E-Voting Seminar (Master)

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

INSTITUT FÜR ANGEWANDTE INFORMATIK UND FORMALE BESCHREIBUNGSVERFAHREN (AIFB)
FORSCHUNGSGRUPPE SECURITY · USABILITY · SOCIETY (SECUSO)

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
- Rebecca Schwerdt rebecca.schwerdt@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 dezentral
- 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 online durchgeführt. Wir behalten uns vor, falls sich die Regelungen ändern, die Vorträge als Präsenzveranstaltung zur gleichen Zeit Vor-Ort durchzuführen.
- Individuelle Treffen mit den Betreuern via Videokonferenz um Thema / Methodik zu konkretisieren
- Veranstaltungen finden über MS Teams statt. Bitte beachten Sie, vorher…
  - der Datenschutzerklärung unter folgendem Link zuzustimmen: https://my.scc.kit.edu/shib/azurefreigabe.php
  - die Anwendung auf dem Rechner zu installieren
- Kick-Off Veranstaltung inkl. Themenvergabe am **29.04.2020**, 12.30 – 14.00 Uhr
  - Link zur Kick-Off Veranstaltung: An Microsoft Teams-Besprechung teilnehmen
- Präsentation der Seminararbeiten
  - Vorträge Teil I: **10.07.2020**, 13.30 – 18.00 Uhr
  - Vorträge Teil II: **17.07.2020**, 13.30 – 18.00 Uhr
  - Genauerer Ablaufplan wird noch bekannt gegeben
- Abgabe der Ausarbeitung bis zum **15.09.2020**

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 und TeX Vorlagen werden noch zur Verfügung gestellt)
- 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 **01.05.2019: 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

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
- 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. Deep Dive into Oblivious Bingo Voting (Schwerdt/Prof. Müller-Quade)
- 2. Das Schweizer Online-Wahlsystem der Post: Explizite und implizite Annahmen an den Angreifer und die Einsatzumgebung (Prof. Volkamer)
- 3. User-Studies im Kontext von Verifizierbarkeit (Prof. Volkamer)
- 4. How to quantify and compare strategic manipulation for voting rules? (Kirsten/Prof. Beckert)
- 5. Manipulations of Election Results and Risk-Limiting Audits (Kirsten/Prof. Beckert)
- 6. Implizite und explizite Annahmen bei Prêt à voter (Dörre /Prof. Müller-Quade)

1. Thema: Deep Dive into Oblivious Bingo Voting (Schwerdt)

- Motivation: Most cryptographic voting system proposals come with a list of properties and a list of assumptions under which these properties hold. This is a good start to assess a proposal. For meaningful comparisons of different proposals and decisions regarding practical application, however, this is seldom sufficient. If, for example, there is no solution (yet) which does not rely on any kind of trusted entity to perform efficiently, it is sensible to compare how much power this trusted entity receives exactly. I.e. which properties still hold in case this entity is corrupted. Both complete and more fine-grained assumptions as well as information about ramifications of unsatisfied assumptions ("graceful degredation") improve the assessment of a voting system.
- Topic: In this seminar topic, we examine one cryptographic voting system to the fullest extent possible. As the example system Oblivious Bingo Voting (OBV) was chosen. Results are presented with the aim of comparability as well as guidance for people who consider practical application of the system.
- Goals: For this topic, the student. . .
  - familiarizes themselves with common properties of cryptographic voting systems.
  - familiarizes themselves with the OBV system in full detail.
  - extensively examines OBV and it's properties under various assumptions.
  - *examines a second system and compares the results.* (The *last goal* is a possible extension of the basic requirements, dependent on the student's prior knowledge as well as the progress with other goals.)
- Literature:
  - Dirk Achenbach et al. "Oblivious Voting - Hiding Votes from the Voting Machine in Bingo Voting". In: International Conference on Security and Cryptography, Lisbon, Portugal, 26–28 July 2016. SCITEPRESS, Setúbal, 2016, pp. 85–96.
  - Dirk Achenbach et al. "Towards Realising Oblivious Voting". In: E-Business and Telecommunications. Ed. by Mohammad S. Obaidat. Cham: Springer International Publishing, 2017, pp. 216–240.
  - Jens-Matthias Bohli, Jörn Müller-Quade, and Stefan Röhrich. "Bingo Voting: Secure and Coercion-Free Voting Using a Trusted Random Number Generator". In: E-Voting and Identity. Ed. by Ammar Alkassar and Melanie Volkamer. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 111–124.

