presented by

Establishing and Protecting a Chain of Trust with UEFI

Spring 2017 UEFI Seminar and Plugfest

March 27 - 31, 2017

Presented by David Chen (Insyde)

Agenda

- What is the Root of Trust?
- What is Secure Boot?
- What is Measured Boot?
- UEFI and Firmware Updates
- Next Steps

What is the Root of Trust?

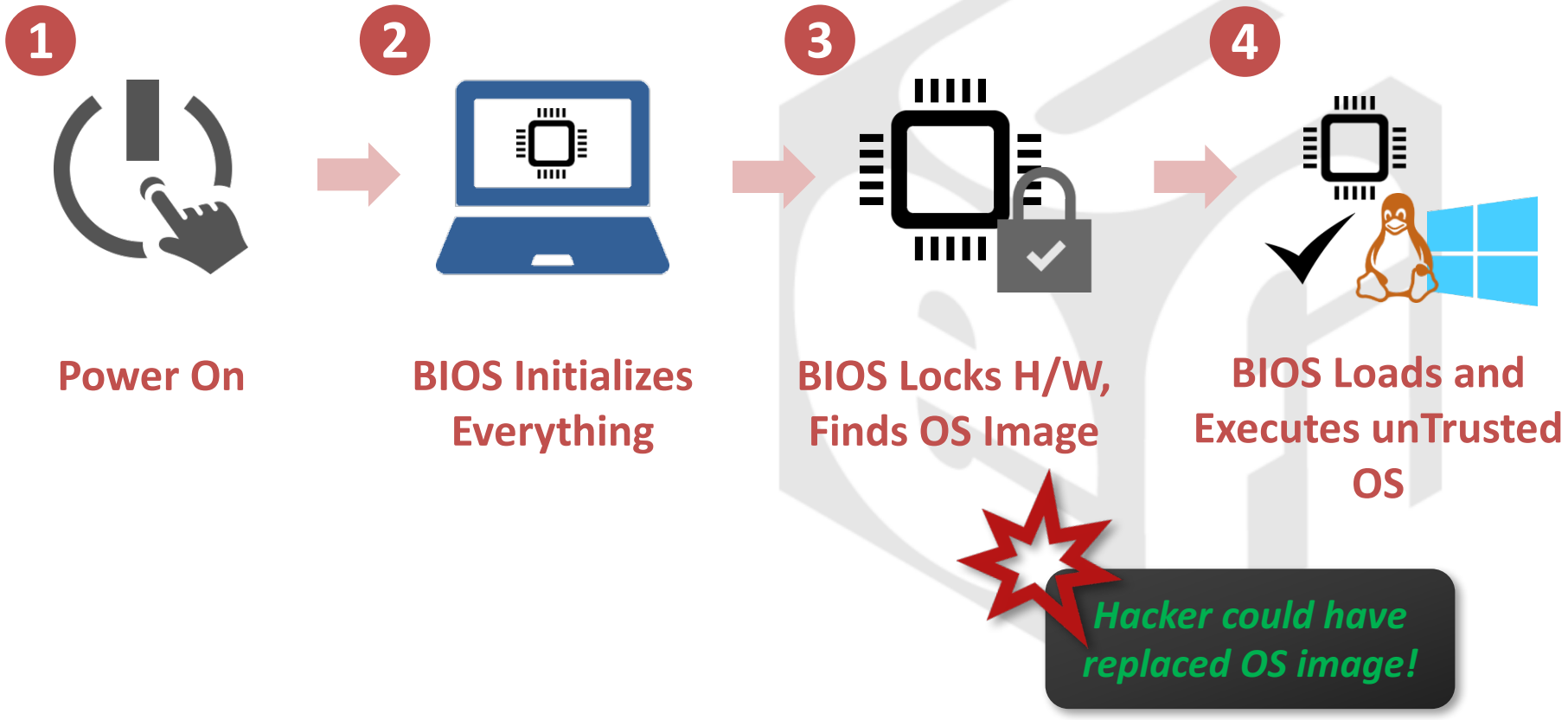
Root of Trust is a Security Concept

- Method to trust the system boot path has not been hacked by scheme like root kit
- Hardware and UEFI Firmware maintain Root of Trust until control transfers to OS
  - Hardware initiates Root of Trust:
    - Hardware starts CPU execution and makes some checks
    - Hardware hands off to the trusted UEFI Firmware
    - UEFI Firmware must maintain the Chain of Trust
  - Hardware is the physical Root of Trust
  - UEFI Firmware must protect Root of Trust

UEFI & Root of Trust

- UEFI & hardware provide features to protect the Root of Trust
  - UEFI Specifications have protection features
    - Authenticated variables
    - Secure Boot databases
    - Secure Boot policies
  - Modern hardware has protection features
    - Regions of Read & Write locks
    - SMIs generated by Write attempts
- UEFI Firmware uses these features to protect the Chain of Trust
- Trust is about the method of trust and trust systems

Traditional Boot is Not Secure



What is Secure Boot?

