

Thursday, August 13. 2015

## Warum Auto-Hacks absehbar sind

Als hÄtte ich es geahnt... Volkswagen hat massive Sicherheitsprobleme und verhÄllt sie anstatt sie zu lÄsen.

Seit drei Jahren ist Volkswagen bekannt dass SchlÄssel fÄr ihre Autos und deren "Security" trivial zu brechen sind. Brechen weil - wie bei Mifare Classic (der Vergleich drÄngt sich einfach auf) - viele einfache Sicherheits-Schranken erst gar nicht gesetzt wurden. Der Pool an Zufallszahlen ist viel zu klein, es gibt keine BeschrÄnkung der Anmeldeversuche, der Halter des Wagens wird gar nicht Äber Fehlversuche informiert (wenn da 1000 stehen kÄnnte er sich ja Gedanken machen) und so weiter.

Wenn das Auto gestohlen wird, geht dann natÄrlich die Versicherung davon aus dass der Halter den SchlÄssel liegengelassen hat. Oder der Dieb anders dran kam; weil es gibt ja keine Einbruchsspuren. Der Halter mÄsste also beweisen dass noch alles in Ordnung ist bei ihm; die Umkehrung der Unschuldsvermutung.

Das perfide ist aber: Volkswagen weiss das seit drei Jahren. Und anstatt was zu machen haben sie die Forscher gezwungen, ihre Forschungsergebnisse zurÄckzuhalten. Das heisst, Diebe haben seit drei Jahren leichtes Spiel. Wurde in den drei Jahren etwas gemacht? Wurden die SchlÄssel und die entsprechenden Sicherheitssysteme in den anfÄlligen Autos getauscht?

Nein. Warum auch? Es gibt keinen Aufschrei.

Und genau deswegen sollte Security by Obscurity verboten sein. Ich weiss nicht, wieviele Autos inzwischen als gestohlen gemeldet wurden aus diesen Fahrzeugreihen, aber es wurde den Dieben ziemlich einfach gemacht...

Posted by rince in CCCS at 11:32

Wednesday, August 12. 2015

### Hacks an Autos sollen zu schwer sein...

Heute las ich einen Artikel, dass Sicherheitsforscher der Meinung sind dass Auto-Hacks schwer zu kopieren sind.

Meine Erfahrungen gehen in die andere Richtung: Alles wird versucht zu vereinheitlichen innerhalb eines Konzerns, um Synergie-Effekte zu haben. Das bedeutet dass dieselben Komponenten (Hard- aber auch Software) Ä¼berall benutzt werden.

Und weil "Security by Obscurity" so gut funktioniert wird erwartet dass "weil ja niemand etwas weiss" alles sicher ist. Selbst wenn "nur" das Auto raustelefonieren darf - was hindert mich daran, von innen eine TCP-Verbindung aufzumachen und stehenzulassen? Okay, ich brauche eventuell physischen Zugriff. Oder ein speziell angepasstes mp3-StÄ¼ck welches ich dem Inhaber des Autos mitgebe. Standard-Libraries (Open Source) haben den Vorteil dass sie fÄ¼r Firmen kostenlos zu benutzen sind und daher auch gerne eingesetzt werden. Wohin das fÄ¼hrt sah man schon bei vielen snmp-Bugs, wo plÄ¼tzlich Hersteller wie Cisco, Juniper, ... alle auffÄ¼llig zeitgleich ihre Systeme patchen mussten.

Also sorry, ich glaube nicht dass es ausreicht sich darauf zurÄ¼ckzuziehen, dass es zu schwer wird oder es sich nicht lohnt.

Posted by rince in CCCS at 10:18

Tuesday, August 11. 2015

## Wie man Katastrophen abwendet, heute: LÄ¶schen von LUKS-SchlÄ¶sseln

Ich bin deutlich zu experimentierfreudig.

