Modul I423 Informationssicherheit und Datenschutz

Thema 1: Einführung

Robert Baumgartl

11. Oktober 2020

Organisatorisches

. . . finden Sie unter

https://www.informatik.htw-dresden.de/~robge/isds/isds.html

Ressourcen

Vorlesungsunterlagen, Bücher

- Vorlesungsfolien (im PDF), Praktikumsaufgaben, aktuelle Informationen erscheinen im Laufe des Semesters unter *http://www.informatik.htw-dresden.de/~robge/is/is.html*
- Bruce Schneier. *Angewandte Kryptographie*. Pearson, 2006 (besser die englische Ausgabe von 1996)
- Matt Bishop. *Introduction to Computer Security*. Prentice Hall, 2004
- Albrecht Beutelspacher. *Kryptologie*. 9. Aufl. Vieweg+Teubner, 2009
- Ross Anderson. *Security Engineering*. 2. Aufl. Wiley, 2008
- Introduction to Cryptography by Christof Paar (https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg)

Ressourcen

Web, Vorschläge

- *https://www.schneier.com*
- *http://www.phrack.org*
- *https://www.kali.org/*
- *https://computer-forensik.org*
- *https://www.ccc.de*
- *https://www.lightbluetouchpaper.org/*
- *https://insecure.org*
- *https://www.alchemistowl.org/pocorgtfo/*

Ressourcen

Belletristik

- Thomas Harris. *Enigma*. TB 01/10001. Heyne, 1995
- Clifford Stoll. *Kuckucksei*. Fischer, 1989
- Neal Stephenson: Cryptonomicon. Goldmann, 1999
- Dan Brown: Digital Fortress. 1998 (deutsch: „Diabolus“)[1]

[1] Keine wirkliche Empfehlung; das Buch demonstriert vor allem die Unkenntnis des Autors.

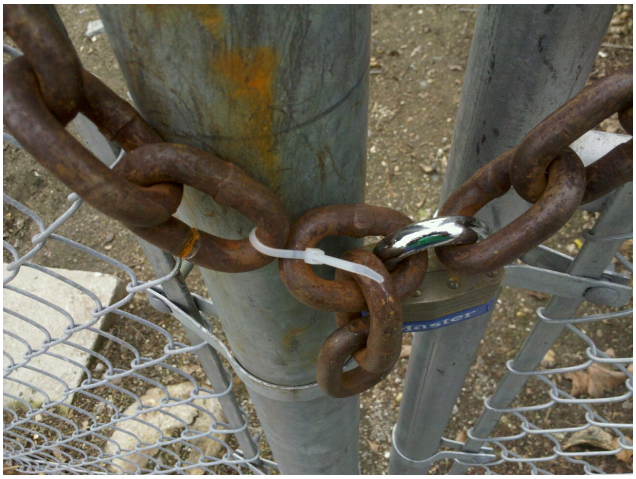
Motivation

Schlagzeilen der letzten Zeit

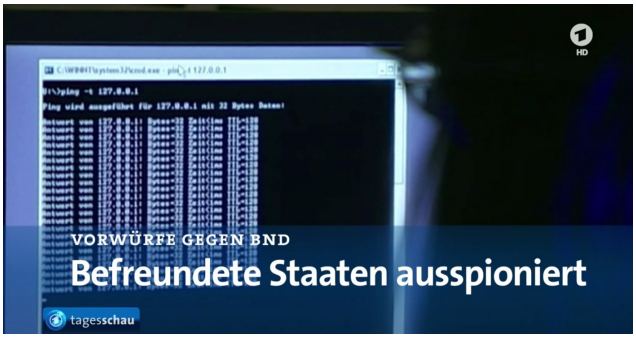
- 2.2 Milliarden Passwort-Credentials gestohlen und veröffentlicht (Link, 25. 01. 2019)
- Cambridge Analytica hat 50 Millionen Facebook-Profile gescrapet und ggf. missbraucht (Link, 21. 03. 2018)
- Gravierende Prozessor-Sicherheitslücken: *Meltdown* und *Spectre* (Link, 04. 01. 2018)
- „Schutz durch Speicherverwürfelung ASLR geknackt“ (Link, 15. 02. 2017)
- „Todesstoß: Forscher zerschmettern SHA-1“ (Link, 23. 02. 2017)
- „Vault 7: Wikileaks präsentiert Liste der CIA-Hacker-Werkzeuge“ (Link, 23. 02. 2017)
- „Kriminelle bieten Mirai-Botnetz mit 400.000 IoT-Geräten zur Miete an“ (Link, 25. 11. 2016)