UEFI Image Signing

- Signing is creating a hash of the protected content and encrypting that hash with a private key held secure by the software author
  - Hashing always generates the same result from the same input
  - Process has very few collisions
    - Mathematically impossible to create a useful hacked image
- Signature checking is a two-step process
- Hash the code to be validated
- Decrypt the hash stored by signing process using the public key and compare with the value created in signing step
- Certificates controlled by Certificate Authorities or OEMs
- Private Keys should be protected!
  - Control physical and electronic access to Private Keys

UEFI Secure Boot

- UEFI Firmware verifies the signature of external firmware and software before execution
  - Option ROMs (Graphics, Network)
  - OS Bootloader Images (Windows, Linux, Android, custom OSs)
  - Test Firmware (Factory firmware, built-in diagnostics)
  - Boot Applications in embedded devices (Drone Flight app)
- The image must be signed by a trusted signer
- Secure Boot process verifies that only trusted images execute

UEFI Secure Boot & Root of Trust

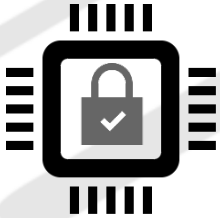
1

Power On

2

BIOS Initializes Everything

3

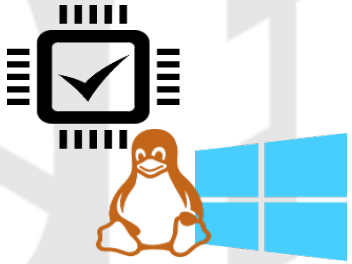


BIOS Locks H/W

4

BIOS Loads & Verifies OS Bootloader Signature

5



Boot Loader Verifies OS Image and Loads Trusted OS

What is Measured Boot?

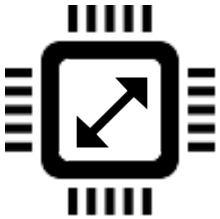
UEFI Image Measuring

- For export, TPM Trusted Boot defined by TCG specifications
- For China domestic, the TCM specification is used
- Measuring uses the PCR register to create a kind of hash of important boot stages
- There are several PCR registers defined to contain the hash of particular elements
- OS checks specific PCR values to discover if there were unexpected changes to the boot path elements
- OS must be informed if authorized changes occur, like if the firmware is updated

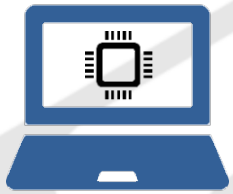
UEFI & Measurements

1. 

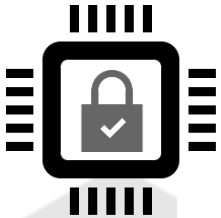
   Power On

2. 

   BIOS Measures Itself

3. 

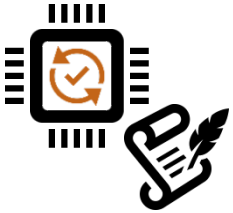
   BIOS Initializes Everything

4. 

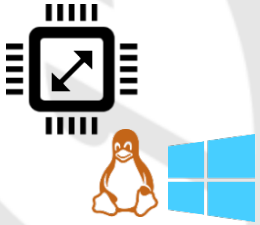
   BIOS Locking H/W Writes to BIOS

5. 

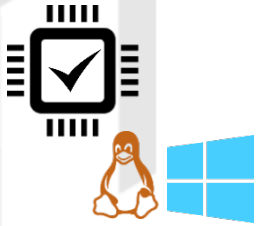
   BIOS Measures Hardware

6. 

   BIOS Measures & Verifies OS Signature

7. 

   BIOS Measures OS

8. 

