Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Einführung IT Security

Vorstellung

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Prof. Dr. Christian Henrich

2007	Master of Science (Neurosciences)
2007	Diplom-Informatiker
2012	Dr. rer. nat. "Improving and Analysing Bingo Voting"
2007-2011	Doktorand am KIT Institut für Kryptographie und Sicherheit (IKS)
2011-2013	Abteilungsleiter am FZI Abteilung Softwaresicherheit und Kryptographie
2013-2021	Bundeskriminalamt Stv. IT-Sicherheitsbeauftragter
seit 2021	Hochschule Albstadt-Sigmaringen Professor für IT-Sicherheit

Kontakt

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

per E-Mail

- henrich@hs-albsig.de
- *bevorzugt*
- Antwort innerhalb von drei Tagen

persönlich

- während der Sprechstunde: Mittwoch 13:30 Uhr – 14:30 Uhr
- nach Vereinbarung
- Geb. ~~2~~10 Raum ~~1~~14

205 304

MS Teams

- ohne Gewähr (zusätzlich E-Mail)

Ziele

Meine Ziele:

- Kompetenz vermitteln
- Klausurergebnis entspricht erworbener Kompetenz

Maßnahmen:

- vorbereitete Vorlesungen
- Aufgabenblätter
- Folienskript
- Vorlesungsaufzeichnungen vergangener Semester
- Antworten & Hilfestellung bei Fragen
- Literaturhinweise
- Unterstützung
- Reaktion auf Feedback

Lernerfolg

Was Sie beitragen können:

- aktive Mitarbeit
- Fragen
- eigenständige Vor- und Nachbereitung
- Bearbeitung der Aufgabenblätter

Was Sie beitragen können:

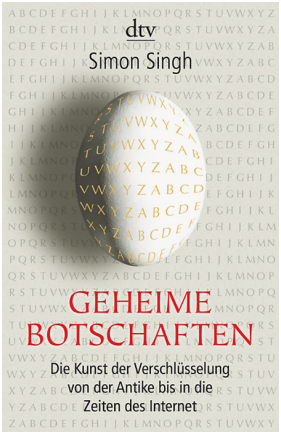
- aktive Mitarbeit
- Fragen
- eigenständige Vor- und Nachbereitung
- Bearbeitung der Aufgabenblätter

Persönlicher Tipp: Machen Sie sich Notizen!

Diskutieren Sie mit Ihren Kommilitoninnen und Kommilitonen!

Simon Singh: *Geheime Botschaften*

- Geschichte der Verschlüsselung
- guter Überblick
- verständlich geschrieben



Modul

Organisatorisches

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Vorlesung & Übung

- Termine
  - Dienstag 11:30 – 13:00
  - Mittwoch 9:45 – 11:15
- Vorlesung
- Wiederholung
- Besprechung des Aufgabenblatts

Prüfungsleistung

- Klausur 90 Minuten

Lernziele

Kompetenz Wissen Tiefes Verständnis der grundlegenden Begriffe und Konzepte der IT Security sowie deren Zusammenspiel mit anderen Informatikteilgebieten

Breites Wissen der für den sicheren Betrieb von IT Systemen notwendigen Grundlagen, Infrastruktur und Anwendungen

Kompetenz Fertigkeiten Fähigkeit Sicherheitsrisiken des IT Betriebs und die Sicherheit von Verschlüsselungsverfahren einzuschätzen und zu bewerten
Fähigkeit Angriffe auf die IT Sicherheit in der Praxis zu erkennen und Lösungen zu deren Abwehr zu erarbeiten

Fähigkeit einfache IT Systeme sicher zu konfigurieren und zu betreiben und dabei IT Sicherheitsmaßnahmen umzusetzen

Sozialkompetenz Fähigkeit im Bereich der Soft-, Hardware- und Organisatorischen IT Sicherheit mit Experten sowie mit Fachabteilungen präziser kommunizieren und zu argumentieren

Selbstständigkeit Fähigkeit sich selbständig neue, weiterführende bzw. noch nicht explizit behandelte Konzepte und Verfahren aus der wissenschaftlichen IT Security Literatur anzueignen