Ich habe vor einiger Zeit meinem Laptop beigebracht, die verschlÄ¶sselte LUKS-Partition nicht nur Ä¶ber eine Passphrase, sondern auch Ä¶ber eine (andere) Passphrase, gepaart mit meinem Yubikey zu entschlÄ¶sseln.

Das hat sich heute gerÄ¶cht, weil ich den Yubikey fÄ¶r andere Zwecke umkonfiguriert hatte. Ich dachte dann, diesen Slot in LUKS iÄ¶schst Du mal.

DafÄ¶r muss man immer noch ein funktionierendes Passwort angeben.

Dumm nur: Es wurde das Passwort gelÄ¶scht welches ich eingegeben hatte. Ganz dumme Geschichte - damit wÄ¶re beim nÄ¶chsten hochfahren das System nicht mehr hochgekommen, weil kein EntschlÄ¶sselungs-SchlÄ¶ssel mehr bereit gewesen wÄ¶re; den initialen hatte ich gerade gelÄ¶scht und der Yubikey hatte andere Werte.

Was tun fragte ich mich, besonders weil eine Suchmaschinen-Suche auf diese Fragestellung keine eindeutige Antwort gab. Ich sah mich schon alles Backuppen, formatieren und restoren (oder - wenn ich gut drauf gewesen wÄ¶re - neues Device mit luks anlegen, dd if.. of ... von A nach B schieben).

Mein GlÄ¶ck ist, dass das Laufwerk ja noch online und damit geÄ¶ffnet ist. Auch der Master-Key ist (fÄ¶r root) auslesbar.

Zugschluss ist gerade auf der DebConf und hat Margarita ManterolagegenÄ¶ber sitzen. Und sie kennt luks sehr gut. Ich weiss nicht ob sie aus Erfahrung spricht, aber sie hat den richtigen Tip gehabt:

```
# cryptsetup luksAddKey $device_name --master-key-file
```

Posted by rince at 17:34

Thursday, August 6. 2015

## Das neue Informationsfreiheitsgesetz des Landes Baden-WÄ¼rttemberg - und die Kommentare

Baden-WÄ¼rttemberg rÄ¼hmt sich, bÄ¼rgerfreundlich und bÄ¼rgernah zu sein. Trotzdem gibt es bisher kein Informationsfreiheitsgesetz wie es der Bund und fast alle anderen BundeslÄ¼nder bereits hat.

Dies mÄ¼chte die Landesregierung Ä¼ndern und hat durch das Innenministerium einen Entwurf zu dem IFG vorgelegt, den man auch kommentieren darf. Sehr lÄ¼blich.

Wenn man allerdings kommentieren mÄ¼chte soll man sich registrieren. Das heisst, man schreibt einen Text, drÄ¼ckt auf "Vorschau" - und dann soll man sich plÄ¼tzlich anmelden.

Na gut.

Also eine Mailadresse generieren, ein PaÄ¼wort sich ausdenken und ins Keepass werfen, auf die BestÄ¼tigungsmail warten, Link anklicken zur BestÄ¼tigung und hoffen dass das kein Phishing war (Digitale Unterschrift ist ja sowas von gestern...).

Danach kann ich mich mit meinem selbstgewÄ¼hlten PaÄ¼wort einloggen.

Und heiÄ¼e da erst einmal "Ohne Namen 28180". So soll mein Kommentar abgeschickt werden.

Finde ich nicht gut, also mÄ¼chte ich meinen Namen Ä¼ndern. Ganz rechts oben auf der Webseite ist inzwischen auch ein neuer Punkt zum Anklicken - "Mein Profil".

Hey, gut! Ich darf mein Profil Ä¼ndern! Was steht denn da Ä¼ber mich drin?

Positiv: Nur mein Name und eine MÄ¼glichkeit das PaÄ¼wort zu Ä¼ndern.

Ich Ä¼ndere meinen Namen.... aber wo kann ich bitte das ganze speichern?

AuflÄ¼sung: Rechts unten die Werbung wegklicken und man findet auf einmal den Knopf.

Posted by rince at 10:11