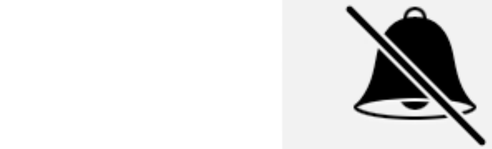
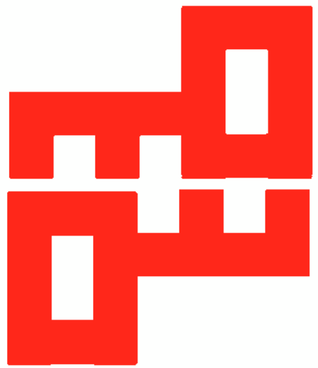



CRYPTO
PARTY

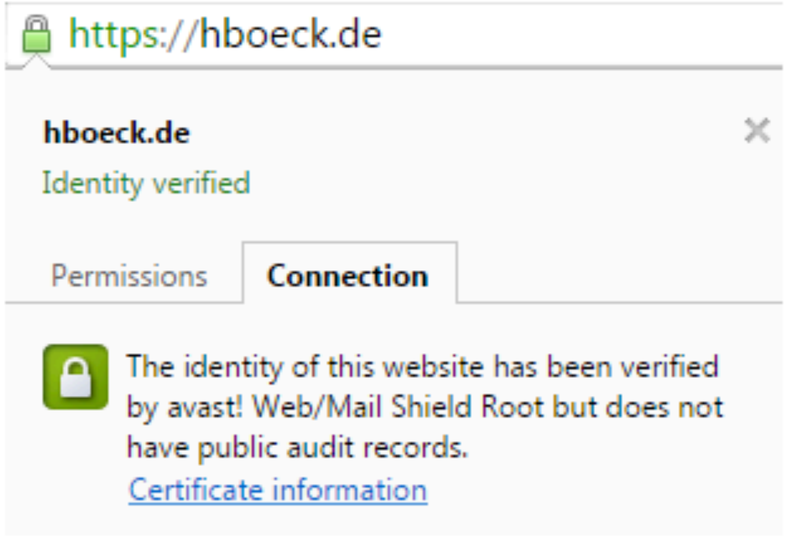


32


TU
WIEN

Ergänzungen…

How Kaspersky makes you vulnerable to the FREAK attack and other ways Antivirus software lowers your HTTPS security



Lately a lot of attention has been payed to software like Superfish and Privdog that intercepts TLS connections to be able to manipulate HTTPS traffic. These programs had severe (technically different) vulnerabilities that allowed attacks on HTTPS connections.

What these tools do is a widespread method. They install a root certificate into the user's browser and then they perform a so-called Man in the Middle attack. They present the user a certificate generated on the fly and manage the connection to HTTPS servers themselves. Superfish and Privdog did this in an obviously wrong way, Superfish by using the same root certificate on all installations and Privdog by just accepting every invalid certificate from web pages. What about other software that also does MitM interception of HTTPS traffic?

Antivirus software intercepts your HTTPS traffic

Many Antivirus applications and other security products use similar techniques to intercept HTTPS traffic. I had a closer look at three of them: Avast, Kaspersky and ESET. Avast enables TLS interception by default. By default Kaspersky intercepts connections to certain web pages (e. g. banking), there is an option to enable interception by default. In ESET TLS interception is generally disabled by default and can be enabled with an option.

About me
Informationen über meine Arbeit als freier Journalist finden Sie hier.

Hanno Böck
mail: **hanno@hboeck.de**
jabber: **hanno@hboeck.de**
gpg: BBB51E42
ssh: RSA

Hanno on Google+
Hanno on Twitter
Hanno on identi.ca

Impressum

Tags
aiglx asia asia2013 atomkraft bahn berlin blog bundestag cacert ccc china co2 compiz copyright creativecommons cryptography datenschutz demonstration demoscene encryption english entropia esoterik ffmpeg film freeculture freesoftware games gentechnik gentoo gps

Achim Barczok

Das Offene

Firefox OS: offenes System, Apps in HTML5 programmieren, günstige Smartphones

Mozilla hat seinen Firefox-Browser in ein Betriebssystem für Smartphones verwandelt. Firefox OS ist Open Source und erlaubt jedem, es mitzugestalten.

Firefox OS überträgt Mozillas Idee eines Open-Source-Browsers in die Welt der Smartphones. Wer HTML5 und JavaScript spricht, kann an dem Open-Source-Projekt sogar teilnehmen und sein mobiles Betriebssystem selbst mitentwickeln. Hier kann man tatsächlich tief unter die Haube schauen und beispielsweise mal eben die virtuelle Tastatur anpassen, wenn einem eine Taste fehlt. Firefox OS stellen noch verschiedene Farbfilter verwenden, das Adressbuch importiert Kontakte aus unterschiedlichen Quellen, synchronisiert sie aber nicht. Das System führt einen getrennten Speicher für Apps, der auf den meisten Geräten nur 1 GByte groß ist und nicht per SD-Karte erweitert werden kann.

Wer sich mit Webtechniken auskennt, kann eigene Apps entwickeln. Sogenannte „Hosted

Firefox OS erinnert mit seiner schlichten Optik an frühere Android-Versionen.

haben einen tieferen Zugriff auf die Smartphone-Funktionen.

Mozilla hat einen Marketplace für Apps eingerichtet. Bisher gibt es dort vor allem kostenlose Anwendungen, die die mobilen An-

Dropbox und Instagram gibt es für Firefox OS nicht.

Ausblick

Mozilla hat sich mit mächtigen Verbündeten zusammengetan: Mobilfunkanbieter wie Telefonica oder die Deutsche Telekom verkaufen die eher günstigen Smartphones vor allem in Südamerika, Asien und Osteuropa in ihren Shops.

Es gibt inzwischen aber auch in Deutschland ein paar Modelle zu kaufen, alle im Einsteiger-Segment bis 150 Euro. Trotz der Unterstützung der Provider hat man das Gefühl, dass Mozilla und vor allem den Geräteherstellern ein bisschen der Schwung ausgegangen ist. Die meisten Smartphones laufen noch mit dem ein Jahr alten Firefox OS 1.3, die Nachfolgerversion 1.4 ist offiziell für keines verfügbar. Updates rüsten immer noch Funktionen nach, die man eigentlich

Keywan Tonekaboni

Das Anpassbare

Sailfish OS: Smarte Gestensteuerung, Code und Hardware anpassen erlaubt

Die Oberfläche von Sailfish OS sieht schick aus und wird über Gesten bedient. Unter der Haube steckt ein vollwertiges Linux mit Root-Zugriff – ein Traum für Bastler. Dennoch laufen Android-Apps fast ohne Einschränkungen und Out-of-the-Box.

Steven Elop krempelte Nokia 2011 komplett um: Künftig sollten Nokia-Smartphones nur noch mit Windows Phone laufen, andere Betriebssysteme warf er kurzerhand über Bord. Das missfiel vielen Mitarbeitern, die ihre jahrelange Arbeit am Linux-basierten Betriebssystem MeeGo nicht aufgeben wollten. Sie starteten unter dem Namen Jolla eine eigene Firma und kombinierten die Open-Source-Komponenten von MeeGo und das Community-Projekt Mer zu einem neuen Betriebssystem, Sailfish OS. Ende 2013 feierte das Jolla Phone Premiere, das erste Smartphone mit Sailfish OS.

Sailfish OS will anders sein; nicht nur optisch, sondern auch bei der Bedienung, die stark auf Gesten setzt: Ein Wisch von der Seite der Bildschirmkante minimiert die laufende Anwendung, einer von oben beendet sie. Wischt man von unten in den Bildschirm, so erscheint die Nachrichtenzentrale. Zur Navigation innerhalb der Apps und auf dem Homescreen wischt man innerhalb des Bildschirms und nicht vom Rand. Jolla hat viele clevere Details eingebaut, die beispielsweise das Wechseln zwischen Apps erleichtern, ohne dass man sie gleich schließen muss.

Minimierte Apps erscheinen auf dem Homescreen als Kacheln, zeigen Status-Informationen und laufen weiter, solange genügend Speicher vorhanden ist. Man kann sie minimiert sogar weiter bedienen, denn auch die Kacheln unterstützen kleine Interaktionen durch Wischen. Der Musik-Player beispielsweise startet oder pausiert mit einem Wisch nach rechts und springt mit einer Bewegung nach links zum nächsten Titel.

Im offiziellen Jolla Store gibt es zwar nur ein paar hundert Anwendungen, aber Jolla bietet mit Alien Dalvik eine eigene Laufzeitumgebung für Android-Apps. Diese laufen ohne Anpassungen ebenso schnell wie unter Android bei gleichwertiger Hardware. Dazu lädt man einfach die Installations-Datei der App (APK) oder installiert sich alternativ einen Android-App-Store. Die Shops Yandex und Aptoide gibt es direkt im Jolla Store, manuell bekommt man auch F-Droid oder die Google Dienste inklusive Google Play Store (als Gapps-Paket für Cyanogenmod) auf sein Jolla Phone. Daneben gibt es mit den Open-Repos und Warehouse auch Paketquellen für die Linux-Softwareverwaltung.

