Karlsruher Institut für Technologie

SECUSO SECURITY · USABILITY · SOCIETY

aifb KASTEL KD²lab Decision&Design

E-Voting Seminar (Master)

Prof. Dr. Bernhard Beckert, Prof. Dr. Jörn Müller-Quade, Prof. Dr. Melanie Volkamer, Michael Kirsten, Felix Dörre, Tobias Hilt

Betreuer

- Prof. Dr. Bernhard Beckert bernhard.beckert@kit.edu
- Prof. Dr. Jörn Müller-Quade joern.mueller-quade@kit.edu
- Prof. Dr. Melanie Volkamer melanie.volkamer@kit.edu
- Dr. Michael Kirsten michael.kirsten@kit.edu
- Felix Dörre felix.doerre@kit.edu
- Tobias Hilt tobias.hilt@kit.edu

MOTIVATION

Chancen und Herausforderungen

- Wahlen im Wahllokal in Deutschland noch „der“ Wahlkanal bei parlamentarischen Wahlen
  - Nachteile, z. B. Wahlrechtsgrundsatz der allgemeinen Wahl nicht optimal umgesetzt, viele Wahlhelfer, langsame Auszählung, anfällig für Fehler bei der Auszählung
- Briefwahlen
  - Adressiert das Problem mit dem Wahlrechtsgrundsatz der allgemeinen Wahl, während der COVID-19 Pandemie sogar aus gesundheitlichen Gründen empfehlenswert
  - Neue Nachteile: Stimmenkauf und –zwang wird einfacher, nicht mehr ganz so zentral, Stimmen müssen rechtzeitig abgegeben werden
- Elektronische Wahlen im Wahllokal
  - Adressiert das Problem mit der langsamen Auszählung und der Anfälligkeit für Fehler bei der Auszählung
  - Neue Nachteile: Komplexe kryptographische Protokolle, um Verifizierbarkeit gewährleisten zu können; nicht mehr einfach zu verstehen, auf welchen Annahmen aufgebaut wird.
- Internetwahlen
  - Adressiert das Problem, dass Stimmen per Brief rechtzeitig abgegeben werden müssen sowie das Problem mit der langsamen Auszählung und der Anfälligkeit für Fehler bei der Auszählung
  - Neue Nachteile: Analog zur elektronischen Wahl im Wahllokal plus zentrales System

Annahmen

- Alle Wahlsysteme beruhen auf Annahmen an die Angreifermächtigkeit und an die Einsatzumgebung
- Um beurteilen zu können, ob ein E-Voting System ein adäquates Sicherheitsniveau bietet, ist es wichtig, die expliziten und impliziten Annahmen des Systems für die einzelnen Sicherheitsanforderung (bzw. Wahlrechtsgrundsätze) auf den unterschiedlichen Ebenen zu kennen
  - Krypto-Protokoll
  - Umsetzung in Software / Hardware
  - Benutzerschnittstellen
  - Anforderungen an die Wählenden
  - Auszählungsalgorithmus

- Daher Seminar in Kooperationen von mehreren Lehrstühlen mit unterschiedlichen Schwerpunkten

ORGANISATION

Seminar Prozess

- Das Seminar wird dieses Semester als Präsenzveranstaltung stattfinden.
- Individuelle Treffen mit den Betreuern um Thema / Methodik zu konkretisieren
- Kick-Off Veranstaltung
  - **30.04.2025, 12:45 – 13:45 Uhr** (Geb. 05.20, Raum 3A – 11.1)
  - Themenzuteilung während des Kick-Offs
- Präsentation der Seminararbeiten
  - Vorträge Teil I: **tbd (innerhalb der letzten 2 Semesterwochen)**
  - Vorträge Teil II: **tbd (innerhalb der letzten 2 Semesterwochen)**
- Abgabe der Ausarbeitung bis zum **30.09.2025**

Seminararbeit

- Sprache: Deutsch oder Englisch
- Format: Springer LNCS https://www.springer.com/gp/computer-science/lncs
  - Vorgaben für Überschriften, Tabellen, Abbildungen sowie für Literaturverzeichnis
  - Overleaf falls Latex (nicht zwingend) → Format muss beachtet werden
- Umfang 10 Seiten (ohne Inhalts-, Literaturverzeichnis, Anhänge), insgesamt nicht länger als 16 Seiten

