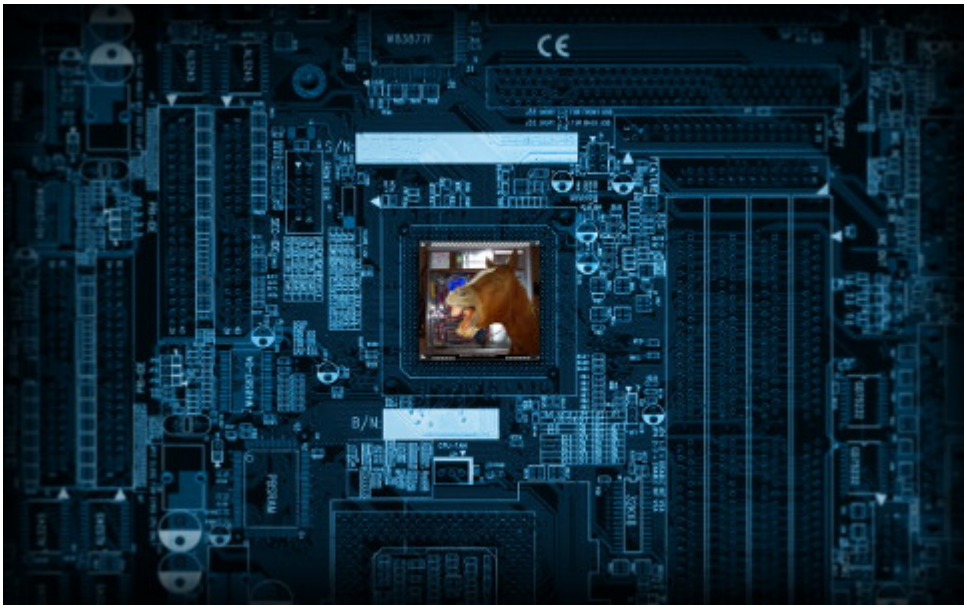
Mit psychologischen Tricks trojanische Pferde reinreiten



Heise über einen so genannten „Trojaner“ für Android, der in Wahrheit ein „Trojanisches Pferd“ ist (weil die Trojaner bekanntlich in Troja saßen und nicht *im* Pferd):

Um sein Opfer anzugreifen, muss der Hacker dieses allerdings dazu bringen, die Software zu installieren. Das geschieht in der Regel mit psychologischen Tricks wie dem Vorwand, Viren hätten das Handy befallen. Die Angreifer geben den Trojaner aber auch als Apps für soziale Netzwerke aus.

Recht so. Am besten noch diesen Pappnasen das Betriebsystem ganz zerschießen. Mein Mitleid hält sich in sehr engen Grenzen. Wenn ich „Apps für soziale Netzwerke“ schon lese, dann krieg ich das kalte Grausen.

Crypto is the Chicken Soup in Plain English

Peter Gutman, „computer scientist in the Department of Computer Science at the University of Auckland, Auckland, New Zealand“, hat etwas publiziert (pdf, via Fefe) über die Schwachstellen gängiger kryptografischer Implementationen und das Computerproblem, das zwei Ohren hat und vor einem Monitor sitzt.

Er lässt sich unter anderem aus über Amazon Kindle 2, Motorola und
Samsung Galaxy Handys, Nikon und Canon Kameras, Android code signing, iPhone/iPad/iOS („lets of security measures, too many to cover here“), Windows 8 UEFI (das ärgert mich sowieso schon seit langem) usw..

Natürlich ist jemand wie Gutman, der sich wirklich auskennt, kein Defätist. Er macht nur noch einmal klar, dass man nicht auf Technik oder Software allein vertrauen sollte: Vertrauen ist gut, Kontrolle ist aber besser.

Auf jeden Fall lesenswert, auch wegen des schwarzen Humors und der lässigen Sprache, den man auf Folien eines Deutschen zu einem solchen Thema so nicht finden würde.

No way back?

Urteil des europäischen Gerichtshofes: „An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties“.
Eine Person kann sich daher, wenn bei einer anhand ihres Namens durchgeführten Suche in der Ergebnisliste ein Link zu einer Internetseite mit Informationen über sie angezeigt wird, unmittelbar an den Suchmaschinenbetreiber wenden, um unter bestimmten Voraussetzungen die Entfernung des Links aus der Ergebnisliste zu erwirken, oder, wenn dieser ihrem Antrag nicht entspricht, an die zuständigen Stellen.

Bin mal gespannt, was Internet Archive: Wayback Machine dazu sagt.

Keine Gefahr, gehen sie weiter!