Um vorhandene Android-Treiber auch für Sailfish OS nutzen zu können, hat Jolla die Kompatibilitäts-Bibliothek libhybris entwickelt. Dadurch kann Sailfish OS zumindest theoretisch auf jedem üblichen Android-Gerät laufen. In der Praxis muss man aber deutliche Einschnitte in Kauf nehmen, wie eine Tabelle im Mer-Wiki zeigt (siehe c't-Link). Im November fährte Jolla eine erfolgreiche Crowdfunding-Kampagne für ein Tablet durch. Dieses soll im Mai mit Sailfish OS 2.0 ausgeliefert werden.

Auf dem Homescreen laufen Apps in einer Mini-Ansicht weiter und können darüber gesteuert werden.

Die Anzahl nativer Apps im Jolla Store ist gering, man kann aber auch Android-Apps installieren.

Spielwiese für Bastler

Wer gerne selbst am Code frickelt und sich mit Linux auskennt, schätzt den leichten und offenen Zugriff aufs System. Root ist man mit nur einem Knopfdruck in den Einstellungen und kann sich danach in der Terminal-App oder per SSH über USB oder WLAN austoben. Linux-Nutzer finden bekannte Tools wie Systemd, bash, oder rpm. Anders als bei Android, iOS oder Windows Phone passt man sein Betriebssystem dadurch auch an tieferen Stellen selbst an, installiert eigene Tastaturlayouts oder benötigte Pakete für den Linux-Unterbau einfach händisch. Auch kleinere Fehler im Betriebssystem beseitigt man so einfach selbst, statt auf die Updates des Herstellers warten zu müssen.

Die Community tauscht Tipps und Tricks auf der offiziellen Plattform together.jolla.com, wo auch Jolla-Mitarbeiter mitdiskutieren und Lösungsvorschläge für Updates übernehmen. Aber auch das aus alten Nokia-Zeiten bestehende Forum talk.maemo.org wird von der Sailfish-Community mitgenutzt, denn nicht wenige alte Maemo- und MeeGo-Nutzer haben jetzt auch ein Jolla-Smartphone.

Hardware

Das einzige Smartphone von Jolla ist vergleichbar mit günstigeren Android-Modellen. Es heißt Jolla Phone, kostet 250 Euro und glänzt nicht gerade bei den Spezifikationen – lässt sich im Alltag aber gut nutzen (einen ausführlichen Test finden Sie über den c't-Link unten). Jolla hat es zudem seit Verkaufsstart mit fast monatlichen Updates versorgt. Eine Besonderheit am Jolla Phone sind die Strom- und Datenanschlüsse auf der Rückseite für die erweiterbaren Wechsel-Cover. Jolla selbst lässt die Idee als Accessoire ohne Funktion verkommen, aber die Community hat darüber unter anderem schon Solar-Ladepanels, ein zusätzliches OLED-Display auf der Rückseite und eine Hardware-Tastatur realisiert.

Für Bastler, trotzdem komfortabel

Wer Google, Apple und Microsoft meiden möchte und dennoch beliebte Apps nutzen will, findet in Sailfish OS eine ungewöhnliche und zugleich Alltagstaugliche Alternative. Linux-Kenner können darüber hinaus auch unter der schönen Oberfläche nach Belieben stöbern.

(acb@ct.de)

ct Mer-Wiki und Test Jolla Phone: ct.de/ykb1

Achim Barczok

Das Offene

Firefox OS: offenes System, Apps in HTML5 programmieren, günstige Smartphones

Mozilla hat seinen Firefox-Browser in ein Betriebssystem für Smartphones verwandelt. Firefox OS ist Open Source und erlaubt jedem, es mitzugestalten.

Firefox OS überträgt Mozillas Idee eines Open-Source-Browsers in die Welt der Smartphones. Wer HTML5 und JavaScript spricht, kann an dem Open-Source-Projekt sogar teilnehmen und sein mobiles Betriebssystem selbst mitentwickeln. Hier kann man tatsächlich tief unter die Haube schauen und beispielsweise mal eben die virtuelle Tastatur anpassen, wenn einem eine Taste fehlt. Firefox OS ist deshalb für Anwender spannend, die sich in den Ökosystemen von Google, Microsoft und Apple eingesperrt fühlen.

Interessant ist Firefox OS aber auch für Sparfüchse: Das System ist so optimiert, dass es auch auf günstiger Hardware problemlos läuft. Brauchbare Smartphones mit der nötigen Grundausstattung gibt es schon ab 60 Euro.

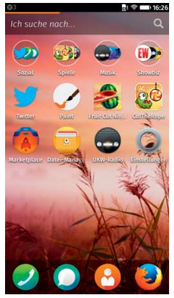
Oberfläche

Im Prinzip ist Firefox OS nichts anderes als ein aufgeblasener Firefox-Browser: Auf einem Linux-Kernel läuft die Browser-Engine Gecko als Runtime für Apps, die auch im Desktop-Browser Firefox steckt. Das Smartphone-Interface mit Startbildschirm, Telefon-App, Kartendiensten und Einstellmenüs heißt Gaia und ist ausschließlich mit offenen Webtechniken umgesetzt.

Dass man sich die ganze Zeit in einem Browser bewegt, merkt man als Nutzer aber nicht. Schnittstellen ermöglichen dem Interface und installierten Apps einen eingeschränkten Zugriff auf die Smartphone-Hardware. Die Entwickler haben sich dabei stark an Android orientiert; wer das kennt, findet sich auch schnell in Firefox OS zurecht. Vom Funktionsumfang her fühlt es sich aber wie eine der ersten Android-Versionen an: In der Kamera-App beispielsweise kann man weder die Fotogröße einstellen noch verschiedene Farbfilter verwenden, das Adressbuch importiert Kontakte aus unterschiedlichen Quellen, synchronisiert sie aber nicht. Das System führt einen getrennten Speicher für Apps, der auf den meisten Geräten nur 1 GByte groß ist und nicht per SD-Karte erweitert werden kann.

Wer sich mit Webtechniken auskennt, kann eigene Apps entwickeln. Sogenannte „Hosted Apps" werden wie eine mobile Webseite per URL aufgerufen und benötigen eine Internetverbindung. „Packaged Apps" können als Paket auf dem Smartphone installiert werden; sie laufen auch offline und haben einen tieferen Zugriff auf die Smartphone-Funktionen.

Mozilla hat einen Marketplace für Apps eingerichtet. Bisher gibt es dort vor allem kostenlose Anwendungen, die die mobilen Ansichten von Facebook, Twitter und anderen Webseiten auf die Firefox-Smartphones bringen. Spiele sind sehr selten, aufwendigere Office- oder Navigations-Software fehlt bisher komplett und auch WhatsApp, Evernote, Dropbox und Instagram gibt es für Firefox OS nicht.



Firefox OS erinnert mit seiner schlichten Optik an frühere Android-Versionen.

Ausblick

Mozilla hat sich mit mächtigen Verbündeten zusammengetan: Mobilfunkanbieter wie Telefonica oder die Deutsche Telekom verkaufen die eher günstigen Smartphones vor allem in Südamerika, Asien und Osteuropa in ihren Shops.

Es gibt inzwischen aber auch in Deutschland ein paar Modelle zu kaufen, alle im Einsteiger-Segment bis 150 Euro. Trotz der Unterstützung der Provider hat man das Gefühl, dass Mozilla und vor allem den Geräteherstellern ein bisschen der Schwung ausgegangen ist. Die meisten Smartphones laufen noch mit dem ein Jahr alten Firefox OS 1.3, die Nachfolgerversion 1.4 ist offiziell für keines verfügbar. Updates rüsten immer noch Funktionen nach, die man eigentlich als völlig selbstverständlich bei Smartphones sieht, zum Beispiel die Anzeige von Fotodetails in der Galerie oder das Speichern von SMS-Entwürfen. (acb@ct.de)

ct Video: ct.de/yyyr

Laufzeiten

	Video (normale Helligkeit) [h] besser ▸	Video (max. Helligkeit) [h] besser ▸	3D-Spiel (normale Helligkeit) [h] besser ▸	WLAN-Surfen (normale Helligkeit) [h] besser ▸
Alcatel OneTouch Fire E	5,1	4,5	4,2	6,8
Geeksphone Revolution	6,1	5,5	3,6	6,2
ZTE Open C	4,6	4,3	3,6	5,5

Normale Helligkeit: 200 cd/m², Video: 320 × 240 Bildpunkte, Spiel: Cut The Rope, Surfen: Abruf einer Standard-Webseite alle 30 s

