presented by

UEFI Secure Boot use cases and Linux

UEFI Summer Summit – July 16-20, 2012

Presented by Matthew Garrett (Red Hat, Inc.)

Agenda

- Introduction
- Supporting secure boot
- Changing kernel policies
- Meeting a range of customer needs
- Summary
- Questions

Introduction

- Secure Boot is not just for Windows
- Secure boot is not just for end-users
- Supporting Linux and wider deployment use-cases is important

Linux design decisions

- Linux has very different demands
- More rapid release cycles
- System level components change within releases
- Gating every update via Microsoft impractical

Our approach

- Simple trusted bootloader
  - Attempts to LoadImage() and StartImage() secondary bootloader
  - If that fails, attempts to validate secondary bootloader against built-in key
  - Obeys dbx entries
  - Installs validation handler protocol

Our approach

- Benefits
  - Small trusted codebase with very little churn
  - Almost entirely Tiano code
  - Independent testing of CryptLib implementation

Our approach

- Secondary bootloader
  - Grub2 – standard Linux bootloader
  - Validates signed kernel image via first-stage validation protocol
  - Provides UI and configuration

Our approach

- Kernel
  - Implements signed driver requirements
  - Various interfaces locked down to avoid administrator→kernel escalations
  - Significant change to the existing Linux model

Handling customer requirements

Serving customers

- Secure boot is not just about end -users
- Customer requirements vary widely

Serving customers

- Can't assume that customers desire default keys
  - Local security requirements
  - Local policy requirements
- Supporting alternative trust roots is vital

Implementation

- Support for re-keying hardware currently awkward
  - Spec mandates clearing Pk, re-enrolling
  - UI and functional inconsistencies
  - Vendors may offer different configuration to large customers
- Thoughts on improving this?

Implementation

- Replacing signed components much easier
  - Tools available for key generation and re-signing
  - Support for building install images and media
- But what about updates?

Summary

- Linux has different requirements, so takes different approaches
- Customers appreciate flexibility, expect to extend this to secure boot

Questions?

Thanks for attending the UEFI Summer Summit 2012

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

presented by