Inhalte

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Kapitel 1: Grundlagen & Begriffe

- Sicherheit & Schutzziele
- Kryptologie, Kryptografie, Steganografie
- Geschichte der Kryptografie
- Kerckhoffs'sches Prinzip
- Entropie
- Algorithmus & Protokoll

Image by 8385 from Pixabay

Kapitel 2: Verschlüsselungsverfahren

- symmetrische Verschlüsselung
- Stromchiffren, One Time Pad
- Blockchiffren: Betriebsmodi
- asymmetrische Verschlüsselung
- Schlüsselaustausch
- Snake Oil

Image by 8385 from Pixabay

Kapitel 3: kryptografische Bausteine

- Hashfunktionen
- Digitale Signaturen
- PKI
- MAC, HMAC

Image by 8385 from Pixabay

Kapitel 4: Authentifizierung & Zugriffskontrolle

- Identifizierung, Authentifizierung
- Passwörter
- Zugriffskontrollparadigmen

Image by 8385 from Pixabay

Kapitel 5: Protokolle

- SSH
- TLS

Image by 8385 from Pixabay

Kapitel 6: Weiterführende Konzepte

- Schwachstellen
- Malware
- Verfügbarkeit, Backup
- ISMS
- Risikomanagement

Image by 8385 from Pixabay

Feedback

Feedback – Positives

- Aktive Veranstaltung. Es konnten direkt Fragen gestellt werden und es wurde nachgefragt, ob alles verstanden wurde.
- Dass alles auch 5 mal erklärt wird wenn man etwas nicht verstanden hat.
- Die Art der Vorlesung, sprich die Erklärung bzw. wie die Themen eingeleitet wurden.
- Die detailreiche Belehrung einzelner Themenbereiche und klare Strukturierung der Themen
- Die Gestaltung der Vorlesung
- Die Vorlesung ist klar strukturiert und man kann dieser sehr gut folgen.

Feedback – Verbesserungsvorschläge

- Des öfteren Verwendung von Fachbegriffen kann durchaus verwirrend sein, vor allem wenn man keinen eloquenten Wortschaft hat
- Die Folien sollten bisschen früher zur Verfügung stehen. Ansonsten war es sehr gut.
- Es wäre schon wenn in allen Fächern die Schreibweise von Formeln bzw. die Bedeutung einzelner Zeichen gleich wären
- Im Skript Übungen (siehe DigLog)

$\mathbb{N} = \{1, 2, \ldots\}$

$\mathbb{N} = \{0, 1, 2, \ldots\}$

Feedback – Positives (ALT)

- Die Art und Wiese der Lehrveranstaltung ist schlüssig und lebendig gestaltet. Obwohl teilweise sehr abstrakte Themen besprochen werden, gibt es gutes anschauliches Bildmaterial.
- Was mir besonders gut an der Lehrveranstaltung gefallen hat ist die Einführung in das Modul, man merkt wie der Stoff von Vorlesung zu Vorlesung komplexer wird
  - Inhalte
  - Tempo
  - Dozent
- Echt netter Professor :). Sehr viel Stoff, versucht immer Fragen hervorzulocken und diese zu beantworten.
- Komplexe Sachverhalte wurden anschaulich erklärt
- Beispiele aus der Praxis wurden oft eingebracht
- Beispiele/Erklärungen aus der Praxis
- Dass es Übungsblätter, eine Klausur und VL-Folien gibt
- Die Zusammenfassung des Stoffs am Ende der VL

Feedback – Negatives (ALT)

- Leider gibt es für das insgesamt umfangreiche Thema zu wenig Übungen.
- Meines Erachtens sind zuviele Information in dem Skript enthalten,was dazu führt das man manchmal leicht den Überblick verliert.
- Konstruktives Feedback ist schwierig, keine Ahnung, eventuell ...
  Tut mir leid, ich sitze seit drei Minuten an den Punkten, ich hoffe, andere haben konstruktives Feedback.
  Edit: Eventuell das nötige Auswendiglernen von Inhalten, aber naja, das ist kein Kritikpunkt, deshalb studiere ich ja, ist eben das Modul. Ich hatte es mir, wenn ich ehrlich bin, schlimmer vorgestellt.