Firefox-Smartphones

Modell	OneTouch Fire E	Revolution	Open C
Hersteller	Alcatel, alcatelonetouch.com	Geeksphone, geeksphone.com	ZTE, ztedevice.com
Betriebssystem	Firefox OS 1.3.0	Firefox OS 1.3.0 (alternativ Android 4.2.2 und CyanogenMod 11)	Firefox OS 1.3.0 (alternativ Android 4.4)
Prozessor / Kerne / Takt	Snapdragon 200 / 2 / 1,2 GHz	Intel Atom Z2560 / 2 / 1,6 GHz	Snapdragon 200 / 2 / 1,2 GHz
RAM / Flash-Speicher (frei) / SD-Slot	512 MByte / 4 GByte (1,8 GByte Medien + 1 GByte Apps) / MicroSD	1 GByte / 4 GByte (2,3 GByte für Apps, Medien nur via zusätzlicher SD-Karte) / MicroSD	512 MByte / 4 GByte (0,9 GByte Medien + 1 GByte Apps) / MicroSD
WLAN / Dual-Band	IEEE 802.11n / –	IEEE 802.11n / –	IEEE 802.11n / –
Bluetooth / NFC / GPS	3.0 / – / ✓	3.0 / – / ✓	3.0 / – / ✓
mobile Datenverbindung[1]	HSPA (42,2 MBit/s Down, 5,76 MBit/s Up)	HSPA (21 MBit/s Down, 5,76 MBit/s Up)	HSPA (21 MBit/s Down, 5,76 MBit/s Up)
Akku: Kapazität / austauschbar / drahtlos ladbar	1700 mAh / – / –	2000 mAh / ✓ / –	1400 mAh / ✓ / –
Abmessungen (H × B × T) / Gewicht	13,9 cm × 6,8 cm × 1 cm / ca. 130 g (je nach Cover)	13,9 cm × 7 cm × 1 cm / 151 g	13,9 cm × 7 cm × 1 cm / 151 g
Kamera-Auflösung Fotos / Video	2592 × 1944 (5 MPixel) / 352 × 288	2560 × 1920 (4,9 MPixel) / 1280 × 720	2048 × 1536 (3,1 MPixel) / 352 × 288
Auto- / Touchfokus / Fotoleuchte (Anz.)	✓ / – / ✓ (1)	✓ / – / ✓ (1)	– / – / –
Frontkamera-Auflösung Fotos / Video	352 × 288 / 352 × 288	1280 × 720 / 352 × 288	–
Display-Messungen			
Technik / Größe (Diagonale)	LCD (IPS) / 10 cm × 5,6 cm (4,5 Zoll)	LCD (IPS) / 10,3 cm × 5,8 cm (4,7 Zoll)	LCD / 8,7 cm × 5,2 cm (4 Zoll)
Auflösung / Seitenverhältnis	960 × 540 Pixel (244 dpi) / 16:9	960 × 540 Pixel (237 dpi) / 16:9	800 × 480 Pixel (234 dpi) / 16:9
Helligkeitsregelbereich / Ausleuchtung	21 … 325 cd/m² / 81 %	7 … 305 cd/m² / 92 %	21 … 238 cd/m² / 85 %
Kontrast / Farbraum	1038:1 / ungefähr sRGB	856:1 / sRGB	1182:1 / schlechter als sRGB
Straßenpreis	90 €	150 €	80 €

[1] Herstellerangabe ✓ vorhanden – nicht vorhanden

Achim Barczok

Das Universelle

Tizen: Betriebssystem von Smartphone bis Mikrowelle

Seit Jahren versuchen Intel und Samsung, einen Konkurrenten zu den etablierten Smartphone-Betriebssystemen ins Rennen zu schicken. Das daraus entstandene Projekt Tizen ist vielversprechend – nur ein Tizen-Smartphone kann man bisher in Deutschland noch nicht kaufen.

Tizen startete als Smartphone-Betriebssystem, doch gibt es inzwischen Versionen für Tablets, Smartwatches, Multimedia-Systeme in Autos, Smart-TVs und andere Geräte. Diese Flexibilität und Vielfalt ist gewollt und gehört zu den Hauptzielen des dahinterstehenden Konsortiums aus diversen Herstellern, von denen vor allem Samsung und Intel die Tizen-Entwicklung vorantreiben. Im Prinzip soll Tizen für alle vernetzten Geräte anpassbar sein: Auf seiner Wiki-Seite sprechen die Macher auch von Druckern, Blu-ray-Playern und sogar Mikrowellen und Waschmaschinen.

Doch ausgerechnet beim ursprünglichen Fokus Smartphones hat sich bisher kaum etwas getan, bis vor einigen Wochen das Samsung Z1 auf den Markt kam. Es ist das erste kommerziell erhältliche Smartphone, Samsung verkauft es bisher aber nur in Indien. Das 80 Euro teure Telefon richtet sich mit 4 GByte Speicher, einer 3-Megapixel-Kamera und einem Dualcore-Prozessor an Leute mit kleinem Geldbeutel. Für den asiatischen Markt typisch ist es ein Dual-SIM-Handy.

Das System ist nicht nur offen für unterschiedliche Gerätetypen. Viele Teile des Quelltexts sind Open Source, und das Konsortium versteht sich als offene Gemeinschaft, die sich klar gegen die von einzelnen Unternehmen kontrollierten Betriebssysteme Android, iOS und Windows Phone positionieren will. Unternehmen können sich an der Entwicklung des Codes beteiligen und die einzelnen Teile so zusammenstellen, wie sie es für ihre Geräte gerade benötigen.

Tizen entstand aus einer langen Historie gescheiterter Versuche, eigene Mobil-Betriebssysteme zu entwickeln. So flossen im Laufe der Zeit die Bemühungen von Nokia (Maemo), Intel (Moblin und MeeGo), der LiMo-Foundation (LiMo) und Samsung (Bada OS) zu Tizen 2.0 zusammen. Von diesem Mischmasch hat Tizen profitiert: So sind beispielsweise die schicke Oberfläche von MeeGo mit dem Funktionsumfang von Bada zusammengekommen, Entwickler können Tizen-Apps für das ursprüngliche Web-Framework von Tizen (HTML5, CSS und JavaScript) oder das native Framework von Bada (C++) entwickeln.

Schwer zu bekommen

In Deutschland kommt man weder an das Samsung Z1, noch gibt es nennenswerte Portierungen auf andere Smartphones. Als Nutzer bleibt einem deshalb nur, selber zu portieren (nichts für Einsteiger), sich im Emulator des Developer-Kits für Tizen umzuschauen oder das Z1 über Samsungs Developer-Seite aus der Ferne auszuprobieren. Was man dort zu sehen bekommt, ist aber vielversprechend.

Das bisher einzige Tizen-Smartphone Z1 ist nur in Indien erhältlich.

Durch die viele Vorarbeit in MeeGo und Bada ist Tizen schon jetzt funktionsreicher als beispielsweise Firefox OS oder Ubuntu. Man kann diverse Konten wie Dropbox, Exchange Active Sync oder Google einbinden, Kontakte und Adressen synchronisieren und in der Kamera-App von Bildgröße über Weißabgleich bis Orts-Tags fast alles einstellen. Die Oberfläche ist schick und hat sich die runden Icons der späten Meego- und Symbian-Versionen abgeschaut. Innovative Bedienelemente wie bei Sailfish OS oder Ubuntu gibt es aber nicht.

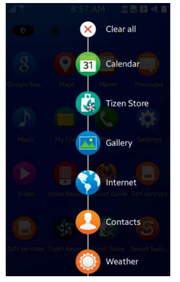
Tizen unterteilt das Interface in einen Startbildschirm mit Widgets und Web Apps sowie ein Menü mit nativen Apps. Letztere erreicht man, indem man die Schnellstartleiste nach oben wischt. Neue Nachrichten sind über die Benachrichtigungsleiste ebenso erreichbar wie Schalter für WLAN oder die Helligkeitsregelung.

Wenig Apps findet man im Tizen Store, der sich derzeit vor allem für den indischen Markt befüllt. Immerhin werden jetzt schon WhatsApp, Dropbox und andere Dienste unterstützt, für die es bei anderen Underdog-Systemen bisher keine native Software gibt.

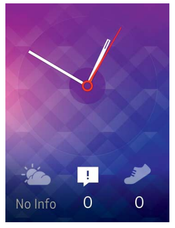
Unterm Strich bringt Tizen damit eigentlich die meisten Voraussetzungen für ein erfolgreiches Smartphone-Betriebssystem mit. Jetzt fehlt hierzulande nur noch das Smartphone.

(acb@ct.de) ct

Tizen teilt die Oberfläche wie Android in einen Startbildschirm mit Widgets und ein App-Menü ein.



Übersichtlich: Ein langer Tipp auf die Home-Taste öffnet den chronologisch sortierten App-Verlauf.



Tizen läuft nicht nur auf Smartphones, sondern auch auf Smartwatches wie der Samsung Gear S.

Dr. Oliver Diedrich

Das Schicke

Ubuntu für Smartphones und Tablets

Was lange währt …: Gut drei Jahre nach der ersten Ankündigung steht das erste Ubuntu-Smartphone vor der Tür. Das mobile Linux enthält eine Reihe innovativer Ideen unter einer ansehnlichen Oberfläche.

Ubuntu macht einiges anders als die Konkurrenz. Das mobile Linux kommt ganz ohne Home-, Windows-, Zurück-, Multitasking- oder Such-Taste aus. An deren Stelle treten Wischgesten, an die man sich schnell gewöhnt – ich habe nach zwei Tagen mit einem Ubuntu-Phone ganz instinktiv versucht, auch auf dem Android-Tablet die Tastatur nach unten wegzuwischen.

Eine Besonderheit von Ubuntu sind die Scopes, ein Zwischending aus Android-Widgets und Apps, um Informationen direkt auf dem Homescreen anzuzeigen und zu bearbeiten. Eine überall verfügbare Sidebar gewährt schnellen Zugriff auf die am häufigsten genutzen Apps. Web-Apps integrieren sich genauso gut in das System wie native Ubuntu-Apps, und Bastler finden unter der schicken Oberfläche ein richtiges Linux – Root-Zugang inklusive.

Der Begrüßungsschirm von Ubuntu für Smartphones zeigt an, was inzwischen los war.

