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
- 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 Krise sogar aus gesundheitlichen Gründen empfehlenswert
  - Neue Nachteile: Stimmenkauf und –zwang wird einfacher, nicht mehr ganz so zentral
- 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 (statt Briefwahlen)
  - 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
  - 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
  - **26.04.2024, 14:00 – 15:30 Uhr** (Geb. 05.20, Raum 3A – 11.1)
  - Bewerbung auf Thema und Themenvergabe nach dem Kick-Off
- Präsentation der Seminararbeiten
  - Vorträge Teil I: **tbd (letzte Vorlesungswoche)**
  - Vorträge Teil II: **tbd (letzte Vorlesungswoche)**
  - Genauerer Ablaufplan wird noch bekannt gegeben
- Abgabe der Ausarbeitung bis zum **30.09.2024**

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 **05.05.2024: 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. Methodische Ansätze in User Studies zum Thema E-Voting(Prof. Volkamer)

2. Neuerungen in ElectionGuard 2.0. (Felix Dörre)

3. Das estländische Wahlsystem (Felix Dörre)

4. Formale Verifikation von Verifiability und Eligibitlity mit ProVerif (Dr. Michael Kirsten)

5. Sichere Mehrparteienberechnung für geheime Ergebnisberechnung von ordnungsbasierten und echten Parlamentswahlen (Dr. Michael Kirsten)

Themen (Volkamer)

- Thema 1: Methodische Ansätze in User Studies
  - Literaturrecherche zur Identifikation von verschiedenen Ansätzen, die bei den unterschiedlichen User-Studies im Bereich E-Voting eingesetzt wurden
  - Welcher E-Voting approach wurde untersucht?
  - Was wurde konkret untersucht (z.B. Nutzbarkeit, Vertrauen, Verständnis, …)?
  - Welche Methodik wurde hierbei angewandt?

Themen (Dörre)

- Thema 2: Neuerungen in ElectionGuard 2.0.
  - Welche Dinge haben sich geändert?
  - Hat das Auswirkungen auf die Sicherheitseigenschaften?
  - Starting Literature: *Benaloh, Josh und Naehrig, Michael. "ElectionGuard Design Specification 2.0.0." GitHub von Microsoft Research. 2024. (https://github.com/microsoft/electionguard/releases/download/v2.0/EG_Spec_2_0.pdf)*

- Thema 3: Das estländische Wahlsystem
  - Wie funktioniert es und welche Sicherheitseigenschaften bietet es?
  - Starting Literature: *Springall, Drew, et al. "Security analysis of the Estonian internet voting system." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014. (https://dl.acm.org/doi/pdf/10.1145/2660267.2660315)*

Themen (Kirsten)

- Thema 4: Formale Verifikation von Verifiability und Eligibility mit ProVerif
  - Wie lassen sich Verifiability und Eligibility für Wahlen formalisieren?
  - Wie lassen sich dafür mit ProVerif formale Sicherheitsbeweise führen?
  - Literatur:
    - *Cheval, Vincent, et al. "Election Verifiability with ProVerif." 2023 IEEE 36th Computer Security Foundations Symposium (CSF). 2023. (https://doi.org/10.1109/CSF57540.2023.00032)*
    - *Cortier, Véronique, et al. "Election Eligibility with OpenID: Turning Authentication into Transferable Proof of Eligibility." Cryptology ePrint Archive, Paper 2024/261. 2024. (https://eprint.iacr.org/2024/261).*

- Thema 5: Sichere Mehrparteienberechnung für geheime Ergebnisberechnung von ordnungsbasierten und echten Parlamentswahlen
  - Wie lassen sich Wahlergebnisse so berechnen, dass man ihnen vertrauen kann, aber die Berechnungsschritte keine Rückschlüsse auf die konkrete Wahlentscheidung zulassen?
  - Was sind die Besonderheiten für komplexere Wahlverfahren?
  - Literatur:
    - *Tassa, Tamir und Dery, Lihi. "Towards Secure Virtual Elections: Multiparty Computation of Order Based Voting Rules." arXiv:2205.10580. 2024. (https://arxiv.org/abs/2205.10580)*
    - *Wabartha, Carmen, et al. "Fully Tally-Hiding Verifiable E-Voting for Real-World Elections with Seat-Allocations." 28th European Symposium on Research in Computer Security – ESORICS 2023. 2023. (https://doi.org/10.1007/978-3-031-50594-2_11)*