   BIOS Executes Trusted OS

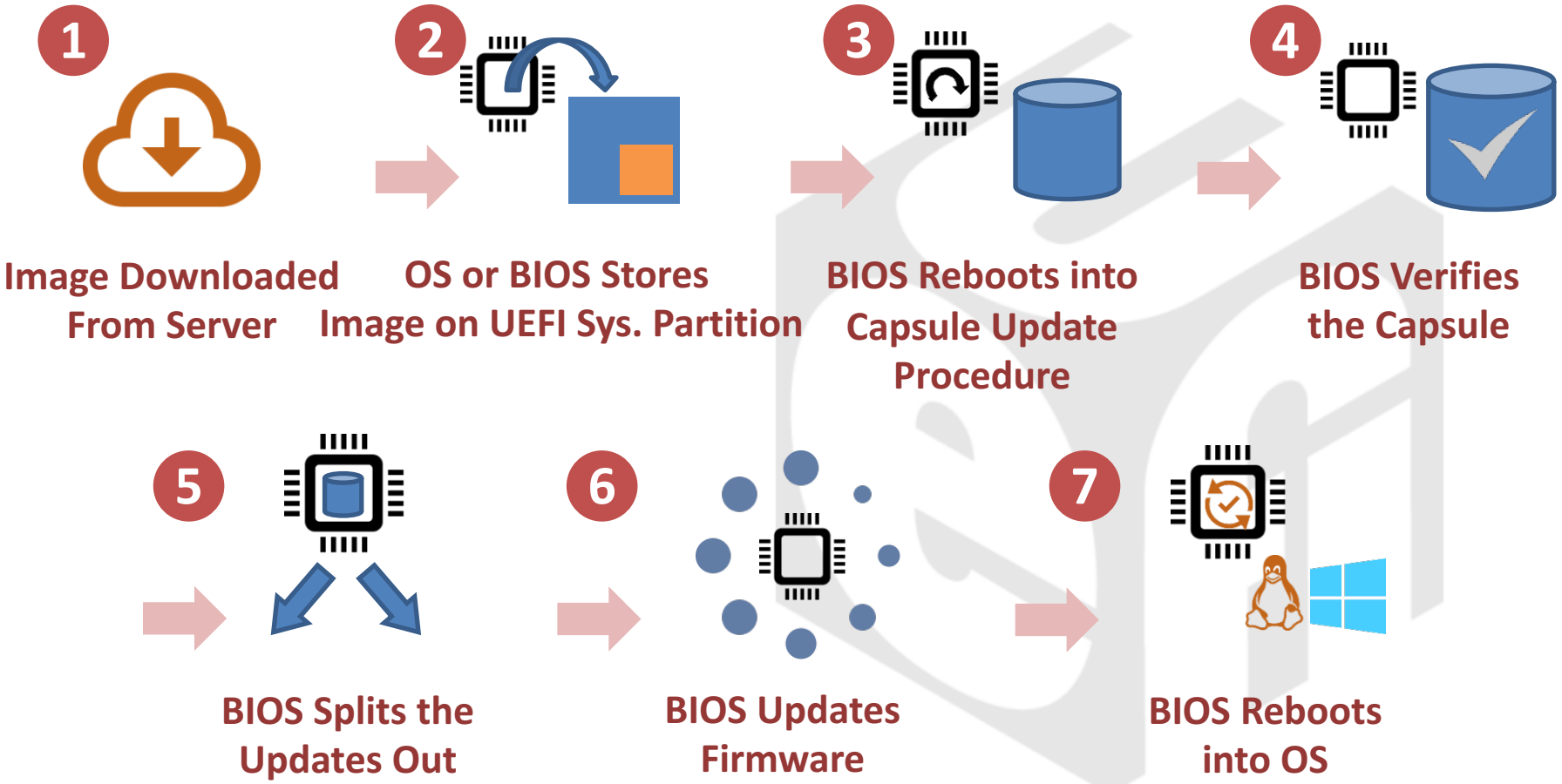
UEFI and Firmware Updates

Firmware Updates

- OS or OEM website can provide updates
  - Windows update already supports
  - Can update UEFI Firmware
  - Can update other firmware components
  - Firmware publishes a list of all updatable elements (get table name)
- Update capsule can be stored on HDD or in memory
  - UEFI reboots to launch the chain of trust and root of trust
  - Verifies the signature on the capsule
  - Updates the correct firmware
- Your system should support UEFI FW Update

UEFI & Firmware Updates

- System Update Process:



Next Steps

Call to action

- Enable Secure Boot
  - Protect the Root of Trust in OS Boot
- Support TPM 2.0 or TCM
  - Load measurements into TPM or TCM PCRs
- Support UEFI Firmware updates
  - Provide updates to end users

Thanks for attending the Spring 2017 UEFI Seminar and Plugfest

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

presented by

insyde™