Funkkolleg 2016/2017

Sicherheit

Zusatzmaterial zur Sendung 07:
Verschlüsselung ist gut - Warum nutzt sie bloß keiner?

vhs Die Volkshochschulen in Hessen

TECHNISCHE UNIVERSITÄT DARMSTADT

HESSEN Hessisches Kultusministerium

hr iNFO

Zusatzmaterial zur Folge 07
Verschlüsselung ist gut – Warum nutzt sie bloß keiner?

Livestream und Podcast: www.hr-inforadio.de

Interessierte Hörerinnen und Hörer finden auf dieser Seite weiterführende Informationen zu den einzelnen Sendungsthemen als Zusatzmaterial. Die Materialien wurden zum Zugriffszeitpunkt 16.12.2016 erstellt von:
Markus Stegeman, Fachgebiet Wirtschaftsinformatik | Software Business & Information Management, Technische Universität Darmstadt

Inhalt

1. Forschungsstudien

Untersuchung von kryptographisch relevanten OpenSSL-Aspekten

Die Kryptobibliothek OpenSSL wird seit mehreren Jahren in verschiedenen kryptographischen Systemen eingesetzt. Sie ist besonders wichtig bei gesicherten Datenübertragungen in Computernetzwerken und spielt aufgrund ihrer großen Verbreitung im Internet eine besonders wichtige Rolle bei der Verwendung von HTTPS (HTTP over SSL/TLS). OpenSSL bietet eine große Zahl von kryptographischen Funktionen an.

Die vorliegende Studie ist eine Untersuchung der OpenSSL-Bibliothek im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI), durchgeführt von der Sirrix AG (als Hauptauftragnehmer) und der 3curity GmbH (als Unterauftragnehmer).

Quelle: Bundesamt für Sicherheit in der Informationstechnik: Quellcode-basierte Untersuchung von kryptographisch relevanten Aspekten der OpenSSL-Bibliothek, 2015

Link: https://www.bsi.bund.de/DE/Publikationen/Studien/OpenSSL-Bibliothek/opensslbibliothek.html;jsessionid=90AB61BD5FA10F04D550779DDD48BFB3.1_cid090

2. Industrienahe Studien

Verschlüsselter Datenverkehr nimmt zu

Laut einer Studie steigt seit Beginn der Enthüllungen des Whistleblowsers Edward Snowden der Anteil an SSL-verschlüsselten Verbindungen im Internet. Die Zunahmen in den USA und Europa unterscheiden sich aber. Dieser Bericht von heise online fasst die Ergebnisse zusammen.

Quelle: heise online: Statistik: Verschlüsselter Datenverkehr nimmt zu, 16.05.2014

Link: https://www.heise.de/newsticker/meldung/Statistik-Verschluesselter-Datenverkehr-nimmt-zu-2191276.html

Verschlüsselung von E-Mails kommt nur langsam voran

Der Einsatz von Verschlüsselungsverfahren für den Schutz von privaten Daten kommt nur langsam voran. Das hat eine repräsentative Umfrage im Auftrag des Digitalverbands Bitkom ergeben. Demnach verschlüsselten im letzten Jahr 15 Prozent der deutschen Internetnutzer E-Mails. Zum Vergleich: Im Jahr davor waren es mit 14 Prozent ähnlich viele.

Quelle: bitkom: Verschlüsselung von E-Mails kommt nur langsam voran, 21.01.2016

Link: https://www.bitkom.org/Presse/Presseinformation/Verschluesselung-von-E-Mails-kommt-nur-langsam-voran.html

Verschlüsselung ist global: Hintertüren wären sinnlos, zeigt neue Studie

In den letzten Monaten ist die Debatte um Verschlüsselung neu entflammt. Eine neue Studie verdeutlicht nun den Unsinn von Verschlüsselungs-Verboten und dem Einbau von Hintertüren anhand greifbarer Zahlen. Wissenschaftler haben eine beeindruckende Liste von über 800 verschiedenen Verschlüsselungs-Produkten aus 55 Ländern erstellt. Sie zeigt, dass es immer Alternativen geben wird, welche außerhalb der Reichweite von Ermittlungsbehörden liegen.

