Defense Against the Dark Arts for the digital world

Rüdiger Weis

Oktober 2014

Zum Glück haben die Nerds nichts zu sagen

NETZPOLITIK.ORG

Martin Schulz: Zum Glück haben die Nerds nichts zu sagen

"Denn wenn wir diese Fragen allein den technischen Experten, den Programmierern und Nerds überließen, lebten wir in einem selbstreferentiellen System, es käme zur Herrschaft der Ingenieure und Mathematiker, zu einer Expertenregierung im Platon'schen Sinne."

von Markus Beckedahl am 12. Oktober 2014.

Flächendeckendes Abhören

Regierungen scheitern beim Schutz der Bürger

Kryptographie und Open Sorce können flächendeckendes Abhören verhindern. Diplomatie bisher nicht.

Bruce Schneier, Guardian, 6. September 2013

"Trust the math. Encryption is your friend."

Kryptomagie = Mathematik + Freie Software

Kryptomagie = Mathematik + Freie Software

Kryptographie ermöglicht durch **Mathematik**
auf einer kleinerfingernagelgroßen Fläche oder
mit einer handvoll Programmzeilen,
Daten sicher selbst gegen eine weltweite
Geheimdienstzusammenarbeit zu verschlüsseln.
Freie Software ermöglicht dies kosten- und hintertürenfrei.

Nach Snowden: Nicht stärkste Kryptographie ist schwach.

- In der Kryptographie rechnet man schon immer mit einem Angreifer, der alle Nachrichten abhören kann und Milliarden Dollars zum Brechen der Verschlüsselung zur Verfügung hat.
-
- **Nach Snowden** wissen wir genauer, an welchen Kabelstellen abgehört wird und auf den Cent genau, wie viel Geld für Kryptoangriffe vorhanden ist.[1]

[1] Nicht uninteressant, aber wissenschaftlich betrachtet nur eine Fußnote.

Die unendliche Geschichte: Trusted Computing

NETZPOLITIK.ORG

Netzpolitik-Podcast mit Rüdiger Weis über Trusted Computing

zum Thema Trusted Computing, Digital Restrictions Management und die Kriminalisierung seiner Studenten durch Urheberrechtsgesetzgebung.

Von Markus Beckedahl am 25. Oktober 2006.

Apple und Trusted Computing 2006

NETZPOLITIK.ORG

Professor Dr. Rüdiger Weis:

"Apple bildet leider die Speerspitze bei der Nutzerentmuendigung mittels DRM und “Trusted” Computing Ueberwachungshardware. Mittelfristig werden Apple-Intel-PC Nutzer zu Podslaves(TM?)."

Digital Rights Management
von Markus Beckedahl am 03. Oktober 2006,

Die fehlende NSA Folie

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) ...and the zombies would be paying customers?

Fröhliche Geheimdienste 2013

NETZPOLITIK.ORG

Interview: Trusted Computing stimmt Geheimdienste fröhlich

"Ansonsten war schon der Versuch mittels Trusted Computing eine schöne neue überwachte Welt zu schaffen, vor 10 Jahren am Widerstand der Netzgemeinde gescheitert. Selbst Apple nutzte die zunächst verbauten TPM Chips nicht und liess sie nach 2009 heimlich, still und leise ganz verschwinden."

von Markus Beckedahl am 20. August 2013,

BSI warnt nicht vor Windows 8

"Stellungnahme des BSI zur aktuellen Berichterstattung zu MS Windows 8 und TPM", August 2013.

"Insbesondere können auf einer Hardware, die mit einem TPM 2.0 betrieben wird, mit Windows 8 durch unbeabsichtigte Fehler des Hardware- oder Betriebssystemherstellers, aber auch des Eigentümers des IT-Systems Fehlerzustände entstehen, die einen weiteren Betrieb des Systems verhindern. Dies kann soweit führen, dass im Fehlerfall neben dem Betriebssystem auch die eingesetzte Hardware dauerhaft nicht mehr einsetzbar ist. Eine solche Situation wäre weder für die Bundesverwaltung noch für andere Anwender akzeptabel."

BSI warnt nicht vor Windows 8, Zugabe:

"Darüber hinaus können die neu eingesetzten Mechanismen auch für Sabotageakte Dritter genutzt werden. Diesen Risiken muss begegnet werden."

Booten mit Elektronischer Fussfessel von Microsofts Gnaden

heise Security News-Meldung vom 11.12.2013, 00:08

"Interessant ist, dass Microsoft en passant gleich neun UEFI-Secure-Boot-Module von anderen Herstellern sperrt (Microsoft Security Advisory 2871690). Systeme mit aktiviertem Secure Boot können damit dann nicht mehr starten."

China verbietet Windows 8

Während deutsche Behörden darüber diskutieren, wie sehr vor Windows 8 gewarnt werden sollte, **verbot die Volksrepublik China Windows 8 auf staatlichen Computern**.

Schneier on Trust

Bruce Schneier, Cryptogram, July 2013:

"This is where we are with all the tech companies right now; we can't trust their denials, just as we can't trust the NSA – or the FBI – when it denies programs, capabilities, or practices."

Schlüsselfrage Schlüsselkontrolle

- "(The Microsoft approach) lends itself to market domination, lock out, and not really owning your own computer."

Whitfield Diffie, 2003:

"To risk sloganeering,
I say you need to hold the keys to your own computer"

Nach Snowden: Hintertüren in Soft- und Hardware

- **Nach Snowden** ist dollargenau bekannt, dass die Geheimdienste über einen Milliarden-Etat verfügen, um die Sicherheit von kommerzieller Software und Geräte mit Hintertüren zu versehen.
- **Lesbarer Quellcode** und aufmerksame Entwickler bieten hiergegen Sicherheit.

Code has agency

Bruce Schneier, 5. September 2013

Remember this: The math is good, but math has no agency. Code has agency, and the code has been subverted.

Algorithmen Empfehlungen aus der Kryptoforschung

- **Starke Kryptographie mit extra Sicherheitsspielraum.**

  Dies bedeutet beispielsweise

  - die Verwendung von 256-bit Schlüssellänge für AES
  - Schlüssellänge größer gleich 4096 bit für RSA und DHE
  - 512-bit Hash-Funktion

- Ohne volle Schlüsselkontrolle für die Anwender, ohne lesbaren Code und offene Hardware helfen die besten kryptographischen Verfahren natürlich nicht gegen Geheimdiensthintertüren.

Kryptographische Lösungen nutzen!

- Kryptographie ist eine notwendige Technologie zum Schutz des Gemeinwesens.
- Trotz der viel diskutierten Angriffe ist es stets die schlechteste Lösung ungeschützt zu kommunizieren.
- Kryptographische Lösungen, wie **Digitales Geld** und **anonyme Abstimmungsverfahren**, können eine wünschenswerte Bereicherungen des Zusammenlebens mit sich bringen.
- Viele neue Ideen aus der Kryptographie warten auf Anwendung.

Defense Against the Dark Arts

Eduard Snowden, Guardan, 11. März 2014

"Crypto works. It's not an arcane black art. It is a basic protection, the Defense Against the Dark Arts for the digital world. We must implement it, actively research it"

- **Die Zeit drängt: Gestalten wir den Digitalen Raum.**