Kryptographische Gestaltung Digitaler Lebenswelten

Rüdiger Weis

Center for Digital Cultures Universität Lüneburg, 14. April 2015

Themen

- Digitale Gesellschaft gestalten
- Kryptographie als Grundfundament
- Notwendigkeit von lesbarem Quellcode
- Immer verschlüsseln.
- Kryptowerkzeug: HHTPS Everywhere
- Soziale Protokolle
- Kryptowerkzeug: OTR
- Ausblick: Wahlen, Digitales Geld

Defense Against the Dark Arts

Eduard Snowden, Guardian, 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"

Kryptomagie = Kryptographie + Open Source

Kryptographie

Kryptographie ermöglicht durch Mathematik auf einer kleinerfingernagelgroßen Fläche oder in mit einer handvoll Programmzeilen, Daten sicher selbst gegen eine weltweite Geheimdienstzusammenarbeit zu verschlüsseln.

Freie Software

Freie Software ermöglicht dies kosten- und hintertürenfrei.

Einfache wissenschaftlicher Erklärung

- Kryptographie geht seit jeher bei der wissenschaftlichen Modellbildung von einem fast allmächtigen Gegner aus.

Angreifer

- Der Angreifer kann alle Nachrichten lesen, alle übertragenen Nachrichten ändern.

Verteidiger

- Die einzige Voraussetzung auf Verteidigerseite ist das sichere Erzeugen und Speichern von wenigen Bits für die kryptographischen Schlüssel.

Reine Mathematik

- Kryptographische Algorithmen gehören zu einer Königsdisziplin der Mathematik.
- Die meist zugrunde liegende Zahlentheorie galt über die Jahrhunderte als eines der schwierigsten und reinsten Wissensfelder der Mathematik.
- In der Vor-Computerzeit meinten viele Mathematiker dies durchaus im Sinne von "nicht mit realer Anwendbarkeit beschmutzt".

Schlüsseltechnologie

Schlüsseltechnologie

Gründlich irrten sich hier kluge Menschen, Kryptographie ist zur zentralen Technologien der digitalen Welt geworden und eine der wenigen Technologien bei der Beschleunigung den Schwachen hilft.

Mathematik als Freundin

Bruce Schneier, Guardian, 6. September 2013.

"Trust the math. Encryption is your friend."

Mathematik kann helfen

Mathematik kann der Politik helfen, wo Diplomatie allein sich als machtlos erwiesen hat.

- Die Regierungen weltweit sind daran gescheitert, das flächendeckende Abhören von Bürgern und Industrie zu verhindern.
- Starke Verschlüsselung kann dies.

Kryptographie notwendig

Kryptographie ist eine notwendige Technologie zum Schutz des freiheitlich demokratischen Gemeinwesens.

Open Source

- Freiheit von Hintertüren
- Freiheit von Kosten
- Freiheit von Herstellern

Exkurs: Lesbarer Quellcode

Lesbarer Quellcode

Lesbarer Quellcode bedeutet nicht zwangsläufig die Verwendung einer offenen Lizenz.

Veröffentlichter Quellcode

Veröffentlichter Quellcode kann unter kommerzielle Lizenzen gestellt werden, die die Verwendung und Weitergabe nahezu beliebig einschränken können.

Shared Code

Shared Code

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.

Missbrauch von Shared Code

Dienste nutzen Wissensvorsprung für Angriffe.

Freie Forschung und Open Source

Die freie Forschung und die Open Sorce Gemeinschaft arbeiten besser als ihre Gegenspieler im Verborgenen und tun dies in der Regel kostenlos für (akademischen) Ruhm und Ehre.

Kryptographische Forschung nutzen!

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

Starke Kryptographie als Standard Einstellung

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

Kompomitierung aller Kunden

- Beim Benutzen der SSL Standard-Eintellungen bedeutet die erzwungene Herausgabe von SSL 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 Geschäftsbetrieb, 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.”

Nicht ungeschützt

Trotz der viel diskutierten Angriffe ist es stets die schlechteste Lösung ungeschützt zu kommunizieren.

HTTPS Everywhere

Werkzeuge wie die Browsererweiterung HTTPS Everywhere der Bürgerechtsvereinigung EFF unterstützen unterstützen sicherere Kommunikation ohne weiteres Zutun.

Beispiel: Jabber und OTR

- Das in vielen Jabber-Programmen integrierte OTR-Protokoll ermöglicht die soziale Eigenschaften eines privaten Gespräches in der digitalen Welt nachzubilden.
- Fortschrittliche Kryptographie kann sogar sich bei oberflächlicher Betrachtung ausschließende Eigenschaften miteinander in Einklang bringen.
  - Zurechenbarkeit
  - Schutz gegen Veröffentlichung

Neue Ideen nutzen!

- 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.

Die Zeit drängt:

Gestalten wir den Digitalen Raum.