2. Thema: Das Schweizer Online-Wahlsystem der Post: Explizite und implizite Annahmen an den Angreifer und die Einsatzumgebung (Prof. Volkamer)

- Beschreibung: Die Schweiz setzt u.a. ein Online-Wahlsystem ein, welches gemeinsam von der Post und der Firma Scytl betrieben wird. Es besteht aus einem kryptographischen Wahlprotokoll, welches die Firma Scytl entwickelt hat und für das Setting in der Schweiz in Kooperation mit der Post konfiguriert wurde. Ziel des Seminarthemas ist es, die Annahmen auf den unterschiedlichen Ebenen (Wahlprotokoll, Konfiguration, Software, Anwendung durch den Wähler) sowohl an die Angreifermächtigkeit als auch die Einsatzumgebung zu identifizieren und zu diskutieren.

3. Thema: User-Studies im Kontext von Verifizierbarkeit (Prof. Volkamer)

- Beschreibung: Zunehmend bieten Elektronische Wahlsysteme dem Wähler, die Möglichkeit zu überprüfen, dass die Stimme richtig verschlüsselt und / oder gespeichert wurde. Dabei ist es wichtig, dass die Wähler in der Lage sind, diese Prüfung durchzuführen, d. h. dass sie merken, wenn eine Manipulation stattgefunden hat. Um zu evaluieren, ob dies gegeben ist, werden Nutzerstudien durchgeführt. Ziel dieses Seminarthemas ist es, sich einen Überblick über die hierzu durchgeführten Arten von Nutzerstudien zu verschaffen und die Vor- und Nachteile der unterschiedlichen Arten gegenüber zu stellen.

4. Thema: How to quantify and compare strategic manipulation for voting rules? (Kirsten)

- In diesem Seminarthema betrachten wir strategische Manipulation, einen Angriff bei der Stimmabgabe auf das Wahlauszählverfahren selbst. Hierbei soll untersucht werden, wie man damit verschiedene Wahlauszählverfahren vergleichen und quantifizieren kann.
- Literatur:
  - How Bad Is Selfish Voting? by Simina Brânzei, Ioannis Caragiannis, Jamie Morgenstern, and Ariel D. Procaccia in Twenty-Seventh Conference on Artificial Intelligence (AAAI 2013)
  - Efficient, Private, and epsilon-Strategyproof Elicitation of Tournament Voting Rules by David T. Lee in Twenty-Fourth International Joint Conference on Artificial Intelligence (IJCAI 2015)
  - How Many Vote Operations Are Needed to Manipulate a Voting System? by Lirong Xia in arXiv 2012

5. Thema: Manipulations of Election Results and Risk-Limiting Audits (Kirsten)

- Beschreibung: In diesem Seminarthema sollen Auditverfahren von Wahlen untersucht werden. Hierbei soll der Fokus auf der Tauglichkeit für verschieden komplizierte Wahlauszählverfahren sowie deren Mächtigkeit hinsichtlich der Erkennung cleverer Manipulationsattacken des Wahlergebnisses liegen.
- Innerhalb des Themas besteht die Möglichkeit, für einen umfassenderen Vergleich weitere Auditverfahren heranzuziehen.
- Literatur:
  - Election Manipulation 100 by Michelle Blom, Peter J. Stuckey, and Vanessa J. Teague in International Conference on Financial Cryptography and Data Security 2019
  - BatchVote: Voting Rules Designed for Auditability by Ronald L. Rivest, Philip B. Stark, and Zara Perumal in International Conference on Financial Cryptography and Data Security 2017
  - Ballot-Polling Risk Limiting Audits for IRV Elections by Michelle Blom, Peter J. Stuckey, and Vanessa Teague in International Conference on Electronic Voting (EVOTE-ID 2018)

6. Thema: Implizite und explizite Annahmen bei Prêt à voter (Dörre)

- Beschreibung: Bei kryptographischen Wahlverfahren werden oft zusätzlich zu den kryptografischen Annahmen auch Annahmen über physische Komponenten des Wahlverfahrens, den Wähler oder andere beteiligte Instanzen gemacht. Diese Annahmen sollen am Beispiel von Prêt à voter identifiziert und diskutiert werden.
- Literatur:
  - RYAN, Peter YA, et al. Prêt à voter: a voter-verifiable voting system. IEEE transactions on information forensics and security, 2009, 4. Jg., Nr. 4, S. 662-673.