Obwohl der Canonical-Gründer und Ubuntu-Mäzen Mark Shuttleworth die ersten Ubuntu-Smartphones bereits für Oktober 2013 versprach, gibt es derzeit noch keine Geräte zu kaufen. Die Crowdfunding-Initiative, mit der Canonical im Sommer 2013 die Entwicklung des Ubuntu-Smartphones Edge finanzieren wollte, brachte nicht einmal die Hälfte der angepeilten 32 Millionen US-Dollar zusammen. Immerhin: Am 24. Februar will der spanische Hersteller Bq in München das erste Ubuntu-Smartphone vorstellen (angekündigt war es schon für 2014). Bis das Gerät tatsächlich zu kaufen ist, muss man jedoch noch selbst Hand anlegen, wenn man Ubuntu auf einem Mobilgerät erleben will.

Eines für alles

Mit der Portierung von Ubuntu auf Mobilgeräte verfolgt Canonical seine Vision einer einheitlichen Oberfläche für unterschiedliche Geräte. Tatsächlich finden Anwender, die Ubuntu auf dem Desktop kennen, einige bekannte Bedien- und Designelemente auch auf dem Smartphone. Beispiel Ubuntu-Launcher: Die Schnellstartleiste für häufig genutzte Apps, die in Art des OS-X-Docks auch alle gerade laufenden Anwendungen anzeigt, lässt sich als Sidebar durch Wischen vom linken Bildschirmrand einblenden. Das funktioniert auf dem Homescreen ebenso wie in Apps. Auf dem Ubuntu-Desktop wird der Launcher standardmäßig am linken Bildschirmrand eingeblendet.

Auch die Scopes gibt es schon länger auf dem Ubuntu-Desktop. Wer mit Google sucht, kennt das Prinzip: Neben der allgemeinen Trefferseite gibt es eigene Seiten mit News, Bildern, Videos, Shopping-Angeboten, Büchern oder Apps. Ähnlich ist das bei Ubuntu: Standardmäßig zeigt der Homescreen, den man über das Ubuntu-Icon unten im Launcher erreicht, eine Übersicht der installierten Apps, auf Wunsch nach Kategorien sortiert. Wischt man nun mitten auf dem Display nach links, wechselt man zu einem anderen Scope: Videos (auf dem Gerät und auf YouTube), Musik (inklusive einiger Online-Dienste), Wikipedia-Artikel, das aktuelle Wetter.

Der Ubuntu App Store hält rund 50 Scopes vor. Fast alle bieten eine Suchfunktion, viele arbeiten kontextsensitiv und berücksichtigen beispielsweise den aktuellen Ort. Sie zeigen die Aufgabenliste oder die nächsten Termine an, finden auf Yelp oder OpenStreetMap Orte in der Nähe, präsentieren aktuelle Schlagzeilen, RSS-Feeds oder den eigenen Instagram-Stream, zeigen die jüngsten Xkcd-Cartoons oder ausgewählte Börsenkurse an. Android-User können sich das vorstellen wie bessere Widgets, die den ganzen Bildschirm einnehmen und auf zusätzlichen Bildschirmen neben dem Homescreen liegen. Der nativen BlackBerry- auch Android-Apps. Die Android-Runtime stammt vom AOSP (Android Open Source Project) und unterstützt deshalb keine Google-Play-Dienste, der offizielle Play Store von Google fehlt also. Am einfachsten bekommt man Apps im seit 10.3 mitgelieferten Amazon App Store. Das Angebot ist lange nicht so groß wie im Play Store, das Wichtigste findet man aber. Außerdem können Installationsdateien von Android-Apps (APKs) per Sideloading manuell installiert werden.

In der Bundesregierung ist BlackBerry aufgrund einer Spezial-Anpassung durch das deutsche Unternehmen Secusmart beliebt: Dieses hat eine per SD-Karte implementierte Krypto-Lösung entwickelt. Secusuite verschlüsselt sowohl Sprache als auch Daten und lässt sich im Unternehmen per Gateway an vorhandene Telefonlösungen anbinden. Mit zirka 2000 Euro pro Endgerät kommt die Lösung für den privaten Einsatz aber eher nicht in Frage. BlackBerry hat Secusmart inzwischen aufgekauft.

Hardware

BlackBerry-Mobilgeräte sind sehr robust. Mit Ausnahme des Z10 halten Sie locker einen Tag intensiver Nutzung durch. Die Tastaturgeräte haben quadratische Bildschirme mit 720 × 720 Pixeln und eignen sich deshalb wenig für die Wiedergabe von Filmen oder Spielen.

Nur das aktuellste und derzeit spannendste BlackBerry-Smartphone Passport hat ein hochauflösendes Display [1]. Die Kamera ist in allen Modellen eher durchschnittlich, mit langsamem Autofokus und schlechter Abbildungsleistung bei geringer Beleuchtung. Nur bei ausreichendem Tageslicht gelingen gute Schnappschüsse.

Fürs Business, sonst nur für Vielschreiber

Das Profil von BlackBerry ist sehr klar. Wer viele Nachrichten erhält und schreibt, findet keine bessere Lösung. Will man dazu noch eine gute Trennung von privaten und geschäftlichen Daten, benötigt man die Management-Plattform von BlackBerry. App-Junkies und Software-Bastler aber sollten sich woanders umschauen.

Daran dürfte sich auch in Zukunft wenig ändern. Lange Zeit versuchte BlackBerry, seine Smartphones den Privatkunden schmackhaft zu machen, doch inzwischen stellt es sich wieder auf Unternehmenskunden ein, die vermehrt mit Software und Services bedient werden. Das Geschäft mit Mobilgeräten wird damit unwichtiger, doch CEO John Chen stellte unlängst klar, dass BlackBerry auch in Zukunft sowohl Hardware als auch Software weiterentwickelt. Die aktuelle Modellpalette aus Passport und Classic soll in 2015 erweitert werden. Die immer noch gut funktionierenden Q5/Q10 und Z30 werden abverkauft.

(acb@ct.de)

Literatur

[1] Volker Weber, Effizienter Reisepass, BlackBerry-Smartphone Passport mit Tastatur und quadratischem Display, c't 22/14, S. 74 c't

Ubuntu installieren

Offiziell unterstützt der Ubuntu-Hersteller Canonical lediglich die Google-Geräte Nexus 4 (mako), Nexus 7 2013 WLAN (flo) und Nexus 10 (manta). Für viele weitere Smartphones und Tablets gibt es allerdings schon Portierungen (siehe c't-Link). Beim Flashen des Ubuntu-Image wird der gesamte Speicher des Geräts gelöscht; zumindest auf die Google-Geräte kann man später aber wieder Android aufspielen. Wir beschreiben im Folgenden die Installation auf einem Nexus 4 mit Android 5 (Kitkat).

Ubuntu für Smartphones lässt sich nur aus einem aktuellen Desktop-Ubuntu heraus installieren. Der Betrieb in einer virtuellen Maschine reicht nicht aus, in einer Ubuntu-VM unter VMware blieb der Flash-Prozess zuverlässig hängen. In Ubuntu müssen einige Programmpakete nachinstalliert werden:

```
sudo add-apt-repository universe
sudo apt-get update
sudo apt-get install android-tools-adb
    android-tools-fastboot ubuntu-device-flash
```

Wenn Sie auf dem Android-Gerät die Datenverschlüsselung aktiviert haben, ist zunächst ein Reset auf die Werkseinstellungen nötig. Außerdem müssen Sie in den Entwickleroptionen das USB-Debugging erlauben. Testen Sie den Zugriff mit

```
adb shell cat system/build.prop
```

Fahren Sie das Nexus 4 nun herunter und starten Sie mit der Tastenkombination Leiser+Power in den Bootloader. Der Befehl

```
sudo fastboot oem unlock
```

entsperrt den Bootloader, was Sie am Telefon mit Lautstärkewippe und Powertaste bestätigen müssen. Achtung: Spätestens dabei werden alle Daten gelöscht.

Der Befehl

```
sudo fastboot reboot-bootloader
```

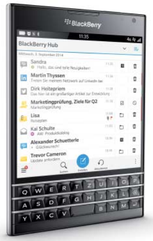
führt einen Neustart in in den Bootloader durch. Nun können Sie mit

```
ubuntu-device-flash --channel=stable --bootstrap
```

die stabile RTM-Version (Release To Manufacturing) aufspielen. Wer die aktuelle Entwicklerversion ausprobieren möchte, die auf unserem Nexus 4 ähnlich stabil lief, verwendet stattdessen die Option

```
--channel=ubuntu-touch/ubuntu-rtm/14.09-proposed.
```

Nach dem Flashen bootet das Gerät automatisch neu.



Volker Weber

Das Arbeitstier

BlackBerry: Perfekte Messenger-Maschinen, Betriebssystem fürs Business

Mit einem BlackBerry-Smartphone und dem Betriebssystem BlackBerry 10 bekommt man die beste Messaging-Maschine auf dem Markt – und kann auf seinem Smartphone Arbeits- und Privatwelt sauber trennen.

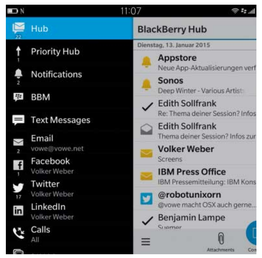
Vor acht Jahren war BlackBerry noch die Nummer zwei im Smartphone-Geschäft, heute ist das kanadische Unternehmen hierzulande ein Außenseiter. Schade, denn eigentlich sind die Schwächen von früher längst behoben: BlackBerry OS ist seit Version 10 wieder ein spannender Konkurrent gegenüber Android, iOS und Windows Phone.

