Kryptography nach Snowden

Rüdiger Weis

netzpolitischer Abend

Dezember 2013

Kryptographie nach Snowden

- Gute Nachricht: Mathe hilft.
- RC4 kaputt!
- Hintertüren.
- Fallbeispiel: NSA Trusted Computing.
- SSL/TLS richtig einstellen!
- Sicher in die Zukunft.

Die gute Nachricht

Die gute Nachricht ist, dass

- **wissenschaftlich starke Kryptographie auch für übermächtige Geheimdienste nicht brechbar sein dürfte.**
-
- *"Trust the math. Encryption is your friend.",*
  Bruce Schneier, Guardian, 6. September 2013.

Kryptomagie

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.

RC4 genial, aber kaputt

- Nicht mehr verwendet werden sollte die bei SSL/TLS häufig als Standard verwendete RC4-Stromchiffre.
- RC4 ist ein Geniestreich von Ron Rivest.
  - Es ist unglaublich elegant,
  - schnell,
  - mit wenigen Progammzeilen und sogar
  - mit Spielkarten implementierbar.

RC4 zu schön

- Die Kryptographie Forscher stehen allerdings nicht nur mit ehrlicher Bewunderung vor einem derart schönen Algorithmus, er weckt natürlich auch den Ehrgeiz der Angreifer.
- Das Verfahren ist ganz anders konstruiert als gängige Algorithmen und deshalb können neue Angriffe einen Totalschaden herbeiführen, was bei alten, langweiligen Verfahren sehr unrealistisch erscheint.

Nach Snowden: RC4 Echtzeit Durchbruch

- **Nach Snowden** können wir, insbesondere dank der Informationen zu TOR-Angriffen, davon auszugehen, dass die NSA hier vor wenigen Jahren einen Durchbruch erreichen konnte.

stuxnet nutzt Hash-Schwäche

- Eine Analyse von **stuxnet** ergab, dass die **NSA** über bessere Techniken zum Angriff auf die MD4-basierte Hashfunktionen Familie verfügt.
- Auch das inzwischen angewendete und bisher noch nicht gebrochene **SHA2**-Verfahren stammt aus dem Hause der NSA und ist ähnlich konstruiert.
- Das neue Hashverfahren **SHA3** wurde in einem offenen transparenten Wettbewerb ausgewählt und ist bewusst völlig anders konstruiert.

Nach Snowden: Quantencomputer

- ECC sind wegen der kürzeren Schlüssellänge viel anfälliger gegen Angriffe mit Quantencomputern (Shor Algorithmus).
-
- **Nach Snowden** wissen wir centgenau, dass die NSA erheblichen Mittel in die Forschung zu Quantencomputern steckt.

Nach Snowden: NSA und NIST

Dual Elliptic Curve Deterministic Random Bit Generator

- **Nach Snowden** bestätigt sich die Existenz einer NSA-Backdoor in einem NIST Standard.
- Der Vertrauensverlust der Standardisierungsbehörde ist ein harter Schlag für die Informatik.

Problemfall NSA Trusted Computing

- Ein Trusted Computing Modul (TPM) in die persönlichen Computer und Mobilgeräte eingebaut werden. Dieses enthält einen Schlüssel auf den der Besitzer des Computer keinen Zugriffs hat.
- Zusammen mit den nun von Microsoft implementierten Verfahren innerhalb von Windows 8 (insbesondere Secure Boot) wird dem Nutzer weitgehend die Kontrolle über seine eigene Hardware und Software entzogen.

TPM (NSA) Hintertüren

- Das TPM ist ein Dream Chip für die NSA.
- Wenn Wirtschaft und Behörden mittels Windows und Trusted Computing eine Sicherheitsinfrastruktur aufbauen, können die US-Behörden im Zweifelsfall die völlige Kontrolle übernehmen.
- Angesichts der Tatsache, dass wiederholt Druck auf Hardwarehersteller ausgeübt wurde, Hintertüren einzubauen, wirkt die Idee, dass ein Schlüssel vom Benutzer nicht ersetzt werden kann, sehr bedrohlich.

Hintertüren beim Herstellungsprozess

- Besonders brisant ist, dass die geheimen Schlüssel während des Herstellungsprozesses außerhalb des Chips erzeugt und danach in den Chip übertragen werden.
- Hier ist es trivial eine Kopie
  - **aller Schlüssel**
    herzustellen.
- Es ist nicht auszuschließen, dass entsprechende Rechtsvorschriften bestehen und über diese nicht berichtet werden darf.

USA oder China

- Zwar besteht die Hoffnung, dass die USA als demokratischer Rechtsstaat hier Änderungen durchführen wird.
  - Im Kongress wurde 2013 eine stärkere Geheimdienstkontrolle nur sehr knapp abgeleht.
  - Trotzdem ist die im Moment bestehende Rechtslage hier völlig unakzeptabel.
- Das andere realistische Szenario, dass der TPM Hersteller nicht in der Reichweite der NSA sondern in China sitzt, kann nicht wirklich beruhigen.

