

Modulbeschreibung

E-Voting

Allgemeine Informationen

Bezeichnung Themenblock, Verantwortlicher

E-Voting

Modulkategorie

Fachliche Vertiefung

Anzahl der Credits

3

Ziele, Inhalt und Methoden

Lernziele, zu erwerbende Kompetenzen

Die Teilnehmer lernen praktisches wissenschaftliches Arbeiten anhand aktueller Forschungsthemen auf dem Gebiet der kryptografischen E-Voting Systeme. Die Teilnehmer lernen, ausgehend von einem ausgewählten, konkreten Thema, die Fachliteratur zu durchsuchen, die teils mathematisch komplexe Materie (unter Anleitung) zu verstehen und die Vor- und Nachteile der Verfahren bei der Anwendung in der Praxis zu erkennen.

Modulinhalt

- Desirable properties of voting systems
 - proof of eligibility
 - Secrecy, privacy, and anonymity
 - Receipt-freeness (vote-selling, coercion)
 - Universal verifiability
 - Robustness against errors, fraud, and attacks.
- Overview of traditional chain-of-custody e-voting systems
 - Principles, advantages & disadvantages
 - Direct recording electronic (DRE) voting machines
 - Current Swiss e-voting systems, etc.
- Overview of modern end-to-end auditable e-voting systems
 - Principles, advantages & disadvantages
 - Proposed systems: Prêt à Voter, Punchscan, Scratch & Vote, Scantegrity, etc.
- Cryptographic building blocks of end-to-end auditable e-voting systems
 - ElGamal and Paillier public key encryption systems
 - Secret-sharing and multi-authority threshold-decryption schemes
 - Homomorphic addition
 - Anonymizing mixnets
 - Zero knowledge proofs

Lehr- und Lernmethoden

Kick-Off Meeting aller Seminarteilnehmer zur Orientierung und Themenvergabe. Selbständiges Erarbeiten des gewählten Themas auf der Basis von wissenschaftlichen Publikationen und teils mittels zur Verfügung gestellter Simulatoren. Mehrere Meetings mit den Betreuern. Erstellen des Fachartikels (betreut und reviewed). Erstellen der mündlichen Präsentation (betreut und reviewed). Mündliche Präsentation der Ergebnisse und Eingehen auf Fragen. Mitarbeit und Fragestellungen in anderen Präsentationen.

Voraussetzungen

Gute Englisch-Kenntnisse (zum Verstehen der Originalliteratur). Besuch des zentralen MSE Moduls „Kryptographie und Codierungstheorie“ oder äquivalente Vorkenntnisse.

Bibliographie

Wikipedia, “End-to_End Auditable Voting Systems”

http://en.wikipedia.org/wiki/End-to-end_auditable_voting_systems

Ben Adida, Ronald Rivest; “Advances in Cryptographic Voting Systems” (2006)

<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.67.8154>

Detaillierte Literatur- und Linkzusammenstellung unter

<http://security.hsr.ch/msevot/>

Leistungsbewertung

Prüfungsart

Mündliche Prüfung

Prüfungsdauer

30 min. Präsentation

Bewertungskriterien

Art und Umfang der Planung & Durchführung.

Inhalt und Form des Fachartikels.

Präsentationsunterlagen und Eingehen auf Fragen.

Aktive Mitarbeit und Fragestellungen in anderen Vorträgen.