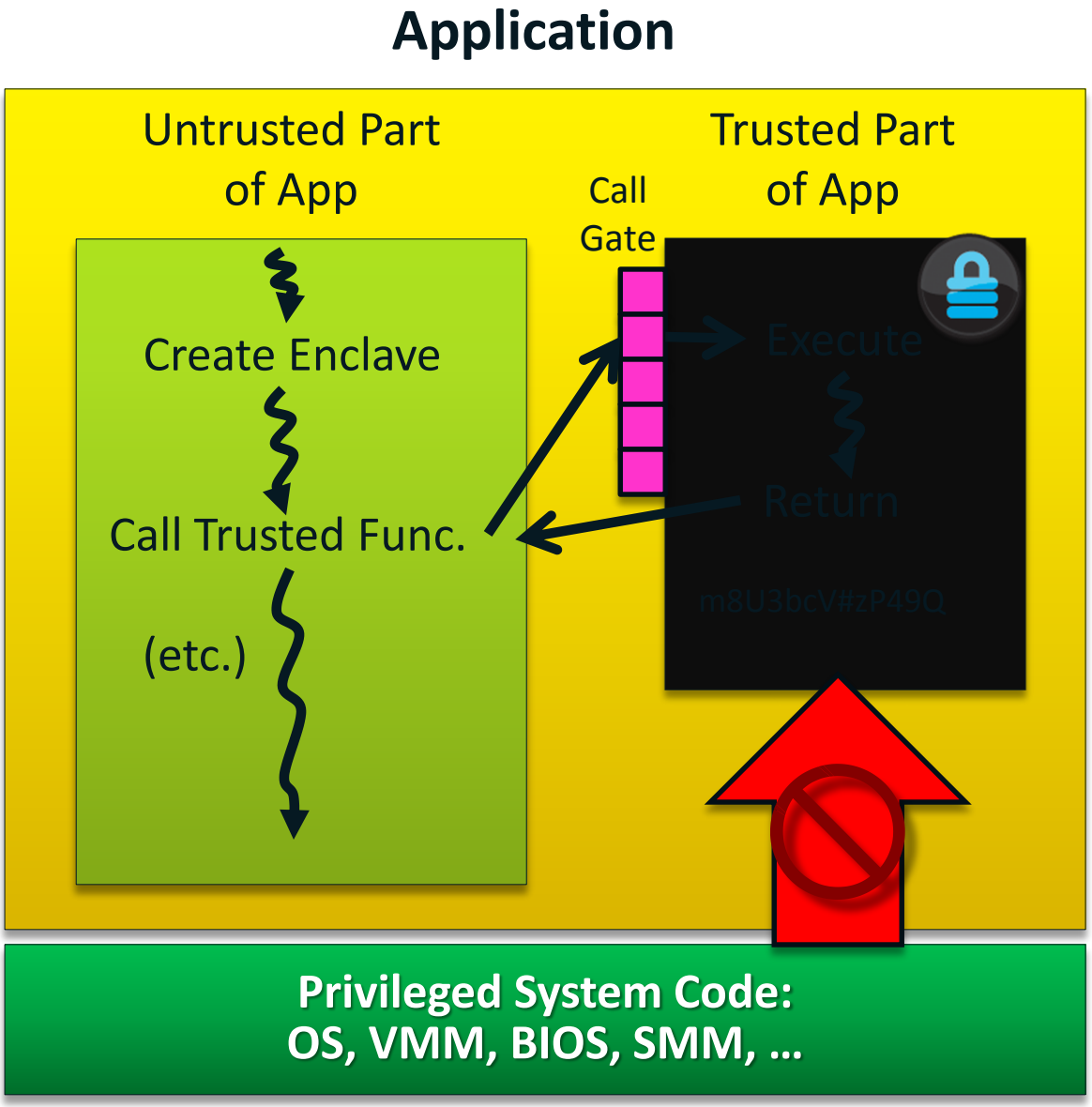
1. App is built with trusted and untrusted parts
2. App runs & creates enclave which is placed in trusted memory