Code has agency

"Remember this: The math is good, but math has no agency. Code has agency, and the code has been subverted.",
Bruce Schneier, 5. September 2013

Kleptographie

- Es gibt eine eigenes Teilgebiet der Kryptographie namens **Kleptographie**, welches sich unter anderem mit dem
  - sicheren Stehlen von Geheiminformationen durch Manipulation von Software und Hardware beschäftigt.
- Ohne Einsicht in den Source-Code und das Hardware-Design ist der Angegriffene **beweisbar hilflos**.

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.

Exkurs: Lesbarer Quellcode

- **Lesbarer** Quellcode bedeutet nicht zwangsläufig die Verwendung einer offenen Lizenz.
- Auch **veröffentlichter** Quellcode kann unter kommerzielle Lizenzen gestellt werden, die die Verwendung und Weitergabe nahezu beliebig einschränken können.
- **Shared Code** Initiativen, die beispielsweise Microsoft mit verschiedenen Regierungen vereinbart hat, bieten geringeren Schutz, da nicht die gesamte kryptographische Forschungsgemeinde an der Sicherheitsanalyse teilnehmen kann.
- Die **freie Forschung** arbeitet besser als ihre Gegenspieler im Verborgenen und tut dies in der Regel kostenlos für (akademischen) Ruhm und Ehre.

Starke Kryptographie als Standard Einstellung

- Anbieter von Internet-Dienstleistungen sollten verpflichtet werden, sichere Kryptographie als Standardeinstellung zu nutzen.
- Die Enthüllung zum Behördenvorgehen gegen den Mail-Anbieter Lavabit zeigen, wie riskant kryptographisch problematiche Einstellungen sind.

Kompomitierung aller Kunden

- Es scheint noch nicht bei allen Verantwortlichen angekommen zu sein, aber beim Benutzung der Standardeintellungen bedeutet die erzwungene Herausgabe von TLS Schlüsseln die automatische Komprimierung der gesamten, sicherlich von der NSA aufgezeichneten Kommunikation
  - **aller** Kunden.

“Todesurteil für US-Kryptographie “

- Der getroffene Mail-Anbieter Lavabit beendete den Gechäftsbetrieb, Kommentatoren schrieben über das “**Todesurteil für US-Kryptographie**” und
- für US Cloudanbieter könnte die in der Tat das Aus des Nicht-US-Geschäftes bedeuten.

Nach Snowden: Perfect Forward Secrecy

- **Nach Snowden** sollten RSA1024 und RC4 nicht mehr verwendet und die Schlüsselvereinbarung auf **Perfect Forward Secrecy** (PFS) umgestellt werden.

Mindeststandard des BSI

- Im Oktober 2013 veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) den "Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung":
  - "Demnach wird in der Bundesverwaltung das Protokoll TLS 1.2 in Kombination mit Perfect Forward Secrecy (PFS) als Mindeststandard auf beiden Seiten der Kommunikationsbeziehung vorgegeben."

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 RS
  - 512-bit Hash-Funktionen

- Ohne volle Schlüsselkontrolle für die Anwender und 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 freiheitlich demokratischen Gemeinwesens.
- Trotz der viel diskutierten Angriffe ist es stets die schlechteste Lösung ungeschützt zu kommunizieren.
- Werkzeuge wie die Browsererweiterung **HTTPS Everywhere** der Bürgerechtsvereinigung EFF unterstützen sicherere Kommunikation ohne weiteres Zutun.

Kryptographische Forschung nutzen!

- Die kryptographische Forschung entwickelt schon seit vielen Jahren Protokolle, die für die menschliche Gestaltung einer digitalen Gesellschaft hilfreich sein könnten.

Beispiel: Jabber und OTR

- So ermöglicht das in vielen Jabber-Programmen integrierte **OTR**-Protokoll
- soziale Eigenschaften eines privaten Gespräches in der digitalen Welt nachzubilden.
  - Fortschrittliche Kryptographie kann sogar sich bei oberflächlicher Betrachtung ausschliessende Eigenschaften, wie Zurechenbarkeit und Schutz gegen Veröffentlichung, miteinander in Einklang bringen.

Neue Ideen nutzen!

- Auch **digitales Geld** und **anonyme Abstimmungsverfahren** können durchaus wünschenswerte Bereicherungen des Zusammenlebens mit sich bringen.
- Viele neue Ideen aus der Kryptographie warten auf Anwendung.
- Und die Zeit drängt.

Anhang: Schlüssellängen

- Cryptophone 2003:
  - DLP 4096 mit PFS
  - 2x SHA256
  - AES256 XOR Twofish256
- Empfehlungen 2013

RSA	4096
DLP	4096
Hash	512
MAC	512
AES	256

Wenn ECC, dass 512.