Firmware Signatur-Relay in einer TEE

Das Program hat den Zweck, Signaturen die von einzelnen Nutzern über eine Firmware gemacht werden, mit einem permanenten Produktions-Key zu maskieren, ohne, dass der Nutzer diesen kennt. Dabei wird eine Encalve als Signatur-Relay verwendet. Die Enclave kann Signaturen über Daten mit einem festen Satz an öffentlichen Schlüsseln, die vertrauenswürdig sind, verifizieren. Wenn die Signatur gültig ist, entfernt die Enclave die Signatur und erzeugt eine eigene Signatur mit dem Produktions-Key.

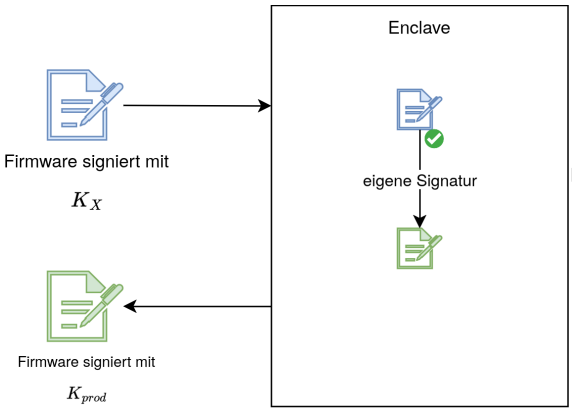

Figure 1: Valid Signature

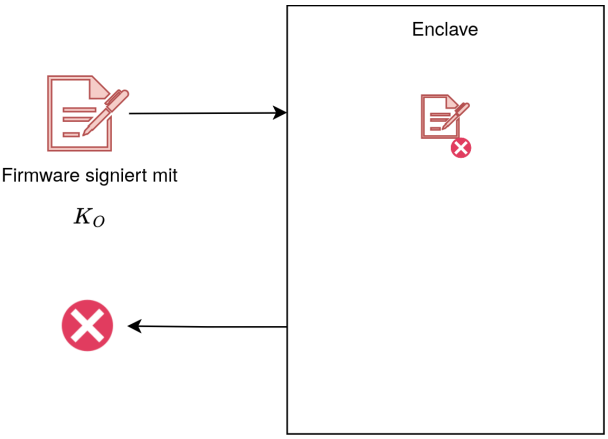

Figure 2: Invalid Signature

Diese Signatur kann dann mit dem öffentlichen Schlüssel der Enclave, der von außen angefragt werden kann, überprüft werden. Damit kann der Nutzer seine eigene Signatur mit der Signatur der Enclave maskieren.

Der Schlüssel ist dabei den Nutzern nie bekannt. Sie haben den Schlüssel nur versiegelt und können ihn der Enclave geben, die den Schlüssel dann entsiegeln und in der vertrauenswürdigen Umgebung verwenden kann.

Szenario

In diesem Szenario wird ein Unternehmen betrachtet, das Embedded Geräte produziert. Für die Geräte sollen regelmäßig Updates für die Firmware veröffentlicht werden. Diese Firmware muss mit einem permanenten Key signiert werden, der in der Produktion der Geräte fest codiert wird. Ist die Signatur nicht vorhanden, lädt keines der Geräte das Update.

Mitarbeitende, die die Firmware hochladen wollen, müssen also die implementierte Firmware mit dem Produktions-Key signieren. Wenn sie den Produktions-Key besitzen, bringt das gewissen risiken, z.B.:

- Mitarbeitende können (absichtlich oder nicht) den Schlüssel veröffentlichen
- Mitarbeitende, die nicht mehr in dem Unternehmen arbeiten, können den Key für schlechte Zwecke missbrauchen

Es ist also sinnvoll, wenn die Mitarbeitende den Key nicht kennen. Dazu kann das beschriebene Signatur-Relay verwendet werden. Die Mitarbeitenden signieren die Firmware vorerst mit ihrem eigenen Key. Diese Keys sind in das Relay als trusted Keys eingebunden. Anschließend kann der Mitarbeitende die

selbst-signierte Firmware an das Signatur-Relay senden. Das Relay prüft dann die Gültigkeit der Signatur und schickt, falls gültig, eine eigene Signatur über die Firmware zurück. Damit kann dann der Mitarbeitende die Firmware an die Embedded Geräte senden, bei Gültigkeit die neue Firmware laden können.

Falls ein Mitarbeitender den eigenen Schlüssel verlieren oder veröffentlichen sollte, besteht in dem Fall auch nicht das Problem, dass der Produktionsschlüssel ungültig wird. Es kann einfach der Schlüssel des Mitarbeitenden von der Liste der trusted Keys zurückgezogen werden.

Zudem ist es wichtig, dass keine bösartigen Programme auf den Systemen der Mitarbeitenden den Signaturprozess mitbekommen oder gar verändern können.

Aus diesen Gründen ist es in diesem Szenario wichtig, dass das Relay mit all seinen Funktionen besonders geschützt ist. Dementsprechend sollte es in einer Enclave laufen.

Details

1. **Key Management**

Das Key Management wird mit der eingebauten `seal` Funktion der Encalve gemacht. Dabei kann jeder Nutzer eine versiegelte Kopie des Schlüssels behalten, da er damit nichts anfangen kann. Erst, wenn der Schlüssel in die Enclave kommt und entsiegelt wird, kann der Schlüssel verwendet werden.

2. **Signatur Erstellung**

Die Enclave bietet eine Schnittstelle für Signaturen mit ECDSA an. Dabei wird die Kurve secp256k1 verwendet.

Vorteile

Dieses Programm bietet einige Vorteile, unter anderem:

- Nutzern unbekannter Hauptschlüssel
- Vereinfacht das Zurückziehen der Schlüssel
- Sicherheit der Gültigkeit der Firmware