Feedback – Negatives (ALT)

- Seeehr viel Stoff, der meiner Meinung nach zu unübersichtlich und chaotisch gezeigt/erklärt wird. Man kann auch mit den Folien nicht wirklich gut arbeiten, ohne dass man sich die Aufzeichnungen nochmal 3 Mal anschauen muss. Auch gut wäre es, falls möglich, wenn der Prof Animationen anstatt 5 Folien mit 99% dem gleichen Inhalt nutzen könnte :). Man muss zum Lernen Sachen zusammenfassen, dafür finde ich fehlt noch so ein Leitfaden oder sowas. Vielleicht kann man zwischendurch so Fragenfolien stellen. Wenn man die beantworten kann, ist man gut auf die Prüfung vorbereitet oder sowas. Oder mehr Inhalt auf den Folien, da man halt hauptsächlich mit den arbeiten möchte :).
- Das Skript wurde manchmal zu spät/ nach der Vorlesung hoch geladen

Feedback – Verbesserungsvorschläge (ALT)

- Mehr Übungen und Beispielklausuren!
- Die Stoffmenge etwas eingrenzen,bestimmte Lerninhalte erst in eimen höheren Fachsemester einführen.Ansonsten bin ich zufrieden
- Siehe Antwort 2, tut mir leid.
- Mehr fällt mir ehrlich gesagt nicht noch mehr ein. Die Aufzeichnungen sind auf jeden Fall sehr wichtig, bitte nehmen Sie weiterhin die Vorlesungen auf. IT Security ist ein wichtiges Modul und hat es verdient, von den Studenten nicht vermieden zu werden, nur weil es schwer ist, mitzukommen oder mit den Folien zu arbeiten. Klar, man merkt, dass der Prof hin und wieder ein bisschen verwirrt ist mit seinen eigenen Antworten und Folien, aber das liegt glaube teils an seiner Persönlichkeit :). Bitte machen Sie weiter!
- Skript zeitig hochladen
- Auf den Folien weniger Stichpunkte, lieber Sätze (ist beim Lernen manchmal etwas schwierig zu verstehen, was gemeint war).

Grundlagen & Begriffe

Die ~~Zukunft~~ Gegenwart ist digital!

Die Zukunft ist digital!

analog / physisch

- gewohnt
- langsam
- physische Objekte
- Kopieren verlustbehaftet

digital

- „alles ist besser“
- neu & ungewohnt
- Information
- Kopieren verlustfrei

Was ist Sicherheit?

Was ist Sicherheit?

Nennen Sie Begriffe mit „Schutz“ oder „Sicherheit“!

aktive Angreifer

Firewall
Anonymität
Verschlüsselung
EMZ/DMZ
Bunker
Einbruchschutz
Grenzüberwachung
Virenschutz
Polizeischutz

Sicherheit

Überwachen
Verbessern
Datenschutz
Sicherheitsmaßnahmen
Backup
Identitätsschutz
Ausfallsicherheit
Integrität

Unfälle

Bevölkerungsschutz
Brandschutz
Schutzausrüstung
Schutzleiter
Sicherheitsunterweisung
Notausgang

Sicherheit

Safety

Security

Safety
Betriebssicherheit

Security

Safety
Betriebssicherheit

Schutz gegen Unfälle und Naturgewalten

Security

Safety
Betriebssicherheit

Security
„Schutz“

Schutz gegen Unfälle und Naturgewalten

Image by 8385 from Pixabay

Safety
Betriebssicherheit

Schutz gegen Unfälle und Naturgewalten

Security
„Schutz“

Schutz gegen zielgerichtete Angriffe

Image by 8385 from Pixabay

Warum ist Sicherheit so kompliziert?

Warum ist Sicherheit so kompliziert?

- Sicherheit ist komplex
- Sicherheit ist fragil
- Sicherheit ist kostspielig