How Intel ® SGX Works: Protection vs. 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

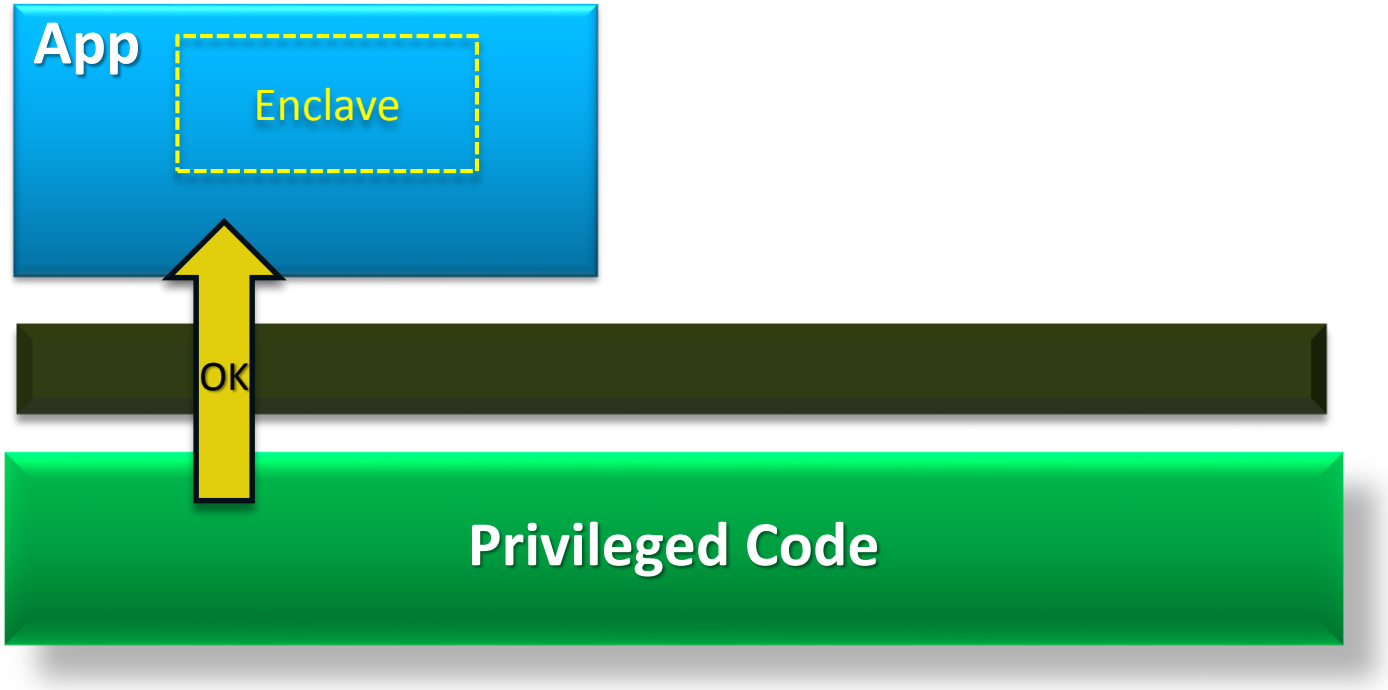
How Intel ® SGX Works: Protection vs. Software Attack



