Donnerstag, 13. August 2015

Warum Auto-Hacks absehbar sind

Als hÃ¤tte ich es geahnt... Volkswagen hat massive Sicherheitsprobleme und verhÃ¼llt sie anstatt sie zu lÃ¶sen.

Seit drei Jahren ist Volkswagen bekannt dass SchlÃ¼ssel fÃ¼r ihre Autos und deren "Security" trivial zu brechen sind. Brechen weil - wie bei Mifare Classic (der Vergleich drÃ¤ngt sich einfach auf) - viele einfache Sicherheits-Schranken erst gar nicht gesetzt wurden. Der Pool an Zufallszahlen ist viel zu klein, es gibt keine BeschrÃ¤nkung der Anmeldeversuche, der Halter des Wagens wird gar nicht Ã¼ber Fehlversuche informiert (wenn da 1000 stehen kÃ¶nnte er sich ja Gedanken machen) und so weiter.
Wenn das Auto gestohlen wird, geht dann natÃ¼rlich die Versicherung davon aus dass der Halter den SchlÃ¼ssel liegengelassen hat. Oder der Dieb anders dran kam; weil es gibt ja keine Einbruchsspuren. Der Halter mÃ¼sste 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 zurÃ¼ckzuhalten. Das heisst, Diebe haben seit drei Jahren leichtes Spiel.
Wurde in den drei Jahren etwas gemacht? Wurden die SchlÃ¼ssel und die entsprechenden Sicherheitssysteme in den anfÃ¤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...

Geschrieben von rince in CCCS um 11:32

Mittwoch, 12. August 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) Ã¼berall 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-StÃ¼ck welches ich dem Inhaber des Autos mitgebe. Standard-Libraries (Open Source) haben den Vorteil dass sie fÃ¼r Firmen kostenlos zu benutzen sind und daher auch gerne eingesetzt werden. Wohin das fÃ¼hrt sah man schon bei vielen snmp-Bugs, wo plÃ¶tzlich Hersteller wie Cisco, Juniper, ... alle auffÃ¤llig zeitgleich ihre Systeme patchen mussten.
Also sorry, ich glaube nicht dass es ausreicht sich darauf zurÃ¼ckzuziehen, dass es zu schwer wird oder es sich nicht lohnt.

Geschrieben von rince in CCCS um 10:18

Dienstag, 11. August 2015

Wie man Katastrophen abwendet, heute: LÃ¶schen von LUKS-SchlÃ¼sseln

Ich bin deutlich zu experimentierfreudig.

Ich habe vor einiger Zeit meinem Laptop beigebracht, die verschlÃ¼sselte LUKS-Partition nicht nur Ã¼ber eine Passphrase, sondern auch Ã¼ber eine (andere) Passphrase, gepaart mit meinem Yubikey zu entschlÃ¼sseln.

Das hat sich heute gerÃ¤cht, weil ich den Yubikey fÃ¼r andere Zwecke umkonfiguriert hatte. Ich dachte dann, diesen Slot in LUKS lÃ¶schst Du mal.

DafÃ¼r muss man immer noch ein funktionierendes Passwort angeben.
Dumm nur: Es wurde das Passwort gelÃ¶scht welches ich eingegeben hatte. Ganz dumme Geschichte - damit wÃ¤re beim nÃ¤chsten hochfahren das System nicht mehr hochgekommen, weil kein EntschlÃ¼sselungs-SchlÃ¼ssel mehr bereit gewesen wÃ¤re; den initialen hatte ich gerade gelÃ¶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 wÃ¤re - neues Device mit luks anlegen, dd if.. of ... von A nach B schieben).

Mein GlÃ¼ck ist, dass das Laufwerk ja noch online und damit geÃ¶ffnet ist. Auch der Master-Key ist (fÃ¼r root) auslesbar.

Zugschlus ist gerade auf der DebConf und hat Margarita ManterolagegenÃ¼ber 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

Geschrieben von rince um 17:34

Donnerstag, 6. August 2015

Das neue Informationsfreiheitsgesetz des Landes Baden-WÃ¼rttemberg - und die Kommentare

Baden-WÃ¼rttemberg rÃ¼hmt sich, bÃ¼rgerfreundlich und bÃ¼rgernah zu sein. Trotzdem gibt es bisher kein Informationsfreiheitsgesetz wie es der Bund und fast alle anderen BundeslÃ¤nder bereits hat.
Dies mÃ¶chte die Landesregierung Ã¤ndern und hat durch das Innenministerium einen Entwurf zu dem IFG vorgelegt, den man auch kommentieren darf. Sehr lÃ¶blich.
Wenn man allerdings kommentieren mÃ¶chte soll man sich registrieren. Das heisst, man schreibt einen Text, drÃ¼ckt auf "Vorschau" - und dann soll man sich plÃ¶tzlich anmelden.
Na gut.
Also eine Mailadresse generieren, ein PaÃŸwort sich ausdenken und ins Keepass werfen, auf die BestÃ¤tigungsmail warten, Link anklicken zur BestÃ¤tigung und hoffen dass das kein Phishing war (Digitale Unterschrift ist ja sowas von gestern...). _Danach_ kann ich mich mit meinem selbstgewÃ¤hlten PaÃŸwort einloggen.
Und heiÃŸe da erst einmal "Ohne Namen 28180". So soll mein Kommentar abgeschickt werden.
Finde ich nicht gut, also mÃ¶chte ich meinen Namen Ã¤ndern. Ganz rechts oben auf der Webseite ist inzwischen auch ein neuer Punkt zum Anklicken - "Mein Profil".
Hey, gut! Ich darf mein Profil Ã¤ndern! Was steht denn da Ã¼ber mich drin?
Positiv: Nur mein Name und eine MÃ¶glichkeit das PaÃŸwort zu Ã¤ndern.
Ich Ã¤ndere meinen Namen.... aber wo kann ich bitte das ganze speichern?

AuflÃ¶sung: Rechts unten die Werbung wegklicken und man findet auf einmal den Knopf.

Geschrieben von rince um 10:11