Quelle: Rebiger, Simon: Verschlüsselung ist global: Hintertüren wären sinnlos, zeigt neue Studie, Netzpolitik.org, 11.02.2016

Link: https://netzpolitik.org/2016/verschluesselung-ist-global-hintertueren-waeren-sinnlos-zeigt-neue-studie/

Harvard-Studie: Strafverfolger werden nicht "blind" durch Verschlüsselung

Die Befürchtungen von Ermittlern, in den neuen sogenannten "Crypto Wars" (Verschlüsselungs-kriege) aufgrund zunehmender Verschlüsselung Verdächtige nicht mehr überwachen zu können, sind laut Harvard-Experten stark übertrieben. Die Ergebnisse der Studie erklärt heise online.

Quelle: Krempl, Stefan: Harvard-Studie: Strafverfolger werden nicht "blind" durch Verschlüsselung, heise online, 02.02.2016

Link: https://www.heise.de/newsticker/meldung/Harvard-Studie-Strafverfolger-werden-nicht-blind-durch-Verschluesselung-3090248.html

3. Sonstiges

3.1. Literatur

Harte Nüsse - Verschlüsselungsverfahren und ihre Anwendungen

Wer Daten über einen unsicheren Kanal wie Internet oder Wireless-LAN versendet, kann sich nur durch Verschlüsseln vor dem unbefugten Mithören schützen. Das ist leichter gesagt als getan: Nicht nur der Verschlüsselungsalgorithmus selbst muss Angriffen widerstehen können, sondern auch der Schlüssel. Das kryptographische Protokoll muss ebenso wasserdicht sein wie seine Implementierung, und nicht zuletzt ist oft der Benutzer die größte Sicherheitslücke. Aus dieser Kette greift der folgende Artikel nur ein Glied heraus, die kryptographischen Algorithmen.

Quelle: Wobst, Reinhard: Harte Nüsse. Verschlüsselungsverfahren und ihre Anwendungen, heise.de, 08.08.2003

Link: https://www.heise.de/security/artikel/Harte-Nuesse-Verschluesselungsverfahren-und-ihre-Anwendungen-270266.html

Was leisten die aktuellen kryptographischen Verfahren für die Medizin?

Kryptographie ist die Grundlage für wirksame Datensicherheit in offenen und verteilten Systemen. Sie kann das Arztgeheimnis, die Integrität und Verbindlichkeit von Dokumenten sowie die Authentizität von Netzteilnehmern sichern. Auf kryptographischen Basisfunktionen bauen kryptographische Protokolle auf, die über eine geeignete Infrastruktur zu sicheren Anwendungs- und Kommunikationssystemen führen. Als Beispiele für den Einsatz kryptographischer Verfahren in der Medizin wird die Pseudonymisierung in medizinischen Forschungsnetzen sowie der Betrieb von sicheren Web-Diensten, etwa für Befundserver, vorgestellt. Kryptographische Verfahren werden im medizinischen Umfeld bereits an vielen Stellen eingesetzt, oft ohne dass der Nutzer dies explizit merkt.

Quelle: Pommerening, Klaus: Was leisten die aktuellen kryptographischen Verfahren für die Medizin?, Mainz, 2011

Link: https://www.staff.uni-mainz.de/pommeren/Artikel/Pomm_Krypt.pdf

Als weiterführende Literatur empfehlen wir:

- Kippenhahn, Rudolph: Verschlüsselte Botschaften: Geheimschrift, Enigma und digitale Code, Rowohlt Taschenbuch Verlag, Berlin, 2012
- Singh, Simon: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, dtv Verlagsgesellschaft, München, 2001

3.2. Video/Audio

Sicher, aber praktisch? - eMail-Verschlüsselung im Praxistest

Mit der so genannten „Volksverschlüsselung“ soll jeder Mensch seine eMails abhörsicher versenden können. Aber wie gut funktioniert das im Alltag? Wie praktikabel ist das? Und: Lohnt sich das überhaupt für den Laien? Ein Beitrag des WDR5.

Link: http://www1.wdr.de/mediathek/audio/wdr5/wdr5-leonardo-service-computer/audio-sicher-aber-praktisch---email-verschluesselung-im-praxistest-100.html

Neue Verschlüsselung bei WhatsApp

Der weltweit verbreitete Kommunikationsdienst WhatsApp hat den Datenschutz für seine Nutzer erhöht: Für alle verschickten Inhalte gibt es nun eine sogenannte Ende-zu-Ende-Verschlüsselung. Damit soll es nur noch dem Absender und dem Empfänger möglich sein, auf die verschickten Inhalte zuzugreifen – selbst WhatsApp kann eigenen Angaben zufolge die Inhalte nicht einsehen. In „Volle Kanne“ (ZDF) werden die Änderungen diskutiert.