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

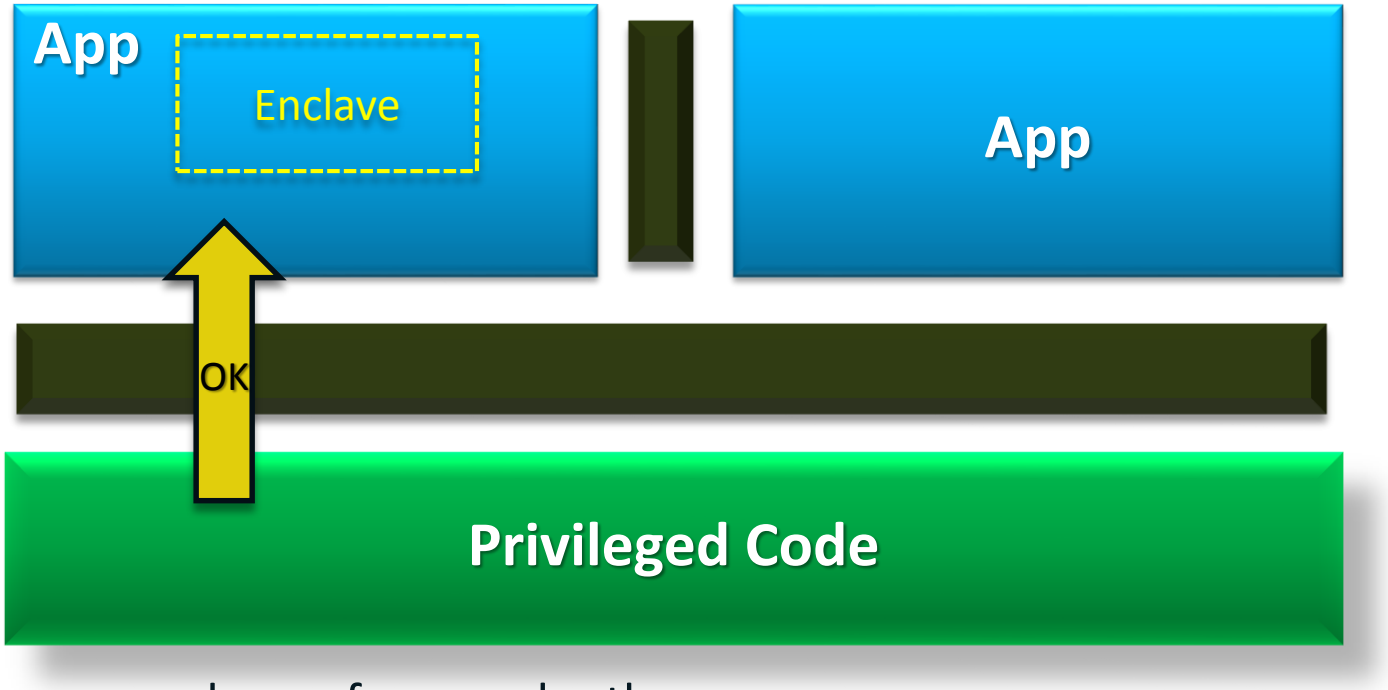
The Basic Issue: Vulnerabilities in Privileged Code

