Hauptseminar
– Informationssicherheit und Kryptographie –

(WS 2017/18)

Institut für Informationssicherheit
Prof. Dr. Ralf Küsters

Inhalt

In diesem Hauptseminar werden aktuelle Forschungsthemen aus verschiedenen Bereichen der **IT-Sicherheit, einschließlich Systemsicherheit, Websicherheit, Netzwerksicherheit, Privacy und Kryptographie**, behandelt. Die Themen richten sich nach jüngsten Veröffentlichungen auf führenden wissenschaftlichen Konferenzen. Üblicherweise werden sowohl Themen mit praktischem als auch mit mathematisch/theoretischem Schwerpunkt angeboten.

Die Palette an Themen ist vielfältig und umfasst **Angriffe, sichere Entwürfe und Implementierungen sowie Sicherheitsanalysen**. Einige mögliche Themen sind zum Beispiel:

- Blockchain (Bitcoin, Ethereum, ...)
- Payment-Lösungen (EMV, Cashier-as-a-Service, ...)
- Internet of Things
- Neuronale Netze/Deep Learning
- Mobile Plattformen (Android, ...)
- Post-Quantum-Kryptographie
- Trusted Computing (SGX, ...)
- Side-Channel-Angriffe (timing, power consumption,...)
- elektronische Wahlen
- Single-Sign-On
- Public-Key-Infrastrukturen
- Vehicular Networks
- elektronische Schlösser und drahtlose Schlüssel
- kryptographische Protokolle (TLS, SSH, WLAN, GSM, Signal [Whatsapp], ...)
- Multi-Party-Computation
- Fully Homomorphic Encryption
- Differential Privacy
- anonyme Kommunikation (Tor,...)
- DDoS

Wir sind ebenso **offen für Themen, die von Studierenden vorgeschlagen werden** (siehe etwa einschlägige Konferenzen: IEEE Symposium on Security and Privacy, ACM Conference on Computer and Communications Security, Usenix Security Symposium, Network and Distributed System Security Symposium, ESORICS, IEEE Computer Security Foundations Symposium, CRYPTO, EUROCRYPT, ASIACRYPT). Falls Sie eigene Themenvorschläge machen möchten, melden Sie sich bitte VOR der Vorbesprechung (siehe unten) beim Ansprechpartner zum Hauptseminar.

Hinweise zum Ablauf

Dieses Hauptseminar ist als Blockveranstaltung ausgelegt. Die konkreten Seminarthemen werden in einer Vorbesprechung zu Beginn des Semesters (voraussichtlich erste Vorlesungswoche) vorgestellt und nach Präferenz der Seminarteilnehmer/-innen verteilt. Sie fertigen während des Semesters sowohl eine schriftliche Ausarbeitung als auch einen Vortrag an. **Alle Vorträge finden gegen Ende des Vorlesungszeit in einer Blockveranstaltung statt**; während des Semesters gibt es dem entsprechend KEINE wöchentlichen Treffen. Die Ausarbeitungen sind bereits VOR den Vorträgen abzugeben.

Ansprechpartner

Daniel Rausch (daniel.rausch@informatik.uni-stuttgart.de)

Vorbesprechung

Voraussichtlich in der ersten Vorlesungswoche, der genaue Termin wird den Seminarteilnehmern zeitnah bekanntgegeben.

Vorkenntnisse

Sie sollten mindestens eine der folgenden Mastervorlesungen am Institut für Informationssicherheit bereits gehört haben:

- System and Web Security
- Introduction to Modern Cryptography
- Security and Privacy

Sprache

Deutsch