OpenXT UEFI/SecureBoot support

Dr. Tamas K Lengyel, Bradley Hansel

November 30, 2017

Overview

- **Background**
  - **UEFI**
  - **SecureBoot**
  - **Upstream status**
- **Proposed OpenXT extensions**
  - **Changes required**
  - **Current status**
- **Questions**

UEFI

- Industry standard specification
- Replaces legacy BIOS interfaces
- Systems shipping today are UEFI systems
- Not just on x86
- “Compatibility Support Module” available
  - Intel intends to deprecate it by 2020
- Does TPM measurements by default
  - PCR 0-3
- It is just a specification
  - Implementations can vary widely

SecureBoot

- **Optional extension of UEFI**
- **Widely used on consumer machines**
  - **Required by Microsoft certification**
  - **Many systems ship with Microsoft keys**
- **UEFI firmware only executes code that has valid signature**
- **SecureBoot Keys stored in NVRAM**
  - **Protected storage, survives reboots**
- **Can be replaced by custom-keys by OEM or by placing the system into “SetupMode”**
  - **Part of the UEFI BIOS implementation**
  - **Varies widely between vendors**

Upstream status

- OpenXT is not UEFI ready
- tboot is not UEFI ready

Upstream status

- **Xen supports UEFI out-of-the box**
  - **Separate EFI binary is compiled**
- **Linux supports UEFI out-of-the box**
  - **bzImage is a polyglot**
- **Can boot Xen with SecureBoot enabled**
  - **Dom0 kernel doesn’t get measured**
  - **Dom0 kernel doesn’t get verified**
  - **XSM policy doesn’t get measured**
  - **XSM policy doesn’t get verified**
  - **Command line arguments can be changed at boot-time with no trace**

Upstream status

- Xen supports the ***shim*** out-of-the box
- Small UEFI application that launches another
  - Mostly used to verify & launch grub
  - Can verify & launch Xen too
  - Tries to load it via UEFI interface first
  - Falls back to verifying with its own key, useful if replacing keys in NVRAM is a problem
- The “shim lock protocol” is exposed via UEFI
  - Can verify and measure additional code
  - Xen uses it to verify dom0 kernel by default!

Upstream status

- **OpenXT already uses TPM PCR 0-3**
  - **UEFI measurements**
- **If we also include PCR 4-7 we would have full coverage of all code that executed during boot + SecureBoot keys and policy**
  - **Static measurements only!**
- **Need to eliminate all boot-time “options”**
  - **No grub**
  - **No command-line arguments**
  - **No separate XSM policy file**
  - **No Separate initrd image**
  - **No DKML / enable KMS**

OpenXT extensions

- **We propose to start UEFI support using what’s available upstream**
- **Introduce minimal changes to the existing build and boot process**
- **Keep legacy boot support intact**
  - **No changes to tboot or TXT for systems using legacy boot**
- **Keep options open to integrate with D-RTM measurements in the future**

Impact

- No impact on systems that continue to use legacy boot
- No changes to the security posture
- No changes to response and recovery
- No changes to upgrade / OTA interfaces

Out-of-scope

- Migrating existing installations to UEFI
- Firmware security analysis
  - Many existing tools and research out there
- Porting tboot to UEFI
  - Can be done in the future
  - Some preliminary work already done

High-level changes

- **Change partitioning to use GPT**
  - **Required for UEFI support**
- **Add an EFI System Partition (ESP)**
  - **~512M FAT32**
- **Compile XSM into Xen**
- **Compile command-line into Xen**
- **Compile initramfs into dom0 kernel**
- **Compile command-line into dom0 kernel**
- **Compile kernel-modules into dom0 kernel**
  - **Or enable kernel-module signing**
- **Boot via the shim when UEFI is enabled**

Status

- **No patches for OpenXT yet**
  - **WiP patches are on github**
- **PoC system tested using vanilla Xen 4.9, Linux 4.14 on Debian Stretch**
  - **Instructions are on github**
- **While mostly everything is there we have encountered issues**

Tweaking the shim

- **Didn’t boot Xen as the PE .reloc section was marked discardable**
  - **Xen uses it for sanity checking, if not present it bails**
- **Only measured the first application it launched into the TPM**
  - **The shim lock protocol only did verification**
  - **Only if SecureBoot is enabled**
- **Ignored TPM errors**
  - **Failed measurements on TPM2 systems**
  - **Have fall-back option for buggy UEFI**
- **Cross-compiling 64-bit version on 32-bit host broken**

Tweaking the shim

- Most of the tweaks are being upstreamed
- Received +1 from Matthew Garret (Google Security)
- Some tweaks will be OpenXT specific as “proper” fixes need to be created for binutils
  - Add option to not mark .reloc discardable
  - For now we just add an option to the shim to ignore the discardable flag

Xen tweaks

- XSM policy can embedded in the Xen EFI image
  - Gets measured & verified during boot
- Embedded XSM policy only used if bootloader doesn’t specify another
  - While we don’t have a “bootloader” an arbitrary XSM policy can be specified in the Xen UEFI boot-config
- Add Kconfig option to only use built-in policy during boot
  - Patch already acked
  - Will be part of Xen 4.11

Expected patches to OpenXT

- **First round before Christmas**
  - **Implement basic UEFI boot with the same but without SecureBoot**
- **Second round in Q1 2018**
  - **Implement SecureBoot key-generation and signing scripts**
  - **Downstream projects will have to determine how to best store SecureBoot keys**
  - **Probably should only use dummy keys during build**

Questions / Discussion