sectpmctl

Secure Boot and TPM2 backed LUKS Full Disc Encryption (FDE)

Entwickelt im Rahmen des T-Systems-MMS
Open Linux Client Projekts

https://github.com/T-Systems-MMS/sectpmctl

FrOSCon 2022
Richard Robert Reitz

Was ist sectpmctl

- Eine TPM gestützte FDE Anwendung ähnlich zu BitLocker
- Notwendig im Open Linux Client Projekt da Konzern Anforderung
- Soll nicht schlechter sein als BitLocker, muss aber auch nicht besser sein

Historie

- Entwicklungszeit 8 Monate
- TPM2 kennenlernen, PCR Werte analysieren, Debian Integration
- Verschiedene Upgrade Pfade evaluieren
- Secure Boot kennenlernen und benutzen
- Verschlüsselte Kommunikation zum TPM (TOFU)
- Verwenden von TPM Policies für TPM + Passwort

Anforderungen

M M S EXPERIENCE BEYOND DIGITAL

- Daten bei Diebstahl von ausgeschalteten Laptop schützen
- Manipulationen an Boot-Codes verhindern (Bootloader, Kernel, initrd)
- Bieten von hardwaregestütztem Schutz
- Administrativ einfach zu pflegen
- Automatisierte Installation
- Eine Recovery Methode bei Soft- oder Hardware Fehlern

Was ist TPM 2.0

- Hardwaregestützter Keystore
- Sichert Passwörter mit Bindung an einen Systemzustand (PCR sealing)
- Unterstützt Dictionary Attack Lockout Mechanismen

Für VPN und TLS EAP Netzwerk relevant:

- Sichert RSA/ECC Private Keys, der Key kann das TPM nicht mehr verlassen

TPM PCR Register

MMS EXPERIENCE BEYOND DIGITAL

0	BIOS
1	BIOS Config
2	Option ROM
3	Option ROM Config
4	Boot Images
5	MBR/GPT Partitionstabelle
6	Resume Event
7	SecureBoot Zustand

8	Grub Bootloader Config
9	Grub Bootloader Files
10	
11	sectpmctl
12	
13	
14	Shim Bootloader, MOK
15	

PCR Brittleness (Firmware)

Die Auswahl stabiler PCR Werte ist aus Firmware-Sicht nicht einfach:

- BIOS Updates ändern PCR 0 und 2
- BIOS Konfiguration ändert PCR 1 und 3
- Partitionstabelle ändert PCR 5
- Secure Boot Einstellungen ändern PCR 7

PCR Brittleness (Software)

Aus Software-Sicht ist die Auswahl leider auch nicht einfach:

- Kernel Updates ändern PCR 4 und 9
- Bootloader Updates ändern PCR 4 und 9
- Bootloader Konfiguration ändert PCR 8

Probleme mit PCR Brittleness

- Kleinste Änderungen am BIOS oder an den Softwareständen führen zu geänderten PCR Werten
- Während jedes Updates muss exakt erkannt werden ob sich etwas relevantes geändert hat
- Woraufhin in einem speziellen Upgrade Vorgang die PCR Werte im TPM aktualisiert werden müssen
- Größtes Risiko das nach einem Update alle User ein Recovery benötigen und zur IT Administration müssen

sectpmctl Features

- Null administrativer TPM Overhead nach Updates
- Keine PCR Brittleness Probleme

Dieses Ziel wird erreicht durch:

- Binden des LUKS Keys einzig an PCR 7 (Secure Boot Zustand)
- Implementierung eines eigenen Secure Boot - Bootloaders

Secure Boot und TPM

Der vom TPM gemessene Secure Boot PCR 7 Zustand umfasst:

- Ob Secure Boot ein- oder ausgeschaltet ist
- Die im UEFI BIOS hinterlegte komplette Secure Boot Datenbank
- Die Zertifikate mit denen der gebootete Bootloader und Kernel signiert wurden

Das TPM erzwingt keinen Secure Boot Status sondern prüft ihn

Dezentrales Secure Boot

- Den NSA UEFI Richtlinien nach die sicherste Methode

Datenbank	Vendor	Signiert / Bootet
PK	sectpmctl	KEK
KEK	sectpmctl	DB, DBX
DB	sectpmctl	Bootloader und Kernel
DB	Microsoft CA	Windows
DB	Microsoft UEFI	Linux, NVIDIA Option ROM
DBX	uefi.org	Blockt Schadsoftware

Implementierung sectpmctl boot

Benutzt die systemd-boot und -stub Infrastruktur

- systemd-stub erzeugt eine EFI Datei aus Kernel, Command Line und initrd, die mit eigenem Secure Boot db Key signiert wird
- systemd-boot wird als eigentlicher Bootloader verwendet. Alle Features wie Cursor-Steuerung oder setzen von Default-Einträgen werden unterstützt

Preseed Installation

Vorbedingung: Das TPM und Secure Boot ist gelöscht

- Die Preseed Installation kann komplett unbeaufsichtigt durchlaufen

Sie besteht aus zwei Teilen:

- Eine Preinstallation zum Setzten der eigenen Secure Boot Keys und binden des LUKS Keys an den schwachen PCR 0 (BIOS) mit anschließendem Reboot
- Eine Postinstallation die den LUKS Key aus dem PCR 0 an den nach dem Reboot nun gültigen PCR 7 bindet

Fazit

- Keine Probleme beim Friendly User Test und in der Pilotgruppe festgestellt
- Erreicht durch Nutzung von Debian Vorgaben hohe Stabilität und gute Integration
- Überlebt Upgrades von Ubuntu 20.04 auf 21.10 und von 21.10 auf 22.04
- Überlebt BIOS Updates
- ca. 120Kb bash-Skripte