„Eine Gefahr für die deutsche Wirtschaft durch den US-Geheimdienst NSA sehen Regierung und Inlandsgeheimdienst dagegen nicht.“

Privacy Badger

Heise: Die Electronic Frontier Foundation (EFF) habe ein Browser-Plugin vorgestellt, das Cookies von Drittwebseiten blocken soll, die sich nicht an Do Not Track Header halten.

Ich blocke sowieso Cookies, da ich nicht davon ausgehe, dass sich irgendjemand an irgendetwas hält. („Der W3C konnte bislang noch keinen Konsens zwischen der Werbeindustrie und der Federal Trade Commission in den USA herstellen“) Vertrauen ist gut, Kontrolle ist besser, sagte schon jemand, der es wissen muss.

If an advertiser seems to be tracking you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading any more content in your browser. To the advertiser, it’s like you suddenly disappeared.

Angesichts meiner „per default“ Browser-Eiinstellungen scheint mir dieser „Privacy Badger“ eher Overkill zu sein. Aber schaden kann es nicht, das Add-on trotzdem zu installieren.

Acht Mythen zur Vorratsdatenspeicherung

Thomas Stadler (via Hal): „Acht Mythen zur Vorratsdatenspeicherung“.

Tatsächlich gibt es in keinem einzigen EU-Mitgliedsstaat (empirische) Belege dafür, dass die Vorratsdatenspeicherung zu einer erhöhten Aufklärungsquote geführt hat, obwohl sie in den meisten EU-Staaten über viele Jahre hinweg praktiziert worden ist. (…)

In einem Rechtsstaat gibt es keine Strafermittlung um jeden Preis. Darin besteht nämlich gerade der Unterschied zu Unrechtsstaaten wie der DDR, die jede Form der Überwachung und Kontrolle des Bürgers für legitim hielten. Der Rechtsstaat muss auf eine Totalüberwachung verzichten und damit evtl. einhergehende Defizite bei der Kriminalitätsbekämpfung in Kauf nehmen.

Augmented Reality

Die Vor- und Nachteile, Risiken und Nebenwirkungen von Augmented Reality via Google Glass beschreibt ein Nutzer im Heise-Forum. „Augmented Reality ist das Ende JEGLICHER Privatsphäre.“ Lesenswert!

Truecrypt, reloaded

iSEC Research Labs hat einen kommerziellen Audit von TrueCrypt vorgelegt (via Fefe, der schon vor einem Jahr mit einigen Verschwörungstheorien dazu aufgeräumt hatte.) Außer einigen nicht relevanten „Code quality issues“ und den schon bekannten Bootloader-Schwachpunkten haben die keine Angriffspunkte gefunden (vgl. „Vulnerability Overview“):

The code to decompress the main bootloader suffers from several implementation weaknesses. Throughout the source code, signed and unsigned integer types are mixed, arrays are accessed without checking if the index is within bounds, and so forth.

Das ist doch mal eine gute Nachricht.

Der beste Schutz: die Verschlüsselung aller Kommunikation

Heise: „Europarat hört Whistleblower Snowden an“.

Deutsche Bürger sowie Internetseiten seien täglich Ziel der Ausspähung durch die NSA-Experten. (…) Die deutschen Dienste gehören nach Angaben des Whistleblowers neben den Niederlanden und Schweden zu den Hauptzielen von speziellen NSA-Kampagnen. (…) Snowden hält ein internationales Verbot von anlassloser Überwachung für ein wichtiges Ziel, brachte aber gleichzeitig seine Sorge zum Ausdruck, dass selbst in einer perfekten Welt der beste Schutz die Verschlüsselung aller Kommunikation sei.

Wieso kriege ich immer noch unverschlüsselte E-Mails?

Vorratsdatenspeicherung vorerst gestoppt

Entscheidung des Gerichtshofes der Europäischen Union (pdf): „Der Gerichtshof erklärt die Richtlinie über die Vorratsspeicherung von Daten für ungültig. Sie beinhaltet einen Eingriff von großem Ausmaß und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, der sich nicht auf das absolut Notwendige beschränkt.“

PGP für den Boulevard

Die Boulevard-Zeitung Berliner Kurier von heute. Ich bezweifele, dass solche Artikel irgendetwas nutzen.

Im November letzten Jahres schrieben die zum Beispiel: „Eine OpenPGP-Umsetzung fürs Smartphone bietet etwa die Anwendung Android Privacy Guard (APG), die mit der E-Mail-App K-9 Mail zusammenarbeitet.“

So schreibt man keine Anleitungen – sogar ich habe bei dem Thema tagelang herumgefummelt. Die Nutzer müssen wissen, was auf sie zukommt und was alles schiefgehen kann und wie lange es dauert, bis man es umgesetzt hat. Ich glaube auch nicht, dass irgendjemand eine Krawall-Zeitung nimmt, um zu lernen, wie man verschlüsselt.

