Lehrveranstaltungshandbuch Identifikation

- Lehrveranstaltung
  - Befriedigt Modul (MID)
  - Organisation
  - Kompetenznachweis
- Lehrveranstaltungselemente
  - Vorlesung

Verantwortlich: Prof. Dr. Uwe Dettmar

Lehrveranstaltung

Befriedigt Modul (MID)

- aktuelle
  - Ma CSN2012 ID

Organisation

Version	
erstellt	2016-10-03
VID	1
gültig ab	WS 2012/13
gültig bis	

Bezeichnung	
Lang	Identifikation
LVID	BRS_ID
LVPID (Prüfungsnummer)	

Semesterplan (SWS)	
Vorlesung	2
Übung (ganzer Kurs)	1
Übung (geteilter Kurs)	
Praktikum	1
Projekt	
Seminar	
Tutorium (freiwillig)	

Präsenzzeiten	
Vorlesung	30
Übung (ganzer Kurs)	15
Übung (geteilter Kurs)	
Praktikum	15
Projekt	
Seminar	
Tutorium (freiwillig)	

max. Teilnehmerzahl	
Übung (ganzer Kurs)	
Übung (geteilter Kurs)	
Praktikum	
Projekt	
Seminar	

Gesamtaufwand: 180

Unterrichtssprache

- Deutsch

Niveau

- Master

Notwendige Voraussetzungen

Literatur

- keine

Dozenten

- Prof. Dipl.-Ing. Markus Ullmann

Wissenschaftliche Mitarbeiter

- tba

Zeugnistext

Identifikation

Kompetenznachweis

Form	
sK	mündlich

Aufwand [h]	
sK	Klausur

Intervall: 2/Jahr

Lehrveranstaltungselemente

Vorlesung

Lernziele

Lerninhalte (Kenntnisse)

- Diese Lehrveranstaltung behandelt die technologischen Grundlagen zur Identifikation von Individuen und Objekten. Ausgehend von den notwendigen informatischen und mathematischen Grundlagen werden sowohl intrinsische - als auch kryptographische Identifikationsverfahren behandelt. Intrinsische Verfahren basieren auf biologischen/physikalischen Phänomenen und ermöglichen somit eine Identifikation einer Person/eines Objektes auf ihren inhärenten Eigenschaften (z.B. Fingerabdruck eines Menschen bzw. Einschaltverhalten einer SRAM-Kaskade für eine mikroelektronische Schaltung). Kryptographische Identifikationsverfahren hingegen sind ausschließlich mathematischer Natur. Diese Lehrveranstaltung behandelt Identifikationsverfahren und ihre Implementierung.
- Einführung Identifikationsverfahren (implizite Identifikation [Fingerprinting: RF-Interfaces, Browser; IP-Adressen, ...] versus explizite Identifikation)
- Theoretische Grundlagen
- Intrinsische Identifikationsverfahren
- Kryptographische Identifikationsverfahren

Fertigkeiten

- Die Studierenden sind befähigt, in der beruflichen Praxis Identifikationsverfahren für unterschiedliche Technologiebereiche zu konzipieren und ihre Sicherheitseigenschaften zu analysieren
- Die Studierenden verstehen die Grundlagen von Identifikationsverfahren im Spannungsfeld zwischen einer eindeutigen Identifikation einerseits und einer Bewahrung der Privatsphäre andererseits sowohl in der Theorie als auch in der Praxis
- Die Studierenden besitzen umfassende Kenntnisse über Identifikationsverfahren.

Begleitmaterial

- Umdrucke und Skript

Besondere Voraussetzungen

- Grundlagen der Mathematik, Informatik, Informationssicherheit
- Kenntnisse zu Sicherheitstoken (Chipkarten, RFID-Systeme, TPMs)
- Kenntnisse der angewandten Kryptographie und kryptographischer (Authentisierungs-)Protokolle

Besondere Literatur

- Ahmad-Reza Sadeghi et al, Towards Hardware-Intrinsic Security, Springer Verlag 2010

- Sanjit Chatterjee et al, Identity-Based Encryption, Springer Verlag 2011
- BSI/TUD, Group Signatures: Authentication with Privacy, online: http://www.bsi.bund.de

Besonderer Kompetenznachweis

Form	
bÜA	begeleitend Übungsaufgaben

Beitrag zum LV-Ergebnis

Intervall:

Das Urheberrecht © liegt bei den mitwirkenden Autoren. Alle Inhalte dieser Kollaborations-Plattform sind Eigentum der Autoren.
Ideen, Anfragen oder Probleme bezüglich Foswiki? Feedback senden