Link: https://www.zdf.de/verbraucher/volle-kanne/was-bringt-die-ende-zu-ende-verschluesselung-bei-whatsapp-100.html

Mathematik zum Anfassen - Kryptographie

In diesem Beitrag des Bayrischen Rundfunks (BR) werden grundlegende Begriffe und Verfahren der Kryptographie erklärt.

Link: http://www.br.de/mediathek/video/sendungen/mathematik-zum-anfassen/mathematik-zum-anfassen-albrecht-beutelspacher-kryptographie100.html

3.3. Webseiten

Kryptowissen.de

Die Seite Kryptowissen.de beschäftigt sich mit den Themen Kryptologie, Kryptographie und Kryptoanalyse. Es werden unter anderem die Unterschiede zwischen asymmetrischer und symmetrischer Verschlüsselung und verschiedene Verschlüsselungstechniken vorgestellt. Darüber hinaus enthält die Seite Links zu weiterführenden Informationen.

Link: www.kryptowissen.de

CrypTool

Das CrypTool-Portal ermöglicht jedermann einen einfachen Zugang zu Verschlüsselungs-Techniken. Alle Lernprogramme im CT-Projekt sind Open-Source und kostenlos. Das CrypTool-Projekt entwickelt die weltweit am meisten verbreitete E-Learning-Software für Kryptographie und Kryptoanalyse.

Link: www.cryptool.org

3.4. Forschungsgruppen

CROSSING (TU Darmstadt)

Das kollaborative Forschungscenter CROSSING verfolgt das Ziel, Kryptographie-basierte Sicherheitslösungen bereitzustellen, die Vertrauen in neue und innovative IT-Umgebungen schaffen. Diese Lösungen sollen dabei sowohl für Anwender als auch für Entwickler und Administratoren einfach zu nutzen sein.

Link: https://www.crossing.tu-darmstadt.de/en/crossing/?no_cache=1

3.5. Zeitschriften

Wie funktioniert ein Quantencomputer?

Auch wenn Forscher weltweit auf dieses Ziel hinarbeiten, Quantencomputer außerhalb der Laborsituation wird es erst einige Jahrzehnte in der Zukunft geben. Allerdings sah noch vor siebzig bis achtzig Jahren die Situation bei herkömmlichen Computern ähnlich aus. Als Universalrechner wird sich ein Quantencomputer jedoch auch künftig nicht durchsetzen.

Quelle: Kusche, Nora: Wie funktioniert ein Quantencomputer?, Welt der Physik, 26.02.2016

Link: http://www.weltderphysik.de/gebiet/technik/quanten-technik/einfuehrung-quantencomputer/

Anti-Terror-Kampf im Internet – Bundesregierung sucht Nerds

Terroristen kommunizieren oft über verschlüsselte Botschaften, auch die Attentäter von Ansbach und Würzburg. Die Bundesregierung will nun eine Einheit zur Entzifferung solcher Chats aufbauen - doch es fehlt an Personal.

Quelle: Gebauer, Matthias; Gruber, Angela: Anti-Terror-Kampf im Internet. Bundesregierung sucht Nerds, Der SPIEGEL, 01.08.2016

Link: http://www.spiegel.de/politik/deutschland/bundesregierung-sucht-verzweifelt-nerds-a-1105653.html

4. Personen

Prof. Dr. Johannes Buchmann leitet das Fachgebiet „Theoretische Informatik - Kryptographie und Computeralgebra“ an der TU Darmstadt. Die Forschung beinhaltet u.a. die Themengebiete Kryptoanalyse und Seitenkanalangriffe, Post-Quantum Kryptographie, Public-Key Infrastrukturen, Langzeitsicherheit und Software-Cluster.

Professor Buchmann ist Experte für Kryptographie, Leibnizpreisträger 1993 und Mitglied der Akademie der Wissenschaften und der Literatur Mainz, der Berlin-Brandenburgischen Akademie der Wissenschaften sowie der Deutschen Akademie der Naturforscher. Zudem entwickelte er das Datensicherheitskonzept des fälschungssicheren Reisepasses.

Link: https://www.informatik.tu-darmstadt.de/de/fachbereich/professoren-des-fachbereichs/single-view/artikel/prof-dr-johannes-buchmann/