Alle neuen BlackBerry-Mobilgeräte haben wenigstens zwei Gigabyte RAM und einen Mehrkernprozessor und sind damit konkurrenzfähig mit iPhone und Co. Die Smartphones Z10 und Z30 sind reine Touchscreen-Geräte, alle anderen Geräte von BlackBerry haben eine hochwertige, mechanische QWERTZ-Tastatur. Sie hat einen deutlich spürbaren Druckpunkt und ausgeformte Tasten und lässt sich damit blind bedienen. BlackBerry 10 liefert dazu Wortergänzungen in bis zu drei Sprachen gleichzeitig – das lästige Umschalten wie auf anderen Plattformen entfällt.

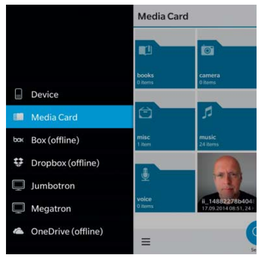
BlackBerrys sind die perfekten Messaging-Smartphones. Alle Nachrichten aus allen Quellen laufen im BlackBerry Hub zusammen, seien es mehrere Mail-Accounts, Twitter, Facebook, SMS, WhatsApp oder das BlackBerry-eigene Chat-System BBM. Der Hub ist von jeder App aus über eine L-Geste erreichbar. Eine Benachrichtigungs-LED signalisiert den Nachrichteneingang (seit BlackBerry 10.3.1) in verschiedenen Farben, sodass man auch ohne Einschalten des Geräts erkennt, ob wichtige Nachrichten eingegangen sind.

Privat und geschäftlich

Setzt man den BlackBerry Enterprise Server als Management-lösung ein, so trennt BlackBerry 10 zuverlässig geschäftliche von privaten Daten und Apps. Der Business-Bereich wird vom Unternehmen aus der Ferne verwaltet, der private bleibt frei. Im privaten Bereich laufen neben



Der BlackBerry Hub zieht alle Konten und den Kalender zu einer Ansicht zusammen.



Der Dateimanager greift auf BlackBerry, Speicherkarte, verbundene PCs und Cloud Services zu.

Achim Barczok

Die Ausgestorbenen

Einst groß, heute vergessen: Symbian, Palm OS, Web OS, Bada und Windows Mobile

Als Nokia und Palm noch große Namen waren, hatten Smartphones Tastaturen und Schreibgriffel. Dann ließen iPhone und Android alles andere alt aussehen. Die wenigsten Smartphone-Pioniere haben die Touch-Revolution überlebt – viele Betriebssysteme blieben einfach auf der Strecke.

Die frühen Jahre der Smartphone-Welle dominierte Nokia. Für seine mit Applikationen erweiterbaren Smartphones nutzte das finnische Unternehmen **Symbian OS**. Das darauf basierende **S60** fand sich bald auf jedem teureren Nokia-Smartphone. Das Betriebssystem erzielte zeitweilig weltweite Marktanteile von über 50 Prozent, auch weil es Hersteller wie Siemens, Panasonic und Samsung ebenfalls auf ihren Geräten installierten. Nach dem iPhone versuchte Nokia das Betriebssystem für Touch-optimierte Smartphones fitzumachen, doch 2011 gab der Schulterschluss mit Microsoft Symbian den Todesstoß.

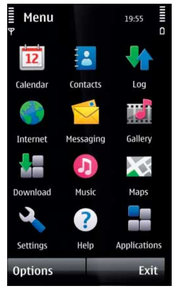
Gegen Symbian positionierte sich Palm Anfang 2000 mit seinem ursprünglich für stiftbediente PDAs entwickelten **Palm OS**. Das System war für billige Hardware optimiert, die sich damit besonders flüssig bedienen ließ. Der Clou war die Steno-Gestenschrift Graffiti, mit der man Buchstaben aufs resistive Display kritzelte. Irgendwann wurde die Hardware schneller und die Betriebssysteme funktionsreicher, und Palm OS hielt nicht mehr mit.

Danach probierte es Palm noch einmal mit einem neuen System auf Augenhöhe mit iOS und Android. **WebOS** basierte auf Webtechniken und hatte viele innovative Features und eine schicke Optik. Vielleicht war das System der Zeit voraus, denn die Palm-Pre-Smartphones waren zu schlecht ausgestattet und hatten zu viele Macken. Den Garaus machte WebOS am Ende aber der Zickzackkurs des Palm-Käufers HP, der im Halbjahrestakt die Mobilstrategie wechselte und am Ende nichts mehr mit Hardware zu tun haben wollte. Inzwischen lebt WebOS in Smart-TVs von LG weiter.

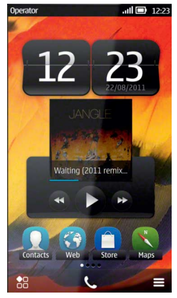
Windows für Handy

Microsoft wollte mit **Windows CE** in den frühen Taschencomputer-Jahren mitmischen; nach mäßigem Erfolg nannte man das System in **Windows Mobile** um, brachte es auf Smartphones und lizenzierte die Software an andere Gerätehersteller. Das Multitouch-Smartphone von Apple ohne Tastatur beläschelte Microsoft-Chef Steve Ballmer 2007 noch, doch schon bald versuchte Microsoft vergeblich, Windows Mobile für die neuen Wünsche der Anwender anzupassen. Am Ende warf Microsoft den Code weg und versuchte einen Neuanfang mit Windows Phone.

Fast alle Samsung-Geräte laufen mit Android, doch am liebsten würde Samsung seine Nutzer auf eine eigene Plattform locken. Einen erfolgversprechenden Versuch startete das koreanische Unternehmen 2010. Das eigene Betriebssystem **Bada OS** war an den meisten Stellen eine 1:1-Kopie von Android und konnte zu Beginn Erfolge verzeichnen – aber nur, weil Samsung die ersten Bada-Handys mit Top-Hardware geradezu verscherbelte. 2013 ging Samsung die Luft aus. Bada wurde eingestellt, die Code-Basis ließ Samsung in das System Tizen einfließen (S. 113). (acb@ct.de)



Symbian S60 (2008)

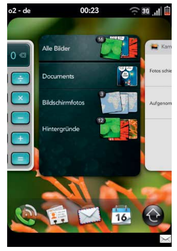


Symbian 3 (2011)

Windows Mobile (2006)

Palm OS (2004)

Bada OS (2010)



Web OS (2009) c't

Ronald Eikenberg, Jörg Wirtgen

Surf-Versicherung für Android

Jelly Bean und älter trotz Schwachstellen sicher nutzen

Wer eine ältere Android-Version als 4.4 nutzt, muss mit Sicherheitslücken im Browser leben, die Google nicht schließen will – und selbst die existierenden Sicherheits-Patches kommen nicht auf allen Geräten an. Bevor die Lücken von Cyber-Ganoven ausgenutzt werden, sollten Sie daher auf Ihrem Smartphone und Tablet ein paar Vorsichtsmaßnahmen ergreifen.

Auf fast der Hälfte der aktuell genutzten Android-Geräte läuft noch Jelly Bean (Android 4.1 bis 4.3), auf über 10 Prozent eine noch ältere Version – und in vielen davon klaffen Sicherheitslöcher. Zwar hat Google bislang stets passende Patches entwickelt, doch die landen nur bei den Herstellern, die es dann oft versäumen, sie den Nutzern in Firmware-Updates zur Verfügung zu stellen. Ob und welche Lücken im eigenen Gerät klaffen, kann man nur mit großem Aufwand herausfinden.

Künftig spitzt sich die Lage für Nutzer alter Android-Versionen Einsatz, die dadurch ebenfalls angreifbar sind. Browser und WebView kann man bis Jelly Bean nur per Firmware-Update auf den aktuellen Stand bringen.

Smartphone als Wanze

Würde es ein Angreifer darauf anlegen, ein Android-Gerät zu kompromittieren, hätte er reichlich Möglichkeiten. So bringt etwa das frei verfügbare Pentesting-Tool Metasploit inzwischen elf Module mit, die verschiedene Android-Lücken ausnutzen. Je älter die Android-Version, desto größer die Auswahl. Mit Metas-

Same-Origin-Policy mit wenigen Zeilen JavaScript-Code umgehen und so auf persönliche Daten seines Opfers zugreifen. Auch das konnten wir nachvollziehen. Diese Angriffsform bezeichnet man als Universal-Cross-Site-Scripting (UXSS).

Der Sicherheitsexperte Tod Beardsley von Rapid7 hat den Angriff kürzlich auf die Spitze getrieben, indem er UXSS mit einer Lücke in Googles Play Store kombinierte. Seine Demoseite steuerte die Web-Ausgabe von Google Play fern. Sie lud zuerst die Produktseite einer beliebigen App und klickte anschließend auf den Kaufen-Button. Kurze Zeit später wurde die App auf dem Gerät des Webseitenbesuchers installiert und gestartet – vollautomatisch und ganz ohne Nutzerinteraktion. Google hat die verwundbaren Browser-Versionen kurz darauf aus der Web-Version des Stores ausgesperrt. Damit wird zwar die auto-

den oben beschrieben UXSS-Bug einen Patch in die Firmware integriert hat. Wir haben dazu eine harmlose Testseite entwickelt (siehe c't-Link am Ende des Artikels), welche die UXSS-Lücke tatsächlich ausnutzt – gelingt das, ist die Wahrscheinlichkeit groß, dass der Hersteller auch andere Patches vernachlässigt hat. Sie sollten also vom Schlimmsten ausgehen.