BKA-trojanhorse.exe Is an

Unknown Application. Install Anyway?

Heise: „Hoffnungen setzte der Generalbundesanwalt auch auf einen einsatzfähigen Trojaner, den das Bundeskriminalamt derzeit entwickele und Ende 2014 in Gebrauch nehmen werde.“

Muahahaha. Und wie wollen die den implementieren? Aber das hatten wir hier schon…

INPOL-neu, revisited

Stern.de: „BKA-Beamte schnüffelten unerlaubt Kollegen hinterher (…) Nach stern-Informationen haben mehrere Mitarbeiter seit Anfang 2012 ihrem damaligen Kollegen D. hinterherspioniert – ohne dienstrechtliche Konsequenzen.“

Kann man etwas missbrauchen, wird es auch missbraucht.

Quasi keine Möglichkeit [Update]

„Wen die NSA im Visier hat, dessen Computer kann sie gezielt und umfassend überwachen – und es gibt quasi keine Möglichkeit, sich dagegen zu wehren.“ Ach ja, Spiegel online? Was raucht ihr da eigentlich? Oder seid ihr einfach nur abgrundtief dämlich und ignorant? PGP? Truecrypt? Tor? Nie

gehört? Sorry, aber über solche Dummschwätzer rege ich mich auf.

[Update] ich halte die Die-sind-ja-eh-scho-ndrin-man-kann-nichts-machen-Schwätzer für genauso schlimm wie die Überwachungs-Lobbby selbst. Vermutlich werden jene auch von diesen bezahlt.

Eigenartig

„So besuchte der SPD-Mann [Edathy] am 18. Mai 2007 das BKA in Wiesbaden, wo er um 14 Uhr mit Behördenchef Ziercke zusammentraf. (…) Bei der mehrtägigen Reise ging es laut einer Bundestags-Pressemitteilung „um die Balance zwischen Sicherheitsinteressen-Wahrnehmung und Grundrechtssicherung“ – also wohl auch um die damals besonders umstrittene Vorratsdatenspeicherung … […] Wurde Edathy bei diesem Besuch auch über die Sorgen und Nöte des BKA-Referats SO 12 informiert, das mit den Ermittlungen im Bereich Kinderpornografie im Internet betraut ist? Darauf gibt es einen Hinweis, der Spiegel online vorliegt und plausibel erscheint. Das BKA hatte mit diesem Thema stets die Notwendigkeit der Vorratsdatenspeicherung gerechtfertigt. Eigenartig: Eine Anfrage zu den Inhalten des Edathy-Besuchs in Wiesbaden wollte das BKA nicht beantworten.“

Edathy unterstützte 2007 das 2010 für verfassungswidrig erklärte Gesetz zur Vorratsdatenspeicherung.

WorldIP

Ich habe mir das Firefox-Add-on WorldIP installiert (Website): „The real location of web server and extended information about datacenter. Advanced Networking Tools. Anti-phishing solution. Security features against DNS spoofing and fake websites.“

WorldIP add-on is created to protect the user. We respect your privacy! and do not sell or pass your personal information to third parties.
1) Cookies
WorldIP add-on does not send any cookies to any web server.
2) Geolocation and Datacenter Databases
To display up-to-date information about physical location of a web server and data center, the WorldIP add-on uses API, it sends the requested IP addresses to api.wipmania.com. The format of API-request is IP-addr?hostname. To prevent the use of API from the name of add-on, we check that IP and hostname accord with each other.
Any other information about the site or user will not be sent to WIPmania, except for its domain name, that says about its IP address. IP addresses will be also used to correct the database. WIPmania do not collect any personal information

about visitors.

Gefällt mir.

Terrorscore

Quelle: Terrorscore

Bananenbundesrepublik

Deutschland, revisited

„Germany was pressured to modify its G-10 law to appease the NSA, and it eroded the rights of German citizens under their constitution.“ (Edward Snowden)

Verschlüsselungszwang verunsichert manche Mail-Nutzer

Heise: „Verschlüsselungszwang verunsichert manche Mail-Nutzer“.

Burks gefällt das.

S/MIME [Update]

S/MIME-Anleitungen (zip-Datei, von „Anti-Prism-Party„) zum Download:
– auf dem PC (unter Windows mit Outlook und Thunderbird, auf

dem Mac mit Thunderbird und unter Linux mit Thunderbird), unter Android und unter iOS.
[Update] Link repariert