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

VarA

VarB
Current Secure Boot Model

Setup Mode

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

User Mode

1. Enroll $PK_{pub}$

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

Secure Boot Off

Secure Boot Ready To Go

PK_{pub} != NULL
SetupMode == 0
SecureBoot == 1
Protect the Variables

- Set Variable without RT attribute

BS+X → BS

- Variable Lock

Critical Variables
UEFI Secure Boot Database

If signed by key in db, driver/loader can Run!
If signed by key in dbt, Check cert’s timestamp!
If signed by key in dbr, loader can Run for recovery!
If signed by key in dbx, driver/loader forbidden!

PK → KEK
Update Enable

2.3.1 → db

2.4 → dbt

2.5 → dbr

2.3.1 → dbx

Update Enable

Update Enable

Update Enable

Update Enable
Scenario to use dbt
Before UEFI Specification v2.4

Images (signed earlier)

If signed by key in dbr, loader can Run for recovery!

Images (signed later)

Key_{Priv}

dbx

Certification
Scenario to use dbt
After UEFI Specification v.2.4

Images (signed earlier)

Key

dbt

Images (signed later)

Certification
UEFI Variables
Secure Boot Modes

- SetupMode
- AuditMode
- DeployedMode
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

User Mode

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

Audit Mode

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

Log more info to IEIT

Set AuditMode to 1

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

Audit Mode
Deployed Mode

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

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

User Mode

AuditMode == 0 (RW)
DeployedMode==0 (RW)
SetupMode == 0
SecureBoot == 1

Set DeployedMode to 1

Platform-Specific DeployedMode Clear

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

Set AuditMode to 1

Audit Mode

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

Enroll PK_{pub}

Deployed Mode

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

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

Enroll PK_{pub}

Setup Mode

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

Set DeployedMode to 0

Platform-Specific DeployedMode Clear
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
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)