KRYPTOLOGIE UND SYSTEMSICHERHEIT

Sommersemester 2020

Technische Hochschule Mittelhessen

Andre Rein

– Motivation –

INFORMATIONEN ZU MIR

Prof. Dr.-Ing. Andre Rein <andre.rein@mni.thm.de>
http://homepages.thm.de/~arin07

- 2000 Ausbildung IT-Fachinformatiker
- 2003 THM — Studium, Systemadmin und Softwareentwicklung
- 2011 Fraunhofer SIT — WiMi
- 2015 Huawei - Cyber Security and Privacy Lab (CSPL) — Security Technologist
- 2018 Universität Bremen: Promotion Dr.-Ing.
- 2019 THM Professor für IT-Security (und Kerninformatik) :)

- Erfahrung
  - 11 Jahre im Security Bereich (9 Jahre davon professionell)
  - 21 Jahre Linux and Unix (*BSD)
- Privates
  - 40 Jahre, verheiratet
  - Laufen, Bergwandern, Klettern
  - Binge-Watching Serien

INFORMATIONEN ZUR VERANSTALTUNG

Die Lehrveranstaltung ist eine Wahl-Pflichtveranstaltung im Modulpool *theoretische Informatik* im Masterstudiengang Informatik und eine freie Wahl-Pflichtveranstaltung in Ingenieursinformatik.

SMU	Mittwoch	15:45 - 17:15	Online	Rein
SMU	Mittwoch	17:30 - 19:00	Online	Rein

INFORMATIONEN ZUR VERANSTALTUNG

- **Leistungsnachweis:** Der Leistungsnachweis für das Fach "Kryptologie und Systemsicherheit" wird durch eine erfolgreiche Teilnahme an der Klausur erbracht
- **Teilnahmevoraussetzung an der Klausur:** Erfolgreiche Bearbeitung und Abgabe von einer anerkannten Hausübungen/Projekt/Vortrag (TBD!)
- **Klausurtermine:** Die Klausur findet, soweit nichts anderes bekanntgegeben wird, in der Klausurwoche vor den Semesterferien statt

Modulbeschreibung

LITERATUR

1. Christoph Paar/Jan Pelzl: Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender (ISBN: 9783662492963)
2. Bruce Schneier: Angewandte Kryptographie - Protokolle, Algorithmen und Sourcecode in C (ISBN: 3827372283)

GIT, MOODLE UND FRAGEN

- GIT: https://git.thm.de/arin07/it_sec_crypto_public/
- Moodle: https://moodle.thm.de/course/view.php?id=3569
- Discord: https://discord.gg/9syP5g2

FRAGEN

???

ÜBERSICHT

KURSINHALTE

- Motivation, Übersicht und Schutzziele (Security Goals)
- Historische kryptographische Methoden und Verfahren
- Moderner Kryptographie: Algorithmen, Methoden und Verfahren
  - Verschlüsselung (symmetrisch/ asymmetrisch)
  - Message Authentication Codes (MACs)
  - Kryptographische Hash Funktionen
  - Schlüsselverwaltung und Schlüsseltausch
  - Digitale Signaturen
- Modulare Arithmetik
- Anwendung moderner Kryptographie
  - Protokolle
  - Systemsicherheit

FRAGEN

???

– Schutzziele –

SICHERHEITSANFORDERUNGEN (SCHUTZZIELE)

Information Security

Definition vom NIST

> *The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.*

https://csrc.nist.gov/glossary/term/information-security

IT-SECURITY: SCHUTZZIELE ✍️

- Informieren Sie sich im Internet über Schutzziele (Security Goals)
  - ⏱️ Bearbeitung: 15 Minuten → Kurzes sammeln und diskutieren der gefundenen Ergebnisse
- Wir bilden für jedes Schutzziel eine Gruppe und erarbeiten innerhalb der Gruppe eine kurze Zusammenfassung (Vorlage) mit folgenden Inhalten:
  - Um was geht es bei dem Schutzziel?
  - Welche Methoden und Verfahren können werden hier verwendet werden?
  - Suchen Sie nach Definitionen (deutsch oder englisch) für das Ihnen zugeteilte Schutzziel und einigen Sie sich in der Gruppe auf eine oder zwei Definitionen, die Sie für passend halten
  - Wenn Sie vorzeitig fertig sind, diskutieren Sie inwiefern sich Ihr Schutzziel mit anderen Schutzzielen kombinieren lässt und wann oder ob dies sinnvoll wäre!
- ⏱️ Bearbeitung: 30 Minuten!

SCHUTZZIELE UND ANGREIFERVERHALTEN

	Aktiv	Passiv	Bedrohte Schutzziele
Beobachten	(✔)	✔	Vertraulichkeit
Manipulieren	✔	×	Vertraulichkeit, Integrität, Verfügbarkeit

Ohne Authentizität können Manipulationen **oft** nicht einmal erkannt werden. Z.B. Man-in-the-Middle Angriffe. (Ohne Nachweisbarkeit kann abgestritten werden, dass etwas gesendet wurde.)

