E-Voting Seminar (Master)

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

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
- Reyhan Düzgün reyhan.duezguen@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. Wir behalten uns vor, falls sich die Regelungen ändern, die Vorträge zur gleichen Zeit online durchzuführen.
- Individuelle Treffen mit den Betreuern um Thema / Methodik zu konkretisieren
- Kick-Off Veranstaltung
  - **20.04.2022, 15.45 – 17.15 Uhr** (Geb. 05.20, Raum 3A – 11.1)
  - Themenvergabe am Ende des Kick-Offs
- Präsentation der Seminararbeiten
  - Vorträge Teil I: **26. Juli 2022, 09.45 – 13.00 Uhr**
  - Vorträge Teil II: **29. Juli 2022, 14.00 – 17.15 Uhr**
  - Genauerer Ablaufplan wird noch bekannt gegeben
- Abgabe der Ausarbeitung bis zum **16.09.2022**

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 **04.05.2022: Mail zur Abmeldung an: reyhan.duezguen@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 des Präsentation
  - Feedback zur „fertigen“ Präsentation

THEMEN

6 Themen

1. Vertrauen in Online-Wahlen (Prof. Volkamer)

2. Verifizierbarkeit im Estnischen Online-Wahlsystem (Prof. Volkamer)

3. Tally-Hiding E-Voting (Felix Dörre)

4. The State of CH-Vote (Felix Dörre)

5. Verified Construction of Correct Election Verifiers Using the Theorem Prover Coq (Dr. Michael Kirsten)

6. Security Proofs of Election Verifiability Using the Automated Prover Tamarin (Dr. Michael Kirsten)

Themen (Volkamer)

- Thema 1: Vertrauen in Online-Wahlen
  - Literaturrecherche zur Identifikation von Faktoren, die einen Einfluss auf Vertrauen in ein Online-Wahlsystem haben.

- Thema 2: Verifizierbarkeit im Estnischen Online-Wahlsystem
  - Literaturrecherche, um die eingesetzten Mechanismen inkl. der getroffenen Trust-Assumptions zu beschreiben und zu diskutieren.

Themen (Dörre)

- Thema 3: Tally-Hiding E-Voting
  - Often the exact tally of an election is not needed, but only e.g. a winner or a ranking of candidates.
  - This topic discusses the advantages and disadvantages of tally-hiding systems e.g. at the example of Ordinos.
  - Starting Literature: "Ordinos: A Verifiable Tally-Hiding E-Voting System"

- Thema 4: The State of CH-Vote
  - Switzerland created an E-Voting system called "CH-Vote", that had quite a few starting difficulties.
  - This topic discusses CH-Vote and its initial problems and improvements.
  - Starting Literature: "CHVote: Sixteen Best Practices and Lessons Learned"

Themen (Kirsten)

- Thema 5: Verified Construction of Correct Election Verifiers Using the Theorem Prover Coq
  - In diesem Seminarthema sollen Ansätze untersucht werden, die Wahl-Verifizierungswerkzeuge (zur Sicherstellung der Integrität der Abgabe oder Verarbeitung einer Stimme) mithilfe des allgemeinen Theorembeweisers Coq formalisiert und verifiziert, sowie direkt aus der verifizierten Formalisierung lauffähige Software generiert haben.
  - Literatur:
    - Thomas Haines, Rajeev Goré, Jack Stodart (2021): “Machine-Checking the Universal Verifiability of ElectionGuard.” In: Secure IT Systems. NordSec 2020. Lecture Notes in Computer Science, Vol. 12556. Springer, doi: 10.1007/978-3-030-70852-8_4.
    - Thomas Haines, Rajeev Goré, and Mukesh Tiwari (2019): “Verified Verifiers for Verifying Elections.” In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, doi: 10.1145/3319535.3354247.

- Thema 6: Security Proofs of Election Verifiability Using the Automated Prover Tamarin
  - In diesem Seminarthema soll eine allgemeine symbolische Definition von Wahl-Verifizierbarkeit (zur Sicherstellung der Integrität der Abgabe oder Verarbeitung einer Stimme) sowie automatische Verifikationsansätzen von Instanzen dieser (allgemeinen) Definition auf die bekannten Wahlprotokolle Helios und Belenios mithilfe des Prozessalgebra-Beweisers Tamarin untersucht und die Ergebnisse jeweils miteinander verglichen werden.
  - Literatur:
    - Sevdenur Baloglu and Sergiu Bursuc and Sjouke Mauw and Jun Pang (2021): “Election Verifiability Revisited: Automated Security Proofs and Attacks on Helios and Belenios.” In: 2021 IEEE 34th Computer Security Foundations Symposium (CSF), doi: 10.1109/CSF51468.2021.00019.