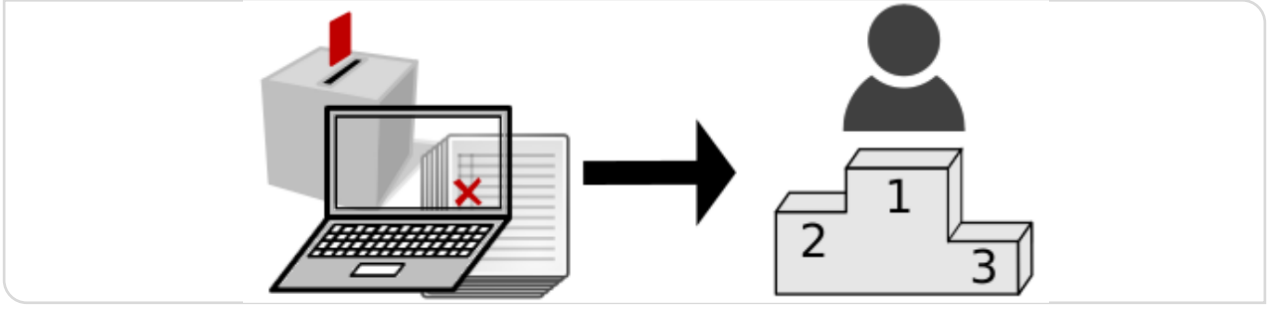
Karlsruher Institut für Technologie

KASTEL

Thema: Sichere Online-Wahlen mit ElectionGuard und Helios

Praxis der Softwareentwicklung im Wintersemester 2022/23

Prof. Bernhard Beckert, Felix Dörre, Michael Kirsten und Prof. Jörn Müller-Quade | 07. November 2022



Sichere Online-Wahlen

Ziel: Komfortabel über das Internet abstimmen

Herausforderungen

- Möglicherweise kompromittierte Endgeräte
- Evtl. durch Wahlautorität hinzugefügte oder veränderte Stimmen

Sichere Online-Wahlen

Ziel: Komfortabel über das Internet abstimmen

Herausforderungen

- Möglicherweise kompromittierte Endgeräte
- Evtl. durch Wahlautorität hinzugefügte oder veränderte Stimmen

Lösung

Ende-zu-Ende-Verifizierbarkeit

Sichere Online-Wahlen

- Wählende können prüfen, dass Stimmen korrekt erfasst wurden (*individ.*)
- Jede:r kann prüfen, dass das Ergebnis korrekt berechnet wurde (*univers.*)

Sichere Online-Wahlen

- Wählende können prüfen, dass Stimmen korrekt erfasst wurden (*individ.*)
- Jede:r kann prüfen, dass das Ergebnis korrekt berechnet wurde (*univers.*)
- Beispiel für ein verifizierbares Onlinewahlsystem: helios Trust the vote.
- Toolkit um Wahlaufzeichnungen zu verifizieren:  ElectionGuard

Sichere Online-Wahlen

- Wählende können prüfen, dass Stimmen korrekt erfasst wurden (*individ.*)
- Jede:r kann prüfen, dass das Ergebnis korrekt berechnet wurde (*univers.*)
- Beispiel für ein verifizierbares Onlinewahlsystem: helios Trust the vote.
- Toolkit um Wahlaufzeichnungen zu verifizieren: ElectionGuard





Aufgabe: Sichere Online-Wahlen mit ElectionGuard und Helios

Anforderungen

- Funktionalitäten für Wählende und Wahlleitung
- Verschlüsselte (Online-)Übermittlung der Stimmen
- Funktionalitäten zur individuellen und universellen Ende-zu-Ende-Verifizierung
- Drei graphische Benutzungsoberflächen (Konfiguration, Abstimmung, Verifizierung)

Technischer Rahmen

- Microsoft-ElectionGuard (in Python) als Bibliothek für Funktionalitäten
- Orientierung an Wahlablauf des Helios-Systems
- **Keine Blockchain!** (just in case)

Betreuer

Felix Dörre

felix.doerre@kit.edu – Raum 275

Michael Kirsten

kirsten@kit.edu – Raum 228

Webseite

https://formal.kastel.kit.edu/teaching/pse/202223/

- Termine
- Dokumente

Betreuer

Felix Dörre

felix.doerre@kit.edu – Raum 275

Michael Kirsten

kirsten@kit.edu – Raum 228

Webseite

https://formal.kastel.kit.edu/teaching/pse/202223/

- Termine
- Dokumente

Vorstellung: Wer sind Sie? Vorwissen? Motivation für Thema?