Protected Mode (rings) protects OS from apps …



The Basic Issue: Vulnerabilities in Privileged Code

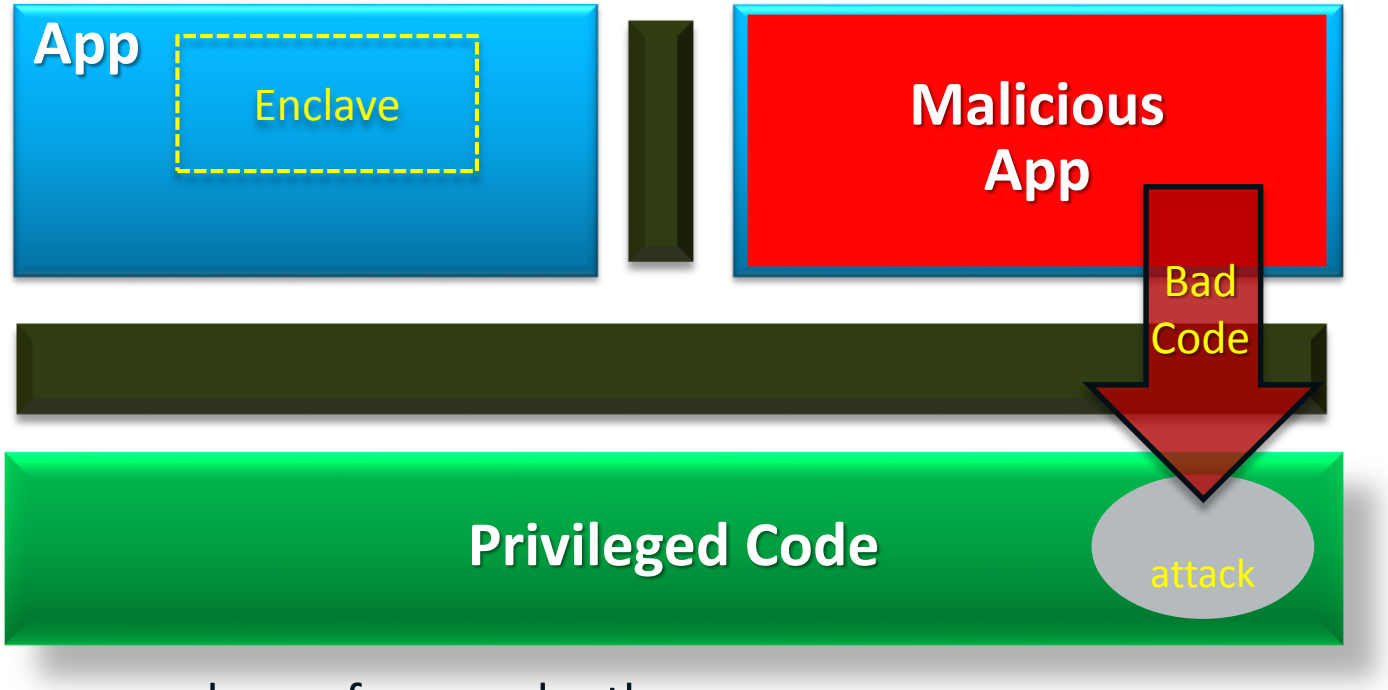
Protected Mode (rings) protects OS from apps …



