Manufacturing Tools in the UEFI Secure Boot Environment

Presented by Stefano Righi

presented by

American Megatrends

Agenda

Introduction

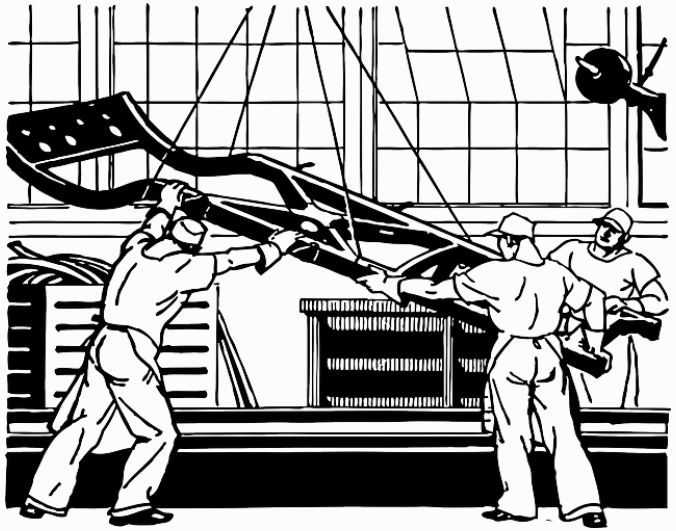
Transition of Manufacturing Tools to UEFI

Manufacturing Tools and UEFI Secure Boot

Call to Action

Introduction

Introduction



As OEMs produce hardware, each system needs to be individually provisioned on the production line

Each system needs individual attention for programming of specific devices and configuration

Manufacturing Tools Uses

Manufacturing tools example uses include:

Pre-installing an OS

Installing OS related keys for activation

Programming of device data like MAC addresses

Updating platforms BIOS to latest version

Programming SMBIOS structures

Locking interfaces used for manufacturing tools

Pre-UEFI Manufacturing Process

OEMs would write custom tools that would run in reduced OS environments where the tools have direct access to hardware

Some ODMs created very advanced manufacturing environments where the system was very modular

Since these tools are legacy based they could never be signed for use in a UEFI Secure Boot environment

UEFI Secure Boot

UEFI Secure Boot is a very important feature that helps prevent attacks during the handoff from firmware to the operating system

UEFI Secure Boot is a feature that allows systems to only execute authenticated images that have been signed by a trusted certificate authority (CA)

More information on Secure Boot here

UEFI CA

Currently there is only one UEFI Certificate Authority

The UEFI CA is responsible for inspecting and signing images

When someone submits an image for signing, the CA will:

- ✘ Reject the image if it does not satisfy signing requirements
- ✓ Provide back a properly signed image to the requester

More info on the UEFI CA here

UEFI Only Systems

Some manufacturers still rely on legacy based manufacturing tools

- UEFI Class 3 systems have no support for the legacy environment the tools rely on
- These manufacturers need a set of tools to support provisioning these types of systems

