presented by

Improving Platform Security with UEFI Secure Boot and UEFI Variables

UEFI Spring Plugfest – March 29-31, 2016

Presented by David Chen (Insyde Software)

Agenda

- Introduction
- UEFI Variables
- New Secure Boot Model
- Call For Action

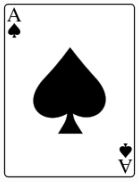
Introduction

Variables may be attacked

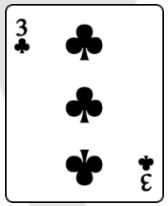
POST

RT

VarA



VarB



Current Secure Boot Model

Setup Mode

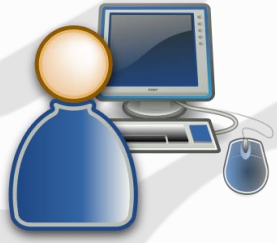
PK_{pub} == NULL
SetupMode == 1
SecureBoot == 0

Secure Boot Off

Enroll PK_{pub}

1. Delete PK_{pub}
2. Platform-Specific PK_{pub} Clear

User Mode



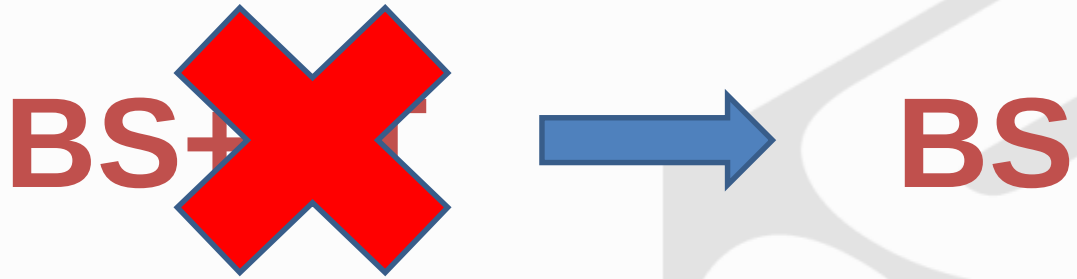
PK_{pub} != NULL
SetupMode == 0
SecureBoot == 1