… and apps from each other …

The Basic Issue: Vulnerabilities in Privileged Code

Protected Mode (rings) protects OS from apps …



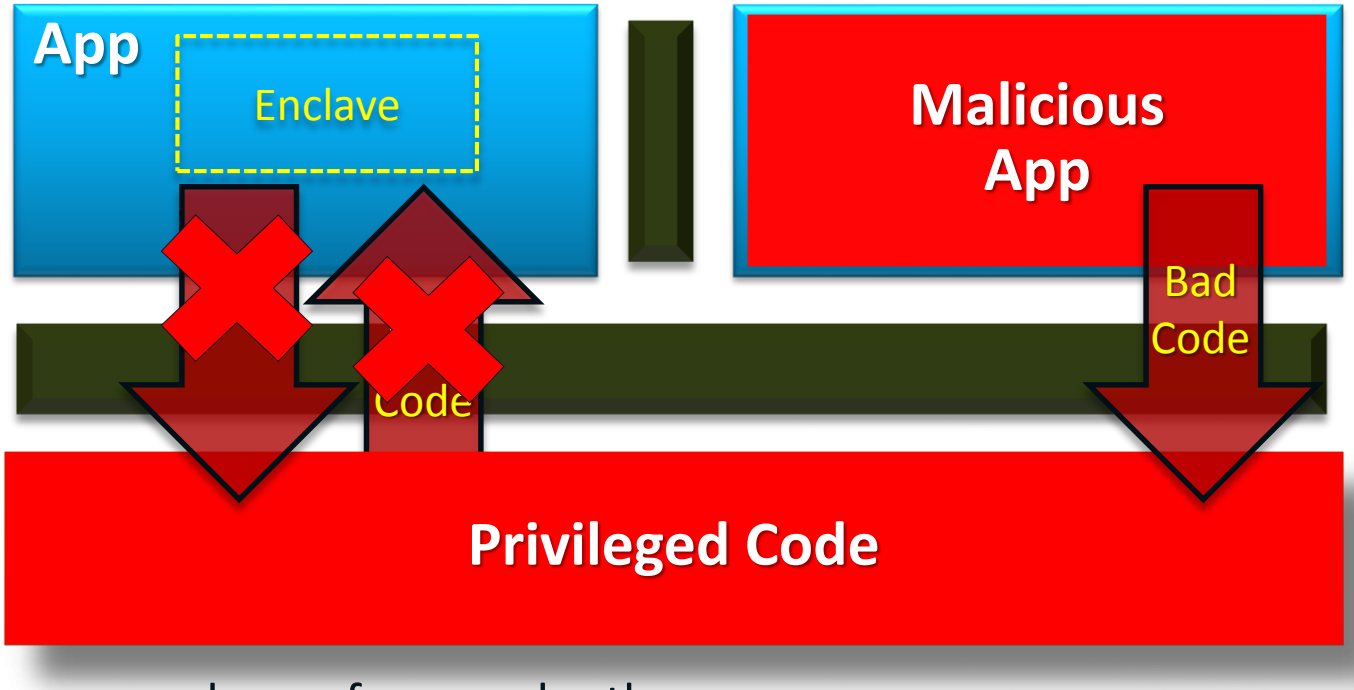
… and apps from each other …

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

Apps protected from privileged code attacks

The Basic Issue: Vulnerabilities in Privileged Code

Protected Mode (rings) protects OS from apps …



… and apps from each other …

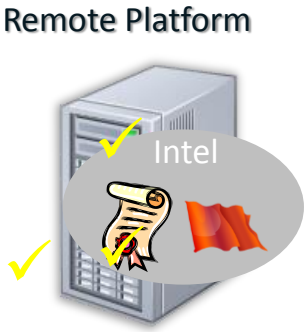
… UNTIL a malicious app exploits a flaw to gain full privileges and then tampers with the OS or other apps

