Wie ein Firmwaredowngrade eines Siemens S450 SIP Handsets durchzuführen ist

Englisches Original Dokument *How To Downgrade The Firmware Version of Siemens S450 SIP Handset*
-> http://cawanblog.blogspot.com/2010/01/how-to-downgrade-siemens-s450-sip.html
von cawan - cawan[at]ieee.org
Deutsche Übersetzung - Christian Prunczak

Zwei Fragen vor weg:

1.) Warum ein Firmwaredowngrade?
Weil die neue Firmware nicht vernünftig arbeitet! (Aussetzer, Verbindungsabrüche bei Anrufen, unbeabsichtigte Neustarts.)

2.) Warum einen langen Artikel schreiben in dem es um das downgraden der S450 Firmware geht?
Weil das S450 dem Nutzer diese Möglichkeit nicht bietet, sobald die aktuellste Firmwareversion hat.
In anderen Worten: Wenn unserer Telefon nach einem Firmwareupdate nicht wie geplant arbeitet, kann dies nicht rückgängig gemacht werden.

Durch die Sammlung und Analyse der mit Etherreal aufgezeichneten Kommunikation zwischen S450 und gigaset.com, kann die Verzeichnisstruktur von gigaset.com wie folgt zusammengefasst werden.

http://gigaset.com/chagall/2/14/ ist zum Beispiel der Pfad zu einer spezifischen Firmware Version.
Es gibt eine *Hauptverzeichnis Datei (master directory file)* namens *master.bin*, welche einen weiteren Dateinamen offenbart: *baselines.bin*.
Nach öffnen der Datei *baselines.bin*, bekommen wir den exakten Dateinamen der zu ladenden Firmware.

Hier ein Beispiel:
a) Aufruf des Verzeichnisses *http://gigaset.com/chagall/2/14/*
(*Anm. d. Ü.:* Dies erzeugt eine Fehlermeldung, da der gigaset server keinen Directory index sendet. Kann aber ignoriert werden. Einfach bei b) weitermachen)

b) Aufruf der Hauptverzeichnisdatei - master.bin durch Eingabe *http://gigaset.com/chagall/2/14/master.bin* im Browser.

c) Öffne die Datei *master.bin* und hol Dir die Information, dass die nächste Datei *baselines.bin* heisst.

d) Aufruf der Datei *baselines.bin* durch Eingabe *http://gigaset.com/chagall/2/14/baselines.bin* im Browser.

e) Öffne die Datei *baselines.bin* und erhalte die Dateinamen der Firmware.
In diesem Beispiel ist dies *chagall083_02.bin.*

f) Lade die Firmwaredateien durch Aufruf von *http://gigaset.com/chagall/2/14/chagall083_02.bin*

Nun werfen wir einen Blick auf die Namenskonvention der S450 Firmware:

chagall083_02.bin -> v02083
chagall072_01.bin -> v01072
chagall184_02.bin -> v02184
chagall191_02.bin -> v02191
chagall214_02.bin -> v02214 <- Letzte Firmware vom 23-Jan-2010

Eine Liste der Firmwareversionen ist hier zu bekommen ->
http://gigaset.com/shc/0,1935,hq_en_0_123868_rArNrNrNrN_variation%253A-5_pageType%253Adownloads_imagePos%253A0,00.html (*Anm. des Ü.:* Zur Zeit der Übersetzung (10.11.2010) nicht mehr erreichbar.)

Jetzt wissen wir, wie wir den genauen Dateinamen der gesuchten Firmwareversion erhalten.

Ein Beispiel:
Sollten wir die Firmwareversion v02214 haben wollen, dann sollte der der korrekte Dateiname *chagall214_02.bin* lauten.
Nun können wir versuchen die Firmware direkt zu laden. Für *chagall214_02.bin* (v02214) sollte dies *http://gigaset.com/chagall/2/chagall214_02.bin* und für *chagall191_02.bin* (v02191) *http://gigaset.com/chagall/2/chagall191_02.bin* sein.

Falls jemand fragt warum *chagall083_02.bin* (v02083) hier *http://gigaset.com/chagall/2/14/chagall083_02.bin* und nicht hier *http://gigaset.com/chagall/2/chagall083_02.bin* lokalisiert ist, so lautet die Antwort, dass *http://gigaset.com/chagall/2/* nur die aktuellsten Firmwares beinhaltet.
Ältere Firmwareversionen werden in einen tieferen Pfad wie z.B. */14* (wie im Beispiel) geschoben.
Ist die Firmware erst einmal verschoben, dann ist ein Herantasten an die gewünschte Firmwareversion notwendig.

Schauen wir uns nun die Methoden an, die S450 Firmware auf den letzten Stand zu bringen.

1. Über das Mobilteil: *Setting->Base->Software Upgrade*

2. Über das Internet unter Nutzung der Siemens Gigaset Seite:
Gehe zu *Setting->Miscellaneous->Firmware Upgrade*
Unter "*Data Server*" ist die Standardeinstellung "*gigaset.com/chagall/*"
Unter "*User Defined Firmware*" ist dies einzugeben "*http://gigaset.com/chagall/2/chagall214_02.bin*"
Klick "*Upgrade Firmware*"