Präsentation und Diskussion

- Sprache: Deutsch oder Englisch
- Format: Präsentation KASTEL Format-Vorlage (PPT Vorlage und TeX Vorlage)
- Anwesenheitspflicht während der gesamten Vortragsreihe
- Ca. 45 Minuten pro Person
  - 25-30 Min Präsentation
  - Ca. 15 Min Diskussion

Prüfungsleistung - Benotung

- 40% Ausarbeitung
- 40% Vortrag zur Präsentation und eigener Diskussionsbeitrag
- 10% Teilnahme an anderen Diskussionen
- 10% Arbeitsverhalten während des Seminars

- 5.0
  - Abmeldung nach dem **07.05.2025: Mail zur Abmeldung an: tobias.hilt@kit.edu und Themen-Betreuer**
  - Keine vollständige Version bis zur Deadline eingereicht
  - Unentschuldigtes Fehlen bei den Vorträgen
  - Inhaltliche Gründe
  - Ausarbeitung **oder** Vortrag 5.0 → gesamte Arbeit 5.0

Prüfungsleistung - Bewertungskriterien

- Für das finale Paper
  - Klarheit von Motivation und Ziel
  - Nachvollziehbarkeit und Angemessenheit der Methode
  - Struktur / Roter Faden
  - Klarheit der Ergebnisse
  - Nachvollziehbarkeit der Diskussion der Ergebnisse

- Für die Präsentation/Diskussion
  - S.o.
  - Zusätzlich: Präsentationsstil inkl. Einbeziehung der Präsentation

Weitere wichtige Modalitäten

- Verantwortung für Terminfindung mit Betreuer liegt bei Studierenden
- Erste Terminabsprache spätestens 1 Woche nach Themenvergabe
- Themen/Fragen für das Treffen mindestens zwei Tage vor dem Treffen schicken
- Protokoll des Treffens (kann stichwortartig sein) maximal zwei Tage nach dem Treffen schicken
- Mails nur über Uni E-Mail Account (gewechselt auf Name.Nachname)

- Themen für Absprachen/Feedback
  - Zu Beginn bis das Thema / Methode stehen – enge Absprachen
  - Struktur des Papers
  - Struktur der Präsentation
  - Feedback zur „fertigen“ Präsentation

THEMEN

5 Themen

1. ElectionGuard: a Cryptographic Toolkit to Enable Verifiable Elections (Felix Dörre)
2. Literature Review on Awareness Measures with Respect to Individual Verifiability (Tobias Hilt)
3. Literature Review on Manipulation Studies in E-Voting (Tobias Hilt)
4. Attacks and Formal Verification for Postal Voting using ProVerif (Michael Kirsten)
5. Formal Verification of Privacy using EasyCrypt for the Voting Systems Selene and Belenios (Michael Kirsten)

Themen (Felix Dörre)

- Thema 1: ElectionGuard: a Cryptographic Toolkit to Enable Verifiable Elections
  - Welche Sicherheitseigenschaften kann ElectionGuard garantieren?
  - Unter welchen Annahmen gelten diese Sicherheitseigenschaften?

Themen (Tobias Hilt)

- Thema 2: Literature Review on Awareness Measures with Respect to Individual Verifiability
  - Welche Art von Awareness Measures sind grundsätzlich vorstellbar?
  - Was wurde bisher eingesetzt (Praxisbeispiele)?
  - Welche Informationen hat der Wähler erhalten (Detailgrad)?
  - Wurde es evaluiert?
- Thema 3: Literature Review on Manipulation Studies in E-Voting
  - Welche Arten der Manipulation wurden bisher untersucht? Wie wurde das untersucht?
  - Wie unterscheiden sich die untersuchten Manipulationen voneinander? Gibt es Gemeinsamkeiten?

Themen (Michael Kirsten)

- Thema 4: Attacks and Formal Verification for Postal Voting using ProVerif
  - Wie (un)sicher ist die Briefwahl wirklich?
  - Welche Vertrauensannahmen sind realistisch und welche Angriffe möglich?
  - Wie sieht ein sicheres Briefwahlprotokoll aus und wie lässt sich das für symbolische Modellierungen formal beweisen?
- Thema 5: Formal Verification of Privacy using EasyCrypt for the Voting Systems Selene and Belenios
  - Wie lässt sich Geheimhaltung sinnvoll sowohl für praktische als auch für rein akademische Wahlsysteme definieren?
  - Welche Vertrauensannahmen sind für die Garantie dieser Eigenschaft notwendig?
  - Wie lässt sich dies für eine rechenbetonte ("computational") Modellierung formal beweisen?