Apps protected from privileged code attacks

Critical Features: Attestation and Sealing

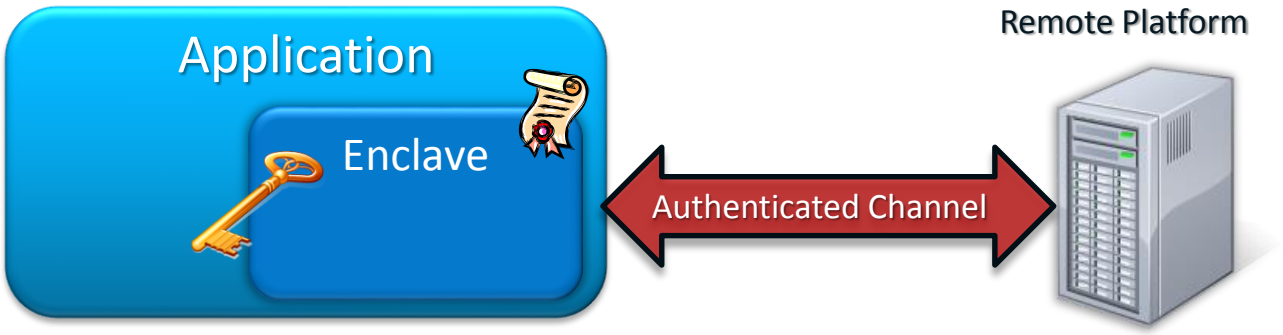
- App executes on local platform

Critical Features: Attestation and Sealing



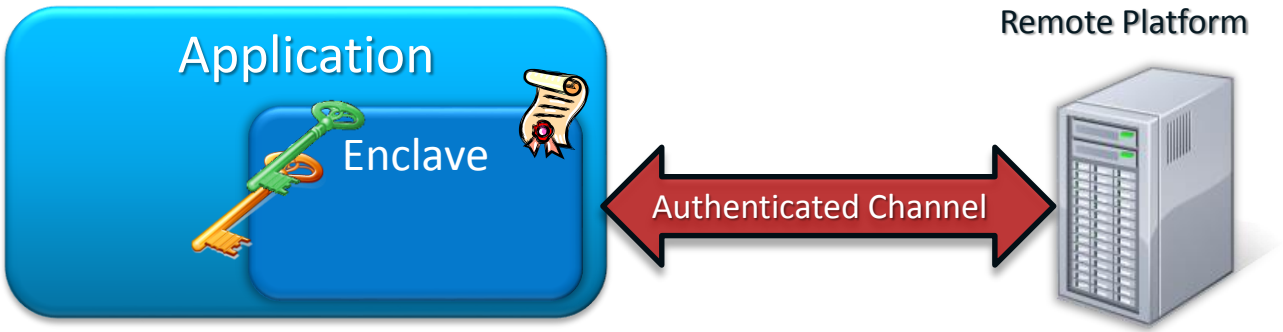
- App executes on local platform
- HW based **Attestation** provides remote platform assurance that “this is the right app executing in the right platform “

Critical Features: Attestation and Sealing



- App executes on local platform
- HW based **Attestation** provides remote platform assurance that “this is the right app executing in the right platform “
  - ⇨Remote platform can provision local platform with secrets

Critical Features: Attestation and Sealing



- App executes on local platform
- HW based **Attestation** provides remote platform assurance that “this is the right app executing in the right platform “
  - ⇨Remote platform can provision local platform with secrets
- App can seal secrets to platform for future use

Intel ® SGX Coverage of Desired Protections

Protection	Description
Protection from firmware attack	SMM, BIOS, Graphics card, etc
Protection from SW attacks	OS, VMM, Drivers, etc.
Operator Access	Operator can't access restricted data
Administrator Access	Admin can't access restricted data
Replay Attacks	Insert old data values in place of latest data value
Protection from translation changes	Privileged code should not be able to change address mappings
Understand platform type	Prove to external party what protection a platform offers
Correct entry and exit points	Only execute at allowed spots
Side Channels	External observers can't gleam data from timing, power, voltage, etc.

Intel ® SGX Coverage of Desired Protections

Protection	Description
Protection from firmware attack	SMM, BIOS, Graphics card, etc
Protection from SW attacks	OS, VMM, Drivers, etc.
Operator Access	Operator can't access restricted data
Administrator Access	Admin can't access restricted data
Replay Attacks	Insert old data values in place of latest data value
Protection from translation changes	Privileged code should not be able to change address mappings
Understand platform type	Prove to external party what protection a platform offers
Correct entry and exit points	Only execute at allowed spots
Side Channels	External observers can't gleam data from timing, power, voltage, etc.

Replay Attacks

- Encrypting data is not sufficient to protect against software attacks
- Privileged software can substitute old state to change control flow and data calculations
- Results in cryptographic and control flow changes
- “Paper clip attack”
- Memory aliasing attack from BIOS, VMM, OS

Research Past, Present, and Future

- Intel ® SGX 1 is shipping in client processors today
- Intel ® SGX 2 architecture defined, published, and software being developed
- Intel ® SGX 3 is under development at Intel Labs, Oregon
- Intel ® SGX 4 work starts this year

Links

- SGX Resource Page: https://software.intel.com/en-us/sgx
- Intel's Software Developers Manual Page (Programming Reference): http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html
- Joint research poster session: http://sigops.org/sosp/sosp13/
- Public Cloud Paper using SGX2: https://www.usenix.org/sites/default/files/osdi14_full_proceedings.pdf
- HASP 2013 Workshop: https://sites.google.com/site/haspworkshop2013/workshop-program
- ISCA 2015 Tutorial: http://sgxisca.weebly.com/
- Real World Crypto:
  - RWC talk: https://drive.google.com/file/d/0Bzm_4XrWnl5zOXdTcUlEMmdZem8/view
  - Attestation: https://drive.google.com/file/d/0Bzm_4XrWnl5zQzB4aHdkZGFkaFE/view?usp=sharing
- MIT Report: https://eprint.iacr.org/2016/086.pdf
- MEE Paper: https://eprint.iacr.org/2016/204

Thank You