3. Über das Internet unter Nutzung unserer eigenen/lokalen Webseite
Gehe zu *Setting->Miscellaneous->Firmware Upgrade*
"*gigaset.com/chagall/*" unter "*Data Server*" ist die Standardeinstellung. (Eine Anpassung ist nicht notwendig, der Eintrag dient Selbstheilungszwecken)
Im Feld "*User Defined Firmware*" ist folgendes einzugeben (*Anm. d. Ü.:* abhängig von der IP-Adresse der eigenen Webseite/ des lokalen Webserver [e.G. Xampp]) "*http://192.168.1.1/chagall214_02.bin*" (die Datei *chagall214_02.bin* wird root-Verzeichnis von *http://192.168.1.1/* abgelegt).
Ein Klick auf "Upgrade Firmware"

Im vorigen Abschnitt war Selbstheilung erwähnt. Das Siemens S450 ist in der Lage eine sogenannte Selbstheilung durchzuführen, sollte der Firmwareupgrade Prozess fehlschlagen.
Dies basiert auf den Standardeinstellungen des S450, sich mit der Siemens Gigaset Seite (wie im Feld "*Data Server*" gezeigt) zu verbinden um die aktuellste Firmware automatisch zu laden.

Wie auch immer; ist "*User Defined Firmware*" mit einer gültigen URL (z.B. *http://192.168.1.1/chagall214_02.bin*) spezifiziert, dann überschreibt dies den "*Data Server*" um die aktuellste Firmwareversion zu laden.
Eine zusätzliche Information: Ist das Feld "*User Defined Firmware*" leer oder nicht korrekt ausgefüllt, dann benutzt das S450 Port 20 um die aktuellste Firmware von der Gigaset Seite zu übertragen.
Für alle S450 die in hinter einem NAT-Router genutzt werden, ist es notwendig ein Portforwarding auf die IP-Adresse des S450 zu setzen, um die Selbstheilungsmöglichkeit zu nutzen.

So, jetzt haben wir den wichtigsten Teil des Artikels erreicht: Wie ist ein Downgrade durchzuführen.
In meinem Fall benutze ich die Firmwareversion v02191 einige Zeit ohne Fehler.
Wie auch immer; sobald die Firmwareversion auf v02214 aktualisiert ist, kann mein S450 keinen Ruf im peer-to-peer mode an einen Asterisk Server oder Barix Annuncicom durchführen.
Jedes Mal, wenn ein Ruf initiiert wird, wird ein "*Connection Lost*" gezeigt und abgebrochen.
Die Statusmeldung lautet "*IP Status Code:701*"... Jetzt brauche ich wirklich meine v02191 zurück! Ich versuche "*http://gigaset.com/chagall/2/chagall191_02.bin*" im "*User Defied Firmware*" Feld einzutragen und klicke die "*Upgrade Firmware*" Schaltfläche. Es erscheint eine Information "*Firmware Upgrade Not Possible: Latest firmware version is already installed.*" und der Aktualisierungsvorgang bricht ab. Dann

lade ich die *chagall191_02.bin* und hinterlege diese im Rootverzeichnis meines lokalen Webservers, starte den Upgrade Prozess erneut mit "*http://192.168.1.1/chagall191_02.bin*" und erhalte den gleichen Fehler. Danach habe ich die Datei umbenannt in *chagall999_02.bin* und erhielt den gleichen Fehler.

Nacheiner Paketanalyse mit Etherreal, war mir klar, dass das S450 zuerst ein Datenpaket von *chagall191_02.bin* erhält bevor die Fehlernachricht angezeigt und der Firmwareupgradeprozess gestoppt wird.
Es ist offenkundig, dass das S450 eine Art von "*version checking*" Mechanismus für die *chagall191_02.bin* Datei hat. Ein hexadezimaler Dateivergleich zwischen *chagall191_02.bin* und *chagall214_02.bin* zeigt, das die vom Webserver zur S450 übertragenen Datensegmente nicht viele Bytes Unterschied aufzeigen.

Auf die schnelle:
Ich fand, dass im offset 0x200 der *chagall191_02.bin* 0xBF (191 Dezimal) und *chagall214_02.bin* 0xD6 (214 Dezimal) steht. Jetzt kann ich das S450 durch die Änderung von 0xBF der *chagall191_02.bin* am offset 0x200 zum 0xff, annehmen lassen, das *chagall191_02.bin* (v02191) v02255 ist.

Dann versuche ich erneut ein Upgrade der *neuen "v02255"* Firmware. Dieses Mal erhalte ich die Nachricht "*Firmware update started. The device will be disconnected and this interface terminated. The device will then shut down and restart. Once completed, you may start the interface again."* und ich kann den Start des Upgradeprozesses mit Etherreal beobachten.

Sobald das Upgrade beendet ist, kann ich die S450 ausschalten und neu starten. Dann versuche ich die S450 mit dem Browser zu erreichen, erhalte aber keine Antwort! Es scheint, dass die S450 die Datenintegrität der Firmware mit einer Art Prüfsumme absichert. Danach setze ich ein *ping* auf die S450 und erhalte eine Antwort von Ihr (ich nehme an das Ladeprogramm existiert fortwährend um Selbstheilung zu gewährleisten). Nun ersetze ich die editierte *chagall191_02.bin* mit der originalen auf meinem Webserver. Dann starte ich meine S450 erneut. Über Etherreal kann ich sehen, dass die S450 die originale *chagall191_02.bin* von meinem Server lädt. Mit anderen Worten: der sog. "*firmware download*" Prozess ist gerade gestartet! Einmal beendet starte ich die S450 erneut und bekomme Zugriff auf die Benutzeroberfläche. Schließlich schaue ich auf "*Status*" und mir wird die Version 0219100000 angezeigt. Mein Firmware downgrade Prozess ist abgeschlossen.

Das ist dass ganze Prozedere um die Firmware eines Siemens S450 downzugraden.
Nachmachen geschieht auf eigene Gefahr!