Signieren von Firmware

Beim Signieren von Firmware handelt es sich um einen Vorgang, bei dem die Firmware mit einer digitalen Signatur versehen wird. Der Einsatzzweck dieser Signatur beschränkt sich aktuell auf die Überprüfung, ob die Firmware bzw. nachladbare Teile davon (=AVM-Plugins) aus einer vertrauenswürdigen Quelle stammen und damit geflasht bzw. nachgeladen und eingebunden werden dürfen. In Bezug auf die Firmware ist dieser Mechanismus erst seit Fritz!OS-6.5x von AVM scharf geschaltet. Seit dieser Version kann über das Standard-Web-Interface von AVM nur noch eine aus einer vertrauenswürdigen und zum Flash-Zeitpunkt der auf der Box laufenden Firmware bekannten Quelle geflasht werden.

Um zu verstehen, was der letzte Satz konkret bedeutet, sei kurz auf die Grundprinzipien des digitalen Signierens eingegangen (für tiefgehende Informationen sei auf zahlreiche Artikeln im Internet verwiesen, z.B. auf diesen Wikipedia-Artikel).

Im Rahmen des digitalen Signierens sind im wesentlichen folgende Schritte/Sachverhalte von Bedeutung:

- Die Erzeugung eines aus einem privaten und aus einem öffentlichen Schlüssel bestehenden Schlüsselpaars. Der private Schlüssel wird dabei mit einem Passwort versehen, sodass der Schlüssel nur von der Person verwendet werden kann, die im Besitz des Schlüssels ist und das Passwort dazu kennt.
- Der private Schlüssel aus dem Schlüsselpaar wird vom Absender einer digitalen Nachricht verwendet und dient dem Zweck, diese digitale Nachricht mit einer digitalen Signatur zu versehen.
- Die digitale Signatur ermöglicht es dem Empfänger der Nachricht mit Hilfe des öffentlichen Schlüssels (auch Verifikationsschlüssel genannt) die nicht-abstreitbare Urheberschaft und Integrität der Nachricht zu prüfen.

Für unseren Anwendungsfall bedeutet es nun folgendes:

- Die digitale Nachricht ist das Firmware-Image.
- Der Absender der Nachricht ist die Quelle, aus der das Firmware-Image stammt. Die Quelle muss im Besitz des gesamten Schlüsselpaars sein (also beider Schlüssel) und das Passwort kennen, mit dem der private Schlüssel geschützt ist.
- Der Empfänger der Nachricht ist die zum Zeitpunkt des Flash-Vorgangs auf der Box laufende Firmware-Version. Diese muss im Besitz des öffentlichen Schlüssels (des Verifikationsschlüssels) sein.

Ein (digital signiertes) Firmware-Image wird also dann als "aus einer vertrauenswürdigen Quelle stammend" eingestuft, wenn der öffentliche Schlüssel dieser Quelle der auf der Box laufenden Firmware bekannt ist und der Signatur-Prüfungsvorgang bestanden wird.

Der private, der geheime Schlüssel, mit dem AVM die Original-Images signiert, liegt uns aus verständlichen Gründen nicht vor (und wenn dies auch anders wäre, müssten wir auch noch das Passwort dazu kennen). Damit bleibt uns nichts anderes übrig, als es zu versuchen, ein selbstsigniertes Image zu erzeugen und die auf der Box laufende Firmware dazu zu zwingen dieses zu akzeptieren. Dabei sind folgende Hürden zu überwinden:

- Der aus mathematischer/technischer Sicht schwierigste Teil besteht darin, es zu verstehen, worin genau nun ein Signiervorgang bzw. ein Signatur-Prüfungsvorgang in der AVM-Firmware besteht? Glücklicherweise hat der (im IPPF-Forum sehr gut bekannte) Entwickler PeterPawn diesbezüglich eine super Arbeit geleistet und im Rahmen seines YourFritz-Projektes alles dokumentiert und den entsprechenden Quellcode zu Verfügung gestellt, der inzwischen auch in Freetz eingebaut ist.
- Wie oben schon mehrfach erwähnt, damit ein signiertes Image den Prüfungsvorgang besteht, muss die auf der Box laufende Firmware den öffentlichen Schlüssel der Quelle kennen. Dies ist für unser selbstsigniertes Image natürlich nicht der Fall. D.h. wir müssen es irgendwie schaffen, unseren öffentlichen Schlüssel auf die Box einzuschleusen. Haben wir dies einmal geschafft, so kann jedes weitere selbstsignierte Image über das reguläre AVM-Web-Interface geflasht werden, vorausgesetzt man verwendet genau dasselbe Schlüsselpaar zum Signieren und vergisst es nicht, den öffentlichen Schlüssel in jedes neue Image mitaufzunehmen.

Diese zweite Aufgabe ist streng genommen nicht ganz trivial. Es ist geplant, einen eigenen Artikel zu diesem Thema zu verfassen. An dieser Stelle seien stichwortartig mögliche Lösungen angedeutet:

- Ein Downgrade (mittels Recovery) auf eine ältere Firmware-Version, die noch unsignierte Images akzeptiert hat. Aus dieser älteren Firmware-Version heraus muss dann eine jüngere Firmware-Version geflasht werden, die unseren öffentlichen Schlüssel enthält.
- Hat man zufälligerweise einen Telnet-Zugang auf die Box, so kann mittels der "drüber mounten"-Methode (`mount -o bind ... ...`) eines der AVM-Schlüssel temporär durch den eigenen ersetzt werden.
- Bei NOR-Boxen kann ein den öffentlichen Schlüssel enthaltendes Image mittels push_firmware auf die Box gebracht werden.
- Bei NAND-Boxen kann ein den öffentlichen Schlüssel enthaltendes Image mittels der eva-to-memory-Methode auf die Box gebracht werden.

Konkrete Anwendung in Freetz

- Man aktiviere die Experten-Ansicht in Freetz ("Level of User Competence" = Expert).
- Unter "Firmware packaging (fwmod) options" aktiviere man die Option "Sign image" und gebe das Passwort für den privaten Schlüssel direkt dadrunter ein (das Passwort wird aus der ins Image kopierten Version der .config entfernt).
- Anschließend baue man ganz normal eine Freetz-Firmware.