SCHUTZZIELE: ANFORDERUNGEN ✍

- Anforderung: Eine Anwendung sammelt u.a. personenbezogene Daten die vor unbefugtem Zugriff "geschützt" werden sollen.
- Welche Schutzziele gilt es für das "schützen" der Daten zu beachten?
- Welche technischen / organisatorischen Maßnahmen würden Sie ergreifen um die Schutzziele zu erfüllen?
- ⏱ Bearbeitung: 15 Minuten → dann sammeln und diskutieren!

SCHUTZZIELE CIAA+ ✍

- Verbessern / Ergänzen Sie Ihre Zusammenfassung zu Ihrem Schutzziel
- Hat sich die Sichtweise auf Ihr und auf die anderen Schutzziele geändert?
- Überlegen und diskutieren Sie: In welchem Zusammenhang stehen die Schutzziele mit dem Kursinhalt zur Kryptographie und Systemsicherheit?

- ⏱ Bearbeitung: 15 Minuten → Abschließende Diskussion!
- Überarbeiten Sie die Zusammenfassung und senden mir diese per E-Mail

ÜBERSICHT SCHUTZZIELE

CONFIDENTIALITY 🎯 (VERTRAULICHKEIT)

NIST

📖 *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*

https://csrc.nist.gov/glossary/term/confidentiality

BSI

📖 *Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.*

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html

INTEGRITY 🎯 (INTEGRITÄT)

NIST

> 📖 *Guarding against improper information modification or destruction […]*

https://csrc.nist.gov/glossary/term/integrity

BSI

> 📖 *Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. […]*

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html

AVAILABILITY 🎯 (VERFÜGBARKEIT)

NIST

> 📖 *Ensuring timely and reliable access to and use of information.*

https://csrc.nist.gov/glossary/term/availability

BSI

> 📖 *Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.*

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html

CIAA - AUTHENTICITY 🎯 (AUTHENTIZITÄT)

NIST

> 📖 *The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.*

https://csrc.nist.gov/glossary/term/authenticity

BSI

> 📖 *[…] Authentizität bezeichnet die Eigenschaft, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. […] Identität von Personen […] IT-Komponenten oder Anwendungen.*

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html

CIAA++

ES GIBT EINE VIELZAHL AN WEITEREN SCHUTZZIELEN:

- Privacy (Privatheit)
- Trustworthiness (Vertrauenswürdigkeit)
- Non-repudiation (Nachweisbarkeit/ Nicht-Abstreitbarkeit)
- Resilience (Widerstandsfähigkeit)…

CIAA TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

CIAA TECHNISCHE MASSNAHMEN

Schutzziel	**Technische Maßnahmen**	**Beispiel**
Vertraulichkeit	Verschlüsselung	AES, RSA, ChaCha
Integrität	Kryptographische Prüfsummen (Hashes)	SHA-256, SHA-3
Authentizität (Identitäten)	Authentifizierung anhand von Wissen, Besitz oder Biometrie	Schlüssel, Passwort, PIN, TAN, Digitale Signatur, Iris, Fingerabdruck
Authentizität (Daten)	Message Authentication Codes (MAC)	CMAC, HMAC (basiert auch auf Wissen/Besitz)
Verfügbarkeit	Schutz auf Netzwerkebene, Systemebene	Routing, Firewalls

CIAA - ORGANISATORISCHE MASSNAHMEN

Schutzziel	Organisatorische Maßnahmen	Beispiele
Vertraulichkeit	Zugriffskontrolle und Richtlinien zum Zugang zu Informationen	MAC, RBAC, PBAC (AC= Access Control)
Integrität	Verwaltung und Veröffentlichung von Prüfsummen von Informationen	Hashwerte von Dokumenten, Programmen, … bereitstellen
Authentizität	Management von Identitäten, 2-Faktor Authentisierung	Digitale Signaturen für Dienste verwenden, Tokens oder Software für 2FA
Verfügbarkeit	Redundante Infrastruktur betreiben, Fall-Back Strategien für IP	Monitoring der Infrastruktur, Load/Balancing, Backups

SCHUTZZIELE CIAA+ ✍

Fortlaufende Bearbeitung über das ganze Semester:

- Ergänzen/Korrigieren Sie die Schutzziele (ihr eigenes oder das einer anderen Gruppe)
- Tauschen Sie sich dazu miteinander aus und diskutieren Sie miteinander.

- ⏱ Bearbeitung: Während des Semesters
- Machen Sie die Änderungen direkt in GIT!
  - Repo: https://git.thm.de/it_sec_crypto_ss_20/security_goals
  - Gruppe: https://git.thm.de/it_sec_crypto_ss_20