Secure Boot Ready To Go

UEFI Variables

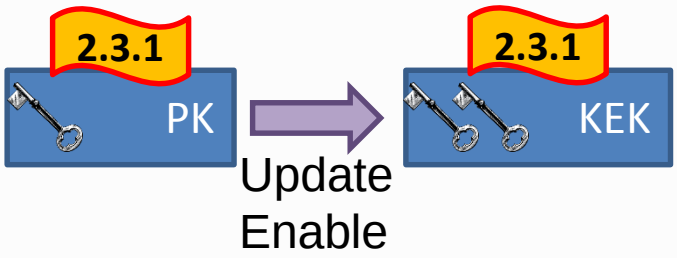
Protect the Variables

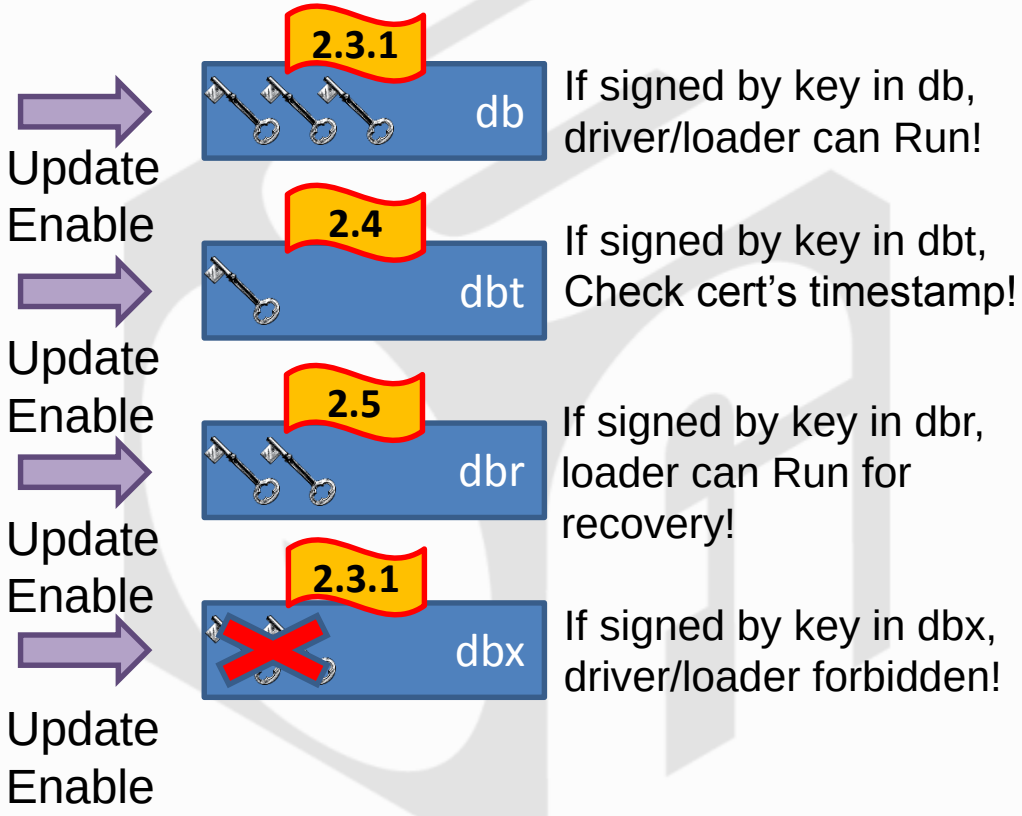
- Set Variable without RT attribute



- Variable Lock

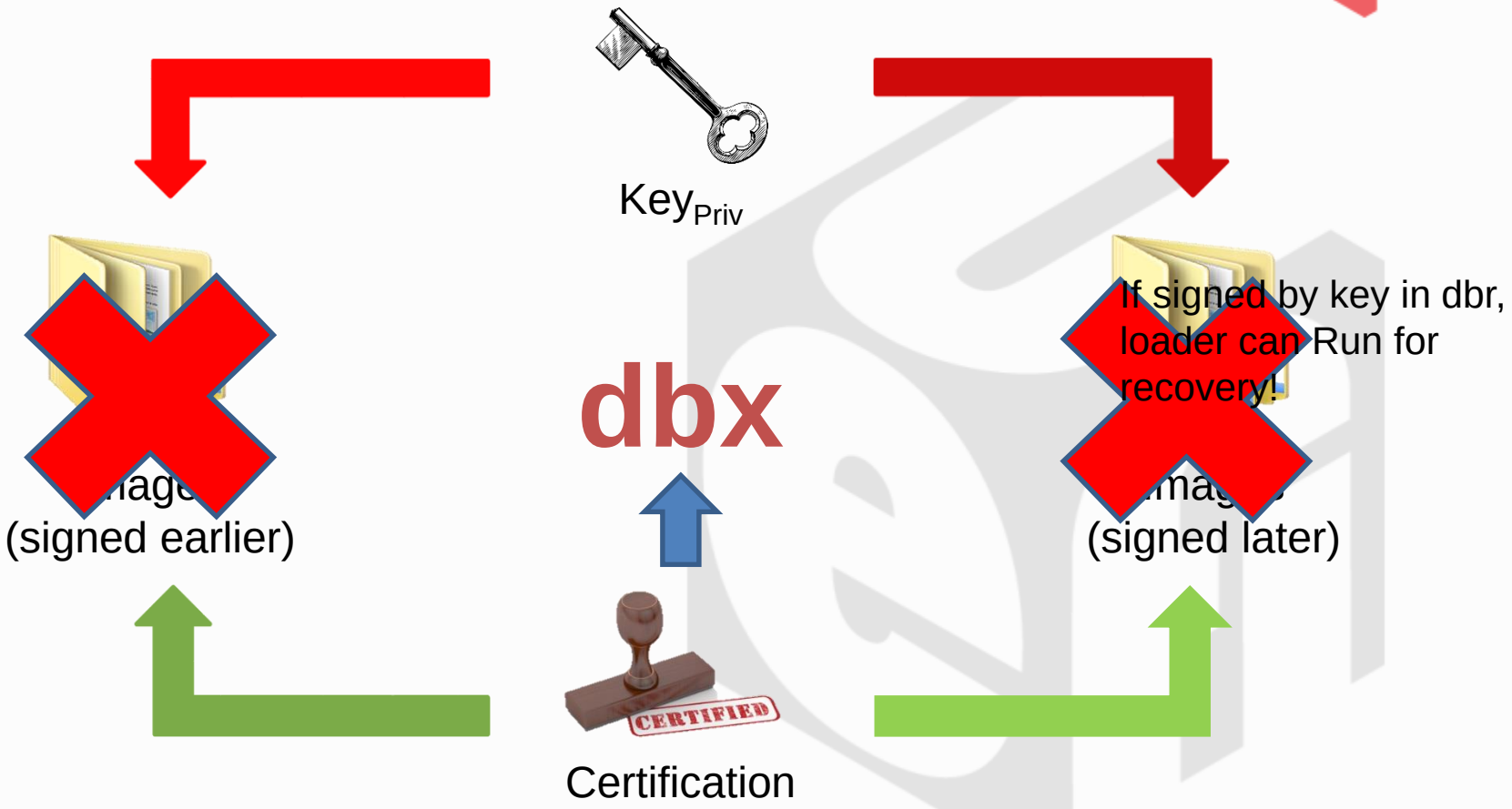
UEFI Secure Boot Database





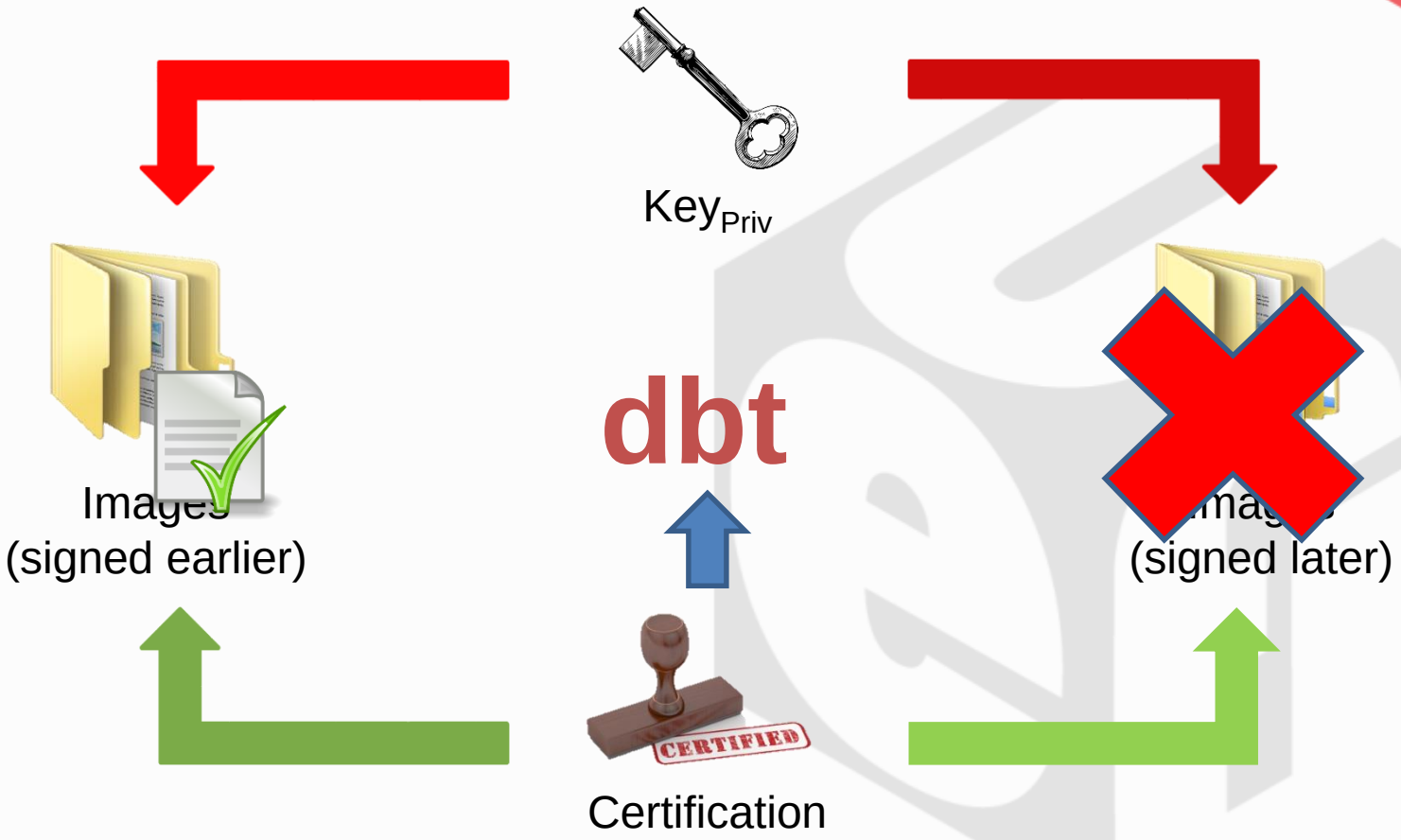
Scenario to use dbt

Before UEFI Specification v2.4



Scenario to use dbt

After UEFI Specification v.2.4



UEFI Variables

Secure Boot Modes

SetupMode

2.3.1

AuditMode

2.5

DeployedMode

2.5

New Secure Boot Model

Why Audit/Deployed Mode?

- Customers (ex: data center, government, etc.) have different requirement for secure boot database.
- But the Secure Boot Database isn’t easy to be customized with the old model!

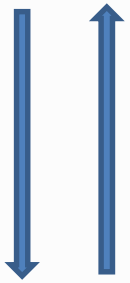
Audit Mode

Log more info to IEIT

User Mode