Gibt es kein offizielles Update auf 4.4 oder neuer, kann ein CustomROM mit Android 4.4 eine Lösung sein; also ein selbst aufgespieltes Alternativ-Android. Für viele Geräte gibt es CustomROMs, eine gute Anlaufstelle ist CyanogenMod. Das ist aber nichts, was man mal eben schnell einspielt, sondern eine grundlegende Entscheidung. Selbst wenn alles glattgeht, müssen Sie Ihr Gerät dazu rooten sowie alle Apps und Einstellungen neu installieren. Sie verlieren meist auch die Hersteller-Garantie und müssen auf jene

Was bisher geschah…

28.03.2015 11:28 55

UberPOP: Kundendaten im Web

Laut Medienberichten gibt es Zugangsdaten zu Tausenden von Nutzerkonten des Taxi-Fahrdiensts UberPOP zu Schleuderpreisen im Web zu kaufen. Darüber lassen sich auch Fahrten im Namen des Kontoinhabers buchen.

Für Kaufpreise ab einem US-Dollar offerieren mehrere Anbieter Kontodaten zum Mitfahrdienst Uber, berichtet das Web-Magazin Motherboard. Demnach enthalten die Datensätze außer Benutzername und Passwort auch die letzten Ziffern und das Verfalldatum von dessen Kreditkarte. Damit kann man, wie das Magazin schreibt, die Dienste von Uber buchen und die bisherigen Fahrten des Kontoinhabers auflisten.

Topic: Security

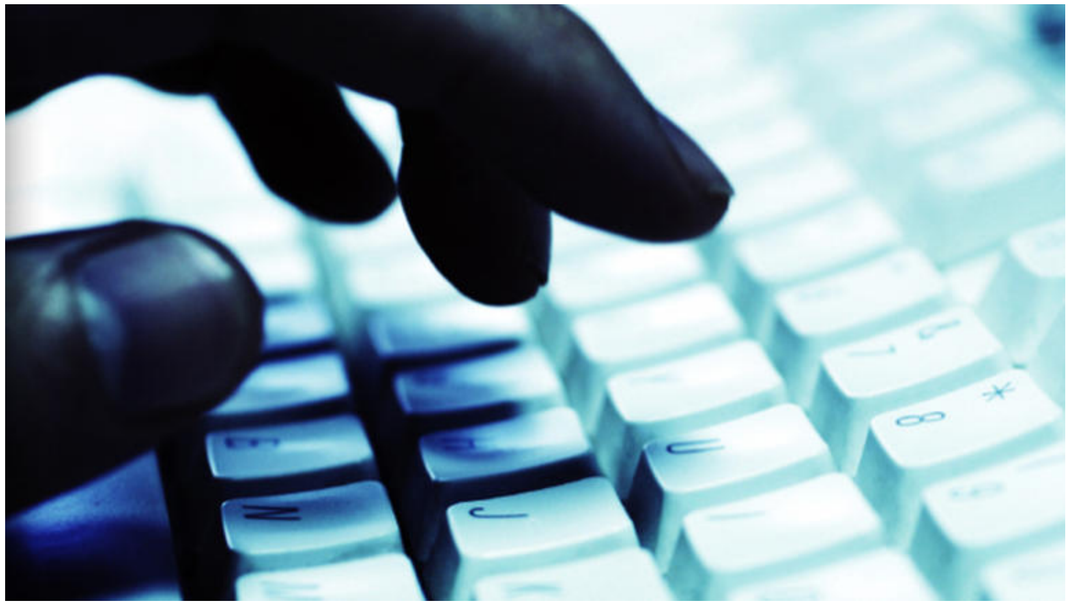
Follow via:

GitHub suffers 'largest DDoS' attack in site's history

Summary: *US coding website GitHub is fending off a DDoS onslaught focused on shutting down anticensorship tools.*

By Charlie Osborne for Zero Day | March 30, 2015 -- 01:43 GMT (02:43 BST)

Follow @ZDNetCharlie



CNET

News

Recent entries

Surveillance system used for censorship in Europe

Censorship attack combines packet injection and Heartbleed

We all know there is censorship online. It happens in China. It happens to "terrorists". But we don't believe it will happen to us.

As Eben Moglen and Kaspersky have pointed out, companies developing crypto are prime targets no matter where they are. So you don't have to be a bad guy for the NSA to attack you. You just have to protect people from the NSA. Even protecting yourself is often enough. NSA prefers their victims to be defenseless.

Detection in the wild

In early 2015 people were still downloading our ISO file for GoodCrypto. But suddenly installations stopped.

After a lot of checking we noticed that the downloads got HTTP 200 result codes, but the lengths were all too short. This isn't supposed to happen. A 200 result means success. These weren't successful downloads, but the web logs said they were. Ordinary log checks didn't show the bug.

Finding the vuln

Downloads from goodcrypto.com to goodcrypto.com worked. Downloads from another site at a different datacenter in the same country worked. A little further away in the network, downloads failed but the server logged a "Success" status code.

The obvious answer was a server misconfiguration. We couldn't find one. A server side packet dump showed the client just dropped the connection in the middle of the download.

We couldn't get a browser to download the whole ISO file. The browser thought it came in fine, but the file was

ZENSUR

Türkische Behörden sperren Twitter und Youtube

06.04.15, 14:23 Mail an die Redaktion

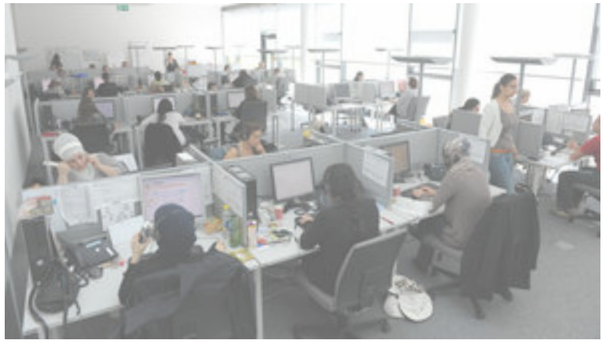
Twitter und YouTube werden immer wieder von den türkischen Behörden gesperrt

ZENSUR

Türkische Behörden sperren Twitter und

Nach der Veröffentlichung von Fotos der tödlichen Geiselnahmen eines Staatsanwaltes ließen die türkischen Behörden YouTube und Twitter sperren.

FEATURED



VISUAL HACKING

MAKING SMART LOCKS SMARTER (AKA. HACKING THE AUGUST SMART LOCK)

By Dcept905 on Sunday 29 March 2015, 23:07 - Permalink

locksport research security smart lock

By: Paul Lariviere & Stephen Hall

Introduction:

During a recent Security Compass 'Hack Week' we decided to take a look at smart locks in an attempt to assess the current state of Smart Lock Security. For our project we decided to take a look at the August Smart Lock. The August Smart Lock is an electronic locking mechanism that can be controlled from a mobile device. It supports Apple and Android platforms and allows the owner to grant access to other smart phones on either a temporary time limited, or permanent basis from anywhere as long as there is internet connectivity. The August Smart Lock is mounted on the back of almost any installed deadbolt replacing the existing thumb latch but leaving the rest of the lock in tact. In our opinion this makes it a

PILOTPROJEKT

Digitales Parkpickerl hält in Wien Einzug

21.04.15, 16:05 Mail an die Redaktion

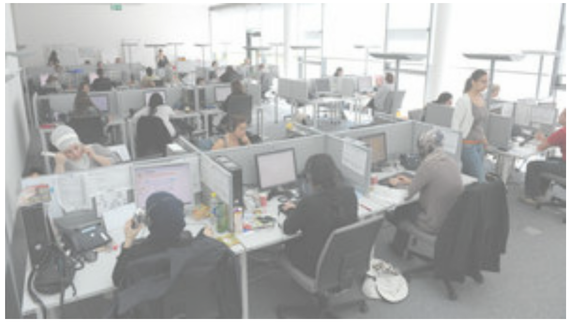
In Zukunft soll ein einziger Chip ausreichen - Foto: KURIER

Im Herbst startet im 4. und 5. Wiener Gemeindebezirk versuchsweise ein elektronisches Parkpickerl auf RFID-Basis.

