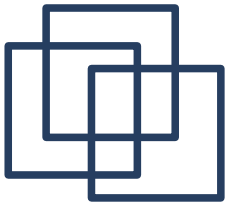
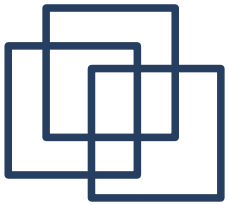


Empfehlungen für den sicheren Einsatz

SSL-verschlüsselter Verbindungen

Dipl.-Inform. Lars Oergel
Technische Universität Berlin

13. Januar 2014



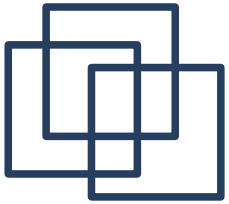
Motivation

Edward Snowden:

„Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.“

Bruce Schneier:

„What I took away from reading the Snowden documents was that if the NSA wants in to your computer, it's in. Period.“



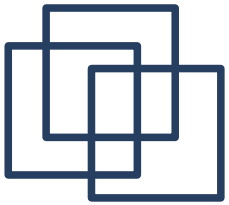
Motivation

Dank Edward Snowden wissen wir, daß die NSA über mächtige Werkzeuge verfügt, um in annähernd jede datenverarbeitende Anlage eindringen zu können. Allerdings sind diese gezielten Angriffe sehr aufwendig und damit teuer!

Der Großteil der abgelauschten Daten wird „im“ Internet, d.h. an Routern, Seekabeln und Satellitenverbindungen sehr effizient und kostengünstig abgehört.

Davor kann uns der korrekte Einsatz starker Kryptografie schützen!

Oft wird hierzu das SSL-Protokoll benutzt.



Das SSL-Protokoll

Das SSL-Protokoll kombiniert mehrere kryptografische Verfahren zur Absicherung einer Internetkommunikation:

- Symmetrische Verschlüsselungsverfahren
  ver- und entschlüsseln die Daten mittels geheimer Schlüssel.
- Asymmetrische Verschlüsselungsverfahren
  ermöglichen den sicheren Schlüsselaustausch geheimer Schlüssel und die Authentisierung des Kommunikationspartners.
- Digitale Signaturen
  schützen die Daten vor Verfälschungen während des Transports.

SSL-Protokollversionen

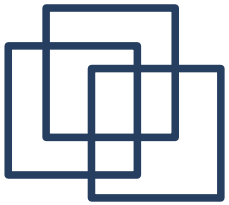
Bisherige SSL/TLS-Protokollversionen:

- 1994 SSL 1.0: UNSICHER! Vermeiden!
- 1995 SSL 2.0: UNSICHER! Vermeiden!
- 1996 SSL 3.0: Veraltet! Vermeiden!

- 1999 TLS 1.0: „Kleinster gemeinsamer Nenner“
- 2006 TLS 1.1: Update, leider selten implementiert
- 2008 TLS 1.2: Aktuell, leider selten implementiert

Empfehlung: SSL 3.0 abschalten!

Firefox: Einstellungen -> Erweitert -> Verschlüsselung: SSL 3.0 abhaken



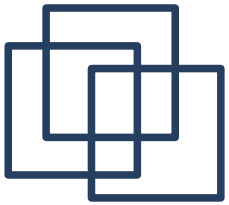
Symmetrische Verschlüsselung

Wichtige Verfahren:

- 1975 DES: Schlüssellänge nur 56 Bit! Vermeiden!
- 1987 RC4: galt lange als „Standardverfahren“ - gilt aber heute als in Echtzeit von der NSA knackbar!
- 1998 AES: Aktuelles Standardverfahren! Gilt als sicher!
- 2000 Camellia: Japanisches Verfahren, neuer, aber weniger weit verbreitet als AES, weniger getestet.

Empfehlungen: RC4 aus! Schlüssellänge mind. 128 Bit!

Firefox: about:config, nach „RC4“ suchen und Einträge auf „false“ setzen



Asymmetrische Verschlüsselung

Wichtige Verfahren:

- 1976 Diffie-Hellman (DH)
- 1977 Rivest-Shamir-Adleman (RSA)

Beide Verfahren gelten ab einer Schlüssellänge von 2048 Bit als sicher!

Einige DH-Varianten bieten „Forward Secrecy“. Damit kann das nachträgliche Entschlüsseln mitgeschnittener Kommunikation durch die NSA verhindert werden!

Empfehlung: FS-Verfahren wie „DHE“ oder „ECDHE“

Manche Browser zeigen das Verfahren an, ansonsten: ssllabs.com (s.u.)

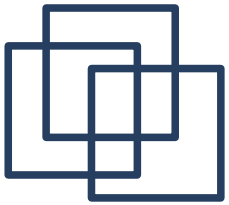
SSL-Zertifikate

SSL-Zertifikate dienen der Authentisierung des Partners. Ansonsten wäre eine „Man-in-the-middle-Attack“ möglich, bei der sich ein Angreifer zwischen den beiden Partnern befindet und die Daten dann „für sich“ verschlüsseln läßt!

„Vertrauenswürdige“ Zertifizierungsstellen sind in alle Browser eingebaut. Sie stellen „offizielle“ Zertifikate aus.
Anzeige im Firefox: Einstellungen->Verschlüsselung->Zertifikate anzeigen

Seit dem 10. Januar 2014 sind alle unsere externen Dienste mit offiziellen SSL-Zertifikaten abgesichert:

- webmail.cfd.tu-berlin.de
- owncloud.cfd.tu-berlin.de
- submission.cfd.tu-berlin.de
- imap.cfd.tu-berlin.de



Überprüfen der Verschlüsselung

Bei den meisten modernen Browsern erscheint bei SSL-verschlüsselten HTTPS-Verbindungen ein Schloßsymbol neben der Adreßleiste. Durch Anklicken des Symbols können Informationen über die eingesetzten Verfahren und Schlüssellängen abgerufen werden. Auch das vom Server vorgezeigte Zertifikat kann eingesehen werden.

Die Webseite SSLLabs.com bietet einen SSL-Servertest an, der alle Sicherheitsaspekte einer SSL-Verbindung eingehend überprüft und schulnotenmäßig bewertet.

Sehr zu empfehlen, auch fürs private Mailen, Einkaufen, Homebanking usw.!

(Es soll ja immer noch Bankwebseiten mit RC4-Verschlüsselung geben...)

Literatur / Quellen

http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower

http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance

https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.3.pdf

http://www.heise.de/security/meldung/NSA-entschluesselt-Webserver-Daten-angeblich-in-Echtzeit-2041383.html

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03023.html

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Klaus Schmeh, Kryptografie: Verfahren - Protokolle - Infrastrukturen, ISBN 978-3864900150

http://www.cfd.tu-berlin.de/Lehre/EDV2/dokus/Verschluesselung.ps