PK_{pub} != NULL
AuditMode==0 (RW)
SetupMode == 0
SecureBoot == 1

1. Delete PK_{pub}
2. Platform-Specific PK_{pub} Clear



Enroll PK_{pub}

PK_{pub} == NULL
AuditMode==0 (RW)
SetupMode == 1
SecureBoot == 0

Set **AuditMode** to**1**

Audit Mode

PK_{pub} == NULL
AuditMode==1 (RO)
SetupMode == 1
SecureBoot == 0

Deployed Mode

PK_{pub} != NULL
AuditMode == 0 (RO)
DeployedMode==1 (RO)
SetupMode == 0
SecureBoot == 1

Platform-Specific DeployedMode Clear

Set **DeployedMode** to1

Deployed Mode

User Mode

PK_{pub} != NULL
AuditMode == 0 (RW)
DeployedMode==0 (RW)
SetupMode == 0
SecureBoot == 1

1. Delete PK_{pub}
2. Platform-Specific PK_{pub} Clear

Enroll PK_{pub}

Enroll PK_{pub}

Setup Mode

PK_{pub} == NULL
AuditMode == 0 (RW)
DeployedMode==0 (RO)
SetupMode == 1
SecureBoot == 0

Set AuditMode to1

PK_{pub} == NULL
AuditMode == 1 (RO)
DeployedMode==0 (RO)
SetupMode == 1
SecureBoot == 0

Audit Mode

Call For Action

Call For Action

- Critical variables need to be protected
- Customers need more flexible customized secure boot databases
- Update your spec to adopt new secure implementation to enhance your platform’s security

Thanks for attending the
UEFI Spring Plugfest 2016

For more information on the Unified EFI Forum and UEFI Specifications, visit
http://www.uefi.org

presented by

insyde®

Backup

UEFI Variables

Secure Boot Databases

- 2.3.1 Platform Key (PK)
- 2.3.1 Key Exchange Key Database (KEK)
- 2.3.1 Secure Boot Signature Database (db)
- 2.3.1 Secure Boot Blacklist Signature Database (dbx)
- 2.4 Secure Boot Timestamp Signature Database (dbt)
- 2.5 Secure Boot Authorized Recovery Signature Database (dbr)