Motivation

Motivation



Motivation



Inhalt der Lehrveranstaltung

- Einführung, Motivation, Grundlagen, Begriffe
- Klassische Verfahren und Angriffe auf diese
- (kryptografische) Hashfunktionen, Kollisionen, Geburtstagsparadoxon, Signaturen,
- Moderne symmetrische Verschlüsselungsverfahren (DES, AES, IDEA)
- mathematische Grundlagen
- asymmetrische Verfahren (Diffie-Hellman, RSA, ElGamal)
- kryptografische Algorithmen, Schlüsselverwaltung, API, Werkzeuge
- Zugangskontrolle, Passwortsysteme, Rainbow Tables
- Anonymität, Mixe, Tor
- Zero-Knowledge-Protokolle
- Programme mit Schadensfunktion (Malware)

Was machen wir hier *eigentlich*?

Beschäftigung mit den grundlegenden Anforderungen an die Sicherheit beim Betrieb von Rechensystemen:

- **Vertraulichkeit**,
- **Integrität**,
- **Verfügbarkeit**.

Des weiteren widmen wir uns den Aspekten

- Authentizität/Authentifizierung,
- Zurechenbarkeit/Nichtabstreitbarkeit,
- Anonymität.

Szenarien: Angriffe und Gegenmaßnahmen

Handhabung ausgewählter Werkzeuge für die Praxis

Betrachtung *beider* Seiten

(vgl. Modulbeschreibung I-423)

Schutzziel: Vertraulichkeit (Confidentiality)

- ist das **Verbergen von Informationen**
- sensitive Daten, z. B.
  - personenbezogen
  - der militärischen Geheimhaltung unterliegend
  - Geschäftsgeheimnisse
- wird durch Mechanismen bzw. Dienste gewährleistet, z. B.
  - Ver- und Entschlüsselung (Kryptografie)
  - Verbergen in „unverdächtigen“ Daten (Steganografie)
  - Zugriffssteuerung (Access Control)
- erfordert Unterstützung durch das System

Schutzziel: (Daten-)Integrität

- Verhinderung der Verfälschung von Daten, Ressourcen etc.
- „Kann ich den Daten trauen?“
- realisiert durch
  - Verhinderung unautorisierten Schreibzugriffs
  - Erkennung einer Integritätsverletzung (z. B. durch kryptografische Prüfsummen)
- Unterscheidung der Integrität der Daten selbst sowie der datengenerierenden Quelle
- Verletzung der Integrität möglich durch
  - unautorisierte Personen (Angriff von außen)
  - autorisierte Personen (Angriff von innen)

Schutzziel: Verfügbarkeit (Availability)

- bezüglich einer Ressource, eines Dienstes, bestimmter Informationen
- auch ein Aspekt der Systemzuverlässigkeit (Security vs. Safety)
- *Denial of Service Attack* vermindert bzw. eliminiert die Verfügbarkeit o. g. Ressourcen, Dienste etc. → wirtschaftlicher Schaden
- meist (aber nicht immer) gegen einzelne Server, Firmen etc. gerichtet

Beispiel: Hackerangriff auf Bundestag 2015

- im Mai 2015 wurde bekannt, dass das gesamte Computernetz des Bundestags Ziel eines Hackerangriffs sei
- Ausgangspunkt: Phishingangriff via Mail (`un.org`), Link auf Seite mit Schadsoftware
- 1 Rechner mit Trojaner infiziert, Verschaffung von Admin-Passworten
- Konsequenz: viertägige (!) Abschaltung des gesamten Netzes
- Ziel war wahrscheinlich der Diebstahl aller möglichen Dokumente (.pdf, .xls, .xlsx, .doc, .docx)

Literatur:

- https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/
- https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/

Policy und Mechanism (Strategie und Mechanismus)

Eine **Sicherheitsstrategie** (security policy) ist die Formulierung, welche Aktionen für welche Nutzer erlaubt bzw. verboten sind.

Ein **Sicherheitsmechanismus** (security mechanism) ist eine Methode oder Vorgehensweise, eine gegebene Sicherheitsstrategie zu verwirklichen.

Beispiel:
Strategie: Jeder Nutzer hat ausschließlich Zugriff auf sein Homeverzeichnis.
Mögliche Mechanismen:

a) BS prüft jeden Zugriff auf Dateisystem, verwehrt Zugriffe auf 'fremde' Dateien

b) jeder Nutzer besitzt mobilen Datenträger (USB-Stick), der sein Homeverzeichnis enthält

c) nutzerspezifische Verschlüsselung der Homeverzeichnisse

Mechanismen können kombiniert werden!