More info on UEFI system classes here

Transition of Manufacturing Tools to UEFI

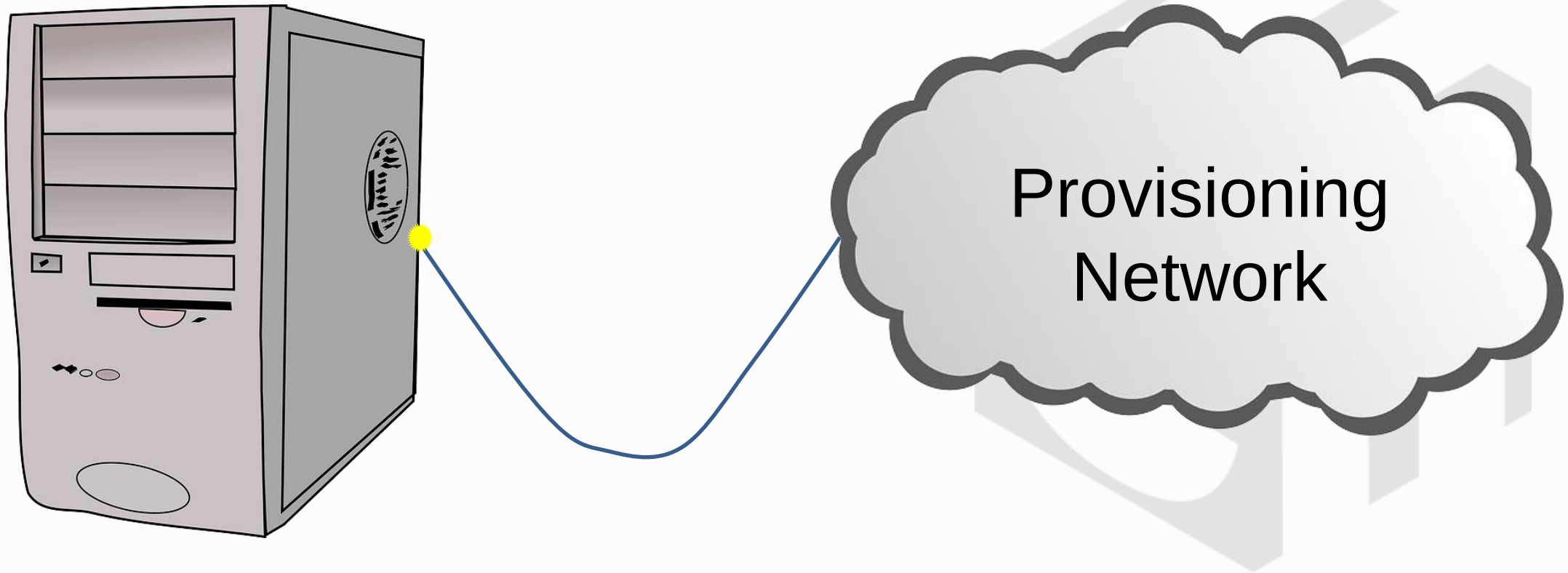
UEFI Manufacturing Tools

UEFI provides a very feature rich environment to create manufacturing tools and easy access to a network

UEFI provides abstracted methods for configuring all hardware of the platform and its attributes, provisioning of the OS, and populating of system tables

Sample code for writing UEFI manufacturing tools can be found at www.tianocore.org

UEFI Manufacturing Tools



UEFI CA and Manufacturing Tools

The UEFI CA does not allow signing of manufacturing tools

Manufacturing tools operate at an equivalent of ring 0 execution to program all components of a platform

If these tools were signed by the CA, they could be used for malicious purposes on any system

How do OEMs run these tools with UEFI Secure Boot?

Manufacturing Tools and UEFI Secure Boot

Self Signing of Tools

OEMs can sign their own utilities

This is done by using a private key to sign the image and inserting a corresponding public key into the UEFI authenticated variable

Once this is done, the system will authenticate their manufacturing utility just like any image signed by the UEFI CA

Signing Tools

For signing on Windows use signtool.exe from Microsoft

Signtool is included with Visual Studio or the Windows Development Kit (WDK) located here

For signing on Linux there is an open source tool based upon OpenSSL located here

Other possible solutions

The OEM can build a manufacturing suite in Linux and sign their own kernel

- Learn how to sign Linux kernel here

The OEM can use the legacy tools and enable Secure Boot at the end of the provisioning

- Requires that the system not be Class 3

The OEM can use unsigned UEFI tools and enable Secure Boot at the end of the provisioning

Demonstration of Self Signing

Demonstration includes:

Showing how to insert a key into the proper database

Signing an image

Proper failed and successful authentication of the signed/unsigned image

Call to Action

Call to Action

Companies should transition their tools for UEFI if they have not already done so

Class 3 system shipments are on the rise

OEMs should evaluate what sort of UEFI provisioning environment works best for them

OEMs and developers should become familiar with how to sign and insert keys for their own utilities

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

presented by