PARKPICKERL, WIEN, RFID

Statt wie bisher jedes Jahr neue Parkpickerl an ihre

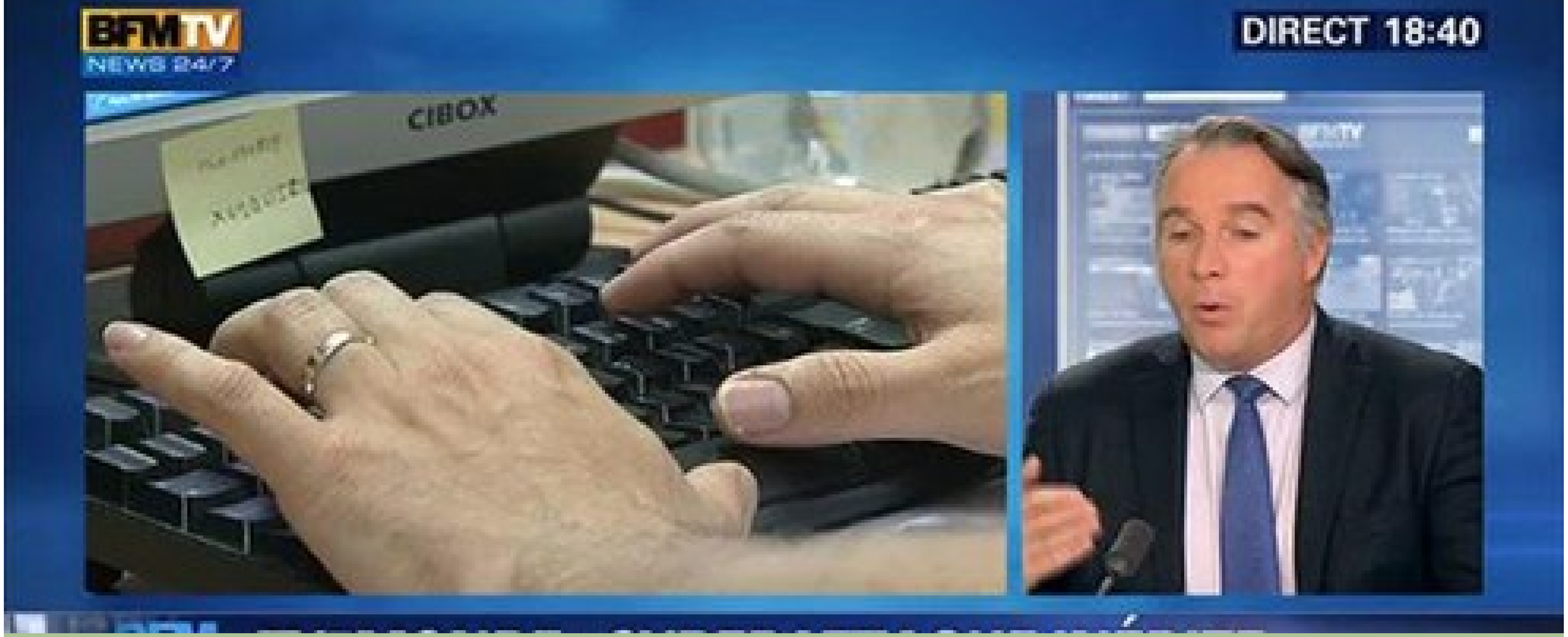
FEATURED



VISUAL HACKING

Wie ein Handyfoto eine ganze Firma ruinieren kann


Les coordonnées du superviseur
47 90



Netzpolitik

Französischer TV-Sender TV5Monde verriet Passwörter unabsichtlich bei Interview

10. April 2015, 10:29

Attention: DATE CHANGED for TROOPERS16 - taking place from 14th to 18th March 2016!

Thanks everybody for an amazing TROOPERS week! We hope all of you had an enjoyable event - We're now working on publishing all the video recordings and presentation slides as soon as possible. Do not forget to mark your calendars for TROOPERS16.

Welcome to TROOPERS, your favorite IT-Security Conference.

Upcoming: TROOPERS16, 14th - 18th March 2016!

Troopers16 will be the ninth edition of the great IT-Security Conference, where the world's leading IT-Security experts and Hackers present their latest research.

Troopers provides a networking platform for Security interested people from all over the world and enables security folks from the industry, academia and the research community to exchange knowledge and talk about their work. Again, Troopers15 is going to be an event unlike most other

TROOPERScon

Subscribe 533

Home Videos Playlists Channels Discussion About

TROOPERS15 - Talks

by TROOPERScon • 33 videos • 1,465 views • Last updated on Mar 27, 2015

Play all Share Save

1	**TROOPERS15 - Welcome Trailer** by TROOPERScon	2:06
2	**[TROOPERS15] Enno Rey - Opening Remarks** by TROOPERScon	9:34