Bedrohungen (Threats)

Eine Bedrohung ist eine *potentielle* Verletzung der Sicherheitsstrategie.

(eine) Möglichkeit der Klassifizierung:

- Aufdeckung (Disclosure) - unautorisierter Zugang zu Informationen (Abhören, Durchsuchen, Kopieren)
- Täuschung (Deception) - Fälschung von Daten
- Unterbrechung (Interruption) - Das System funktioniert nur noch teilweise oder gar nicht mehr
- Übernahme (Usurpation) - das System wird teilweise oder vollständig durch Dritte genutzt und gesteuert

Einige Gesetzestexte

§202a StGB: „Ausspähen von Daten“

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Einige Gesetzestexte

§202b StGB: „Abfangen von Daten“

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

(in Kraft getreten am 7. August 2007)

Der „Hackerparagraf“

§202c StGB: „Vorbereiten des Ausspähens und Abfangens von Daten“

(1) Wer eine Straftat nach §202a oder §202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§202a Abs.2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.

(2) §149 Abs.2 und 3 gilt entsprechend.

„Datenhehlerei“

§202d StGB, 2015

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie
2. solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

Straffreiheit

§149 StGB: „Vorbereitung der Fälschung von Geld und Wertzeichen“

(2) Nach Absatz 1 wird nicht bestraft, wer freiwillig

1. die Ausführung der vorbereiteten Tat aufgibt und eine von ihm verursachte Gefahr, daß andere die Tat weiter vorbereiten oder sie ausführen, abwendet oder die Vollendung der Tat verhindert und
2. die Fälschungsmittel, soweit sie noch vorhanden und zur Fälschung brauchbar sind, vernichtet, unbrauchbar macht, ihr Vorhandensein einer Behörde anzeigt oder sie dort abliefert.

(3) Wird ohne Zutun des Täters die Gefahr, daß andere die Tat weiter vorbereiten oder sie ausführen, abgewendet oder die Vollendung der Tat verhindert, so genügt an Stelle der Voraussetzungen des Absatzes 2 Nr. 1 das freiwillige und ernsthafte Bemühen des Täters, dieses Ziel zu erreichen.

(*http://dejure.org/gesetze/StGB/*)

Zusammenfassung §202

- Früher: Bloßes Eindringen in fremde Systeme nicht strafbar.
- Nun: Unbefugter Zugang unter Überwindung von Sicherheitsvorkehrungen ist strafbar!
- Hauptmangel: fehlende präzise Definition strafrechtlich relevanter Werkzeuge („Hackertools“)
- Werkzeuge nach § 202b sind offensichtlich auch viele Sicherheitstools, deren Einsatz zur *Gewährleistung* der Systemsicherheit unabdingbar ist?!
- Gesetz wurde ziemlich kontrovers diskutiert, im Mai 2007 in Kraft gesetzt.
- „Gutartige“ Verwendung von Hackertools ist bislang nicht bestraft worden.

„Literatur“: Chaosradio CR 137 *Der Hackerparagraph. Der §202c auf dem Prüfstand.* Podcast vom 31. 7. 2008 *http://chaosradio.ccc.de/cr137.html*

Beispiel: John the Ripper

- Passwortcracker für Unix und Windows
- *http://www.openwall.com/john/*
- gern genutzt, um schwache Passphrasen zu entdecken (und damit die Systemsicherheit zu *erhöhen*)
- Download und Verbreitung ist nach § 202c strafbar, Nutzung im o. g. Sinne nach § 202a möglicherweise auch

Einige Formen der Computerkriminalität

ohne Anspruch auf Vollständigkeit

- Einbruch
- Identitätsdiebstahl
- Spionage
- Denial-of-Service (z. B. www.bundeskanzlerin.de, 7. 1. 2015)
- Sabotage (z. B. Stuxnet)
- Manipulation (Fälschen) von Daten (z. B. *Defacement* von Webseiten)
- Spamming
- unerlaubte Verbreitung urheberrechtlich geschützter Werke („Piraterie“)
- unerlaubte Beschaffung persönlicher Daten, Kreditkartennummern, Passwörtern mittels gefälschter Mails und Webseiten (*Phishing*)
- . . .

Beispiel: Defacement

Website der Brazilian Air Force, 3. 9. 2013

Zusammenfassung: Was haben wir gelernt?

1. Warum gibt es das Fach *Informationssicherheit*?
2. 3 Säulen: Vertraulichkeit, Integrität, Verfügbarkeit
3. Was beinhaltet der *Hackerparagraf* und verwandte Gesetze?