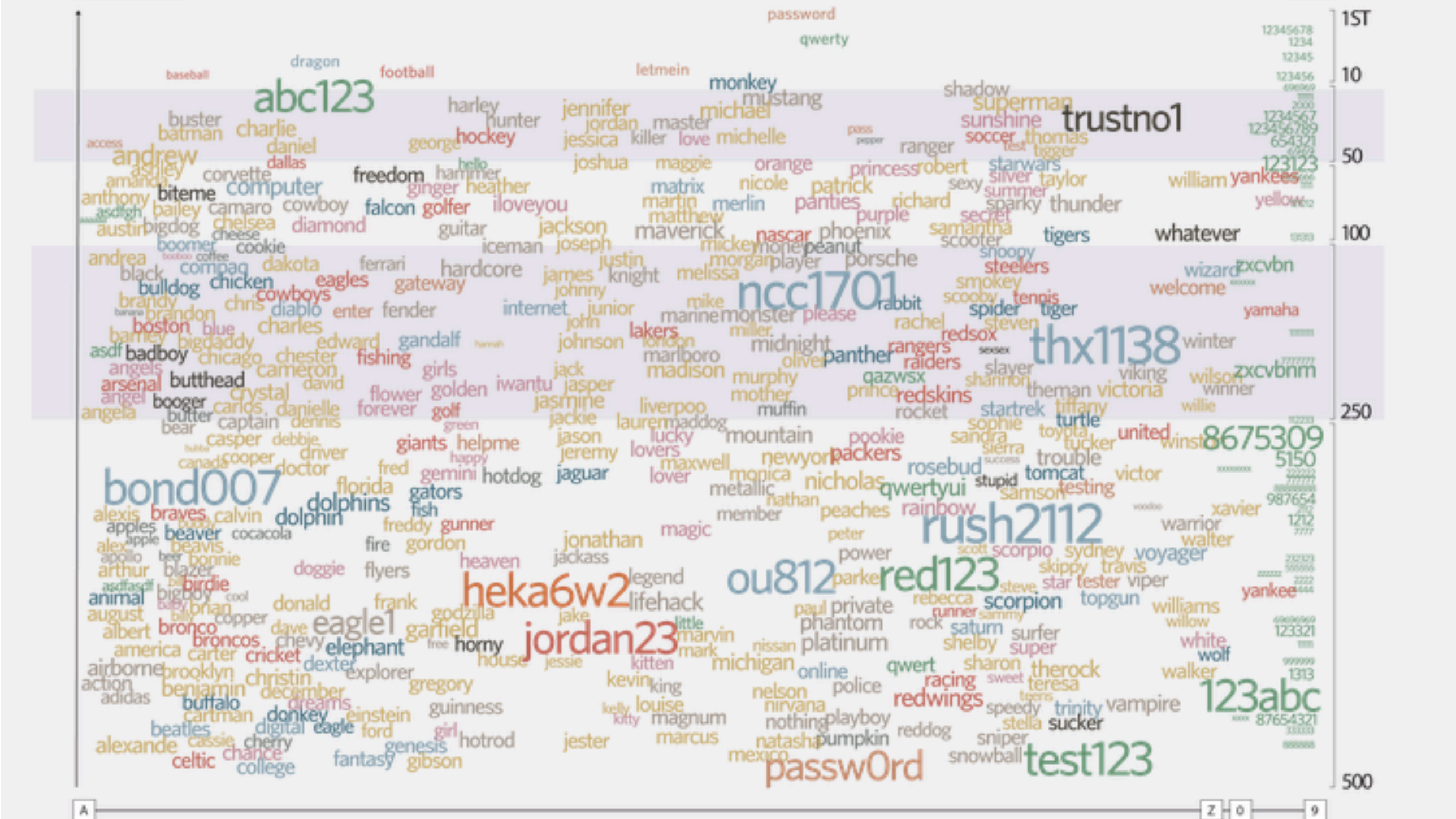

1ST
10
50
100
250
500
A
Z
0
9
password
qwerty
dragon
baseball
football
letmein
monkey
abc123
shadow
superman
trustno1
harley
jennifer
michael
mustang
buster
hunter
jordan
master
sunshine
batman
charlie
hockey
jessica
killer
lowe
michelle
soccer
thomas
access
daniel
george
ranger
tigger
andrew
dallas
joshua
maggie
orange
princess
robert
starwars
123123
ashley
hello
corvette
freedom
hammer
sexy
silver
taylor
william
yankees
amanda
computer
ginger
heather
matrix
nicole
patrick
summer
biteme
anthony
falcon
golfer
iloveyou
martin
merlin
panties
richard
sparky
thunder
yellow
bailey
camaro
cowboy
matthew
purple
secret
asdfgh
austin
bigdog
chelsea
diamond
guitar
jackson
maverick
nascar
phoenix
samantha
tigers
whatever
cheese
boomer
cookie
iceman
joseph
mickey
money
peanut
scooter
snoopy
andrea
coffee
compaq
dakota
ferrari
hardcore
justin
morgan
player
porsche
steelers
wizard
zxcvbn
black
james
knight
melissa
ncc1701
smokey
welcome
bulldog
chicken
eagles
gateway
johnny
scooby
tennis
cowboys
brandy
chris
diablo
enter
fender
internet
junior
mike
rabbit
spider
tiger
yamaha
banana
brandon
boston
blue
charles
john
lakers
marine
monster
please
rachel
steven
barney
bigdaddy
edward
gandalf
hannah
johnson
london
miller
midnight
redsox
thx1138
winter
asdf
badboy
chicago
chester
fishing
marlboro
oliver
panther
rangers
raiders
sexsex
angels
cameron
girls
jack
madison
murphy
qazwsx
shannon
slayer
viking
wilson
zxcvbnm
arsenal
butthead
david
iwantu
jasper
mother
prince
redskins
theman
victoria
winner
angel
booger
crystal
flower
golden
jasmine
angela
carlos
danielle
forever
golf
liverpoo
muffin
rocket
startrek
tiffany
willie
butter
captain
dennis
jackie
laurenm
maddog
turtle
bear
green
sophie
toyota
united
casper
debbie
giants
helpme
jason
lucky
mountain
pookie
sandra
tucker
winston
8675309
bubba
cooper
driver
happy
jeremy
lovers
packers
sierra
trouble
5150
canada
doctor
fred
gemini
hotdog
jaguar
maxwell
newyork
success
rosebud
tomcat
victor
bond007
florida
gators
lover
monica
nicholas
stupid
testing
xxxxxxxx
dolphins
fish
metallic
qwertyui
samson
987654
alexis
braves
calvin
dolphin
member
nathan
peaches
rainbow
rush2112
xavier
apples
beaver
cocacola
freddy
gunner
magic
peter
warrior
1212
alex
apple
beavis
fire
gordon
jonathan
power
scott
scorpio
sydney
voyager
walter
apollo
bonnie
heaven
jackass
arthur
blazer
doggie
flyers
ou812
parker
red123
skippy
travis
birdie
heka6w2
legend
star
tester
viper
yankee
animal
bigboy
cool
lifehack
rebecca
scorpion
topgun
williams
donald
frank
paul
private
august
brian
copper
godzilla
jake
little
phantom
rock
saturn
surfer
willow
albert
bronco
dave
eagle1
garfield
marvin
shelby
super
123321
broncos
chevy
elephant
free
horny
jordan23
mark
nissan
platinum
white
america
carter
cricket
dexter
house
jessie
kitten
michigan
wolf
airborne
brooklyn
explorer
online
qwert
sharon
therock
walker
1313
action
christin
gregory
kevin
king
racing
sweet
teresa
123abc
benjamin
december
nelson
police
redwings
adidas
buffalo
dreams
guinness
louise
nirvana
speedy
trinity
vampire
tigers
cartman
donkey
einstein
magnum
nothing
playboy
stella
sucker
beatles
digital
eagle
ford
girl
hotrod
jester
marcus
natasha
pumpkin
reddog
sniper
alexande
cassie
cherry
genesis
chance
celtic
college
fantasy
gibson
mexico
passw0rd
snowball
test123

Foto: Google

Google macht in seinem Chrome Store sauber.

GOOGLE

Hunderte Browser-Erweiterungen aus Chrome Store entfernt

Letztes Update am 08.04.2015, 10:23

Millionen Nutzer, die Google-Seiten aufrufen, haben laut einer aktuellen Untersuchung bösartige Add-ons auf ihren Browsern installiert.

Gemeinsam mit Sicherheitsexperten hat Goolge mehr als 100 Millionen Browser untersucht, mit denen Google-Sites aufgerufen wurden. Bei rund fünf Prozent der untersuchten Browser wurden bösartige Add-ons entdeckt, berichtet die BBC.

NEGATIVAUSZEICHNUNG

Lauschende Barbie erhält Big Brother Award

Mattels sprechende Barbie, der Bundesnachrichtendienst und Amazon gleich zweimal: Sie alle erhalten den Big Brother Award 2015 für einen allzu laxen Umgang mit persönlichen Daten. Den Publikumspreis bekamen Thomas de Maizière und Hans-Peter Friedrich.

Sie zeichnet Gespräche der Kinder auf und lässt sie in der Cloud des Herstellers analysieren, bevor sie eine passende Antwort formuliert: Die sprechende Barbie von Mattel und Toytalk erhält deshalb den Big Brother Award 2015 im Bereich Technik. Weitere Preise wurden in den Kategorien "Neusprech", "Verbraucherschutz" und "Politik" vergeben. Amazon erhielt den Preis gleich zweimal, in den Kategorien "Wirtschaft" und "Arbeitswelt". Und wenig überraschend bekommt der Bundesnachrichtendienst den Preis in der Kategorie "Behörden & Verwaltung".

Die sprechende und lauschende Barbie erhält den diesjährigen Big Brother Award im Bereich Technik. (Bild: Mike Licht, CC BY-2.0)

Datum: 18.4.2015, 22:59

Autor: Jörg Thoma

Themen: Datenschutz, Amazon, BND, CCC, Max Schrems, Verbraucherschutz, Überwachung, Internet, Politik/Recht, Security

Teilen: 1 35 57 12

Tools: Drucken

Automattic Sponsors Let's Encrypt Initiative

Sarah Gooding April 10, 2015 14

★ CURRENTLY ON TAP


XSS Vulnerability Affects More Than a Dozen Popular WordPress Plugins


Zero Day XSS Vulnerability in WordPress 4.2 Currently Being Patched


18 Free

The EuroDiVision Contest - feat. Merkel, Žižek & IMF [RAP NEWS 31]

thejuicemedia

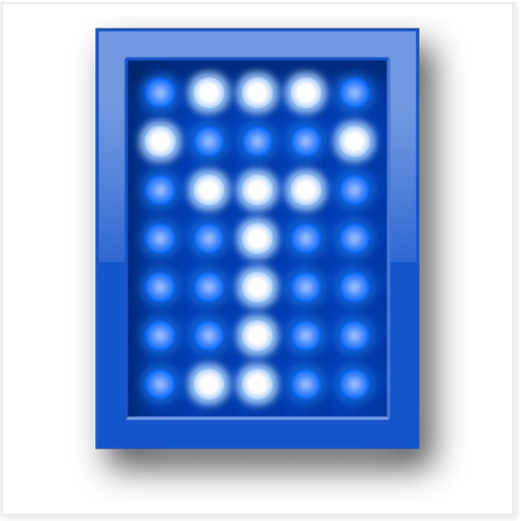
A Few Thoughts on Cryptographic Engineering

Some random thoughts about crypto. Notes from a course I teach. Pictures of my dachshunds.

T h u r

Truecrypt report

A few weeks back I wrote an update on the Truecrypt audit promising that we'd have some concrete results to show you soon. Thanks to some hard work by the NCC Crypto Services group, soon is now. We're grateful to Alex, Sean and Tom, and to Kenn White at OCAP for making this all happen.



You can find the full report over at the Open Crypto Audit Project website. Those who want to read it themselves should do so. This post will only give a brief summary.

The TL;DR is that based on this audit, Truecrypt appears to be a relatively well-designed piece of crypto software. The NCC audit found no evidence of deliberate backdoors, or any severe design flaws that will make the software insecure in most instances.

That doesn't mean Truecrypt is perfect. The auditors *did* find a few glitches and some incautious programming -- leading to a couple of issues that could, in the right

About Me

Matthew Green

I'm a cryptographer and research professor at Johns Hopkins University. I've designed and analyzed cryptographic systems used in wireless networks, payment systems and digital content protection platforms. In my research I look at the various ways cryptography can be used to promote user privacy.

My website
My twitter feed
Useful crypto resources
RSS
Bitcoin tipjar
Matasano challenges

Journal of Cryptographic Engineering
(not related to this blog)

View my complete profile

Wie sicher ist Email?


CUPERTINO, CA


CUPERTINO, CA

Who's attacking email?

1. Passive man-in-the-middle (MITM)
   - ➢ STARTTLS
2. Passive MITM with your TLS keys
   - ➢ STARTTLS + Forward Secrecy
3. Active MITM
   - ➢ STARTTLS "pinning"
4. Malicious/compromised email provider
   - ➢ End-to-End Encryption
5. Email account hacked
   - ➢ End-to-End Encryption

Header
Body

Header

Von:
An:
Kopie:
Blindkopie:
Betreff:

Body

Text:
Anhänge:
Signaturen:

S/MIME

Email

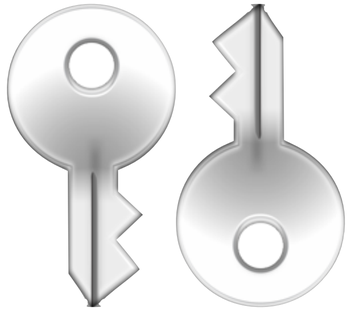
Von:	info@anonyme-alkoholiker.at
An:	reblaus@kampftrinker.at
CC:	office@wgkk.at
Blindkopie:	k.brinkmann@schwarzwaldklinik.de
2 Zeitstempel:	Mon Jun 25 19:29:40 CEST 2012
Betreff:	Re: Überwachungssta.at Flyer
Inhalt:	Liebes BVT!
Anhänge:	Pwnies.pdf

Von:	info@anonyme-alkoholiker.at
An:	reblaus@kampftrinker.at
CC:	office@wgkk.at
Blindkopie:	k.brinkmann@schwarzwaldklinik.de
Zeitstempel:	Mon Jun 25 19:29:40 CEST 2012
Betreff:	Re: Überwachungssta.at Flyer

Inhalt:	Liebes BVT!
Anhänge:	Pwnies.pdf

Symmetrische Verschlüsselung

Asymmetrische Verschlüsselung



Public

Private

Public

*Ver*schlüsseln

Entschlüsseln

Private

Signieren

Private

Public

Überprüfen

Vertrauen

Public Keys

GPG Keyserver

https://Keybase.io

Nicht glauben

Überprüfen

❖ http://www.gpg4win.org/

 https://www.gpgtools.org/

 https://gnupg.org/

RSA/4096

GPG Key-Signing