Wöchentliche Treffen

- Wann haben Sie Zeit für ein wöchentliches Treffen?
- Welche Klausuren schreiben Sie dieses Semester? Wann?

Ende-zu-Ende-Verifizierbarkeit (E2E-V)

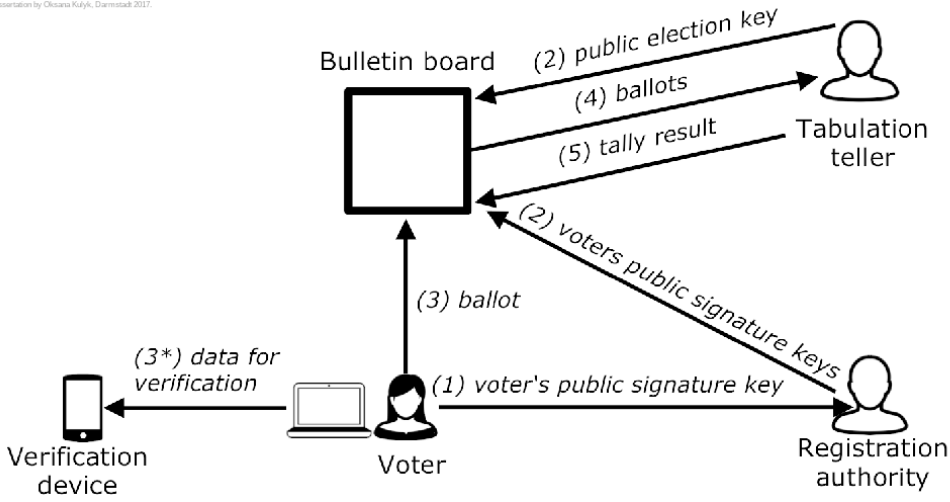
1. Stimmabgabe wie beabsichtigt: *Cast-as-Intended* (*indiv.*)
2. Stimmerfassung wie abgegeben: *Collected-as-Cast* (*indiv.*)
3. Korrekte Zählung wohlgeformter und erfasster Stimmen: *Tallied-as-Collected* (*univ.*)
4. Verifizierung der Wahlberechtigung: *Eligibility-Verifiability* (*univ.*)

Ende-zu-Ende-Verifizierbarkeit (E2E-V)

1. Stimmabgabe wie beabsichtigt: *Cast-as-Intended* (*indiv.*)
2. Stimmerfassung wie abgegeben: *Collected-as-Cast* (*indiv.*)
3. Korrekte Zählung wohlgeformter und erfasster Stimmen: *Tallied-as-Collected* (*univ.*)
4. Verifizierung der Wahlberechtigung: *Eligibility-Verifiability* (*univ.*)

E2E-V-Wahlsysteme sind idealerweise *software-unabhängig*!

Interaktionen im Helios-System



Crypto-Grundlagen

- Threshold encryption
- Homomorphic encryption
- Zero-knowledge proofs

Zeitplan

Phase	Dauer	Kalenderwoche	Jahr
Einlesen	ca. 1 Woche	45	2022
Pflichtenheft	3 Wochen	46–48	2022
Entwurf	4 Wochen	49–02	2022/23
Implementierung	4 Wochen	03–06	2023
Klausurpause	2 Wochen	07–08 ?	2023
Qualitätssicherung	3 Wochen	09–10 ?	2023
Interne Abnahme	–	12 ?	2023
Abschlusspräsentation	–	13 ?	2023

Zeitplan

Phase	Dauer	Kalenderwoche	Jahr
Einlesen	ca. 1 Woche	45	2022
Pflichtenheft	3 Wochen	46–48	2022
Entwurf	4 Wochen	49–02	2022/23
Implementierung	4 Wochen	03–06	2023
Klausurpause	2 Wochen	07–08 ?	2023
Qualitätssicherung	3 Wochen	09–10 ?	2023
Interne Abnahme	–	12 ?	2023
Abschlusspräsentation	–	13 ?	2023

Phase

Phasenverantwortliche:r

- koordiniert die Arbeit
- präsentiert die Ergebnisse im Kolloquium
- Zuteilung liegt bei Ihnen

Kolloquium

- Abschluss einer Phase
- Vortrag von/m Phasenverantwortlicher/n
- Fragenrunde

Abgaben und Bewertung

Abgaben (Artefakte)

- Abgaben mit den geforderten Artefakten stets per GIT (Link t.b.d.)
- Teil der Prüfungsleistung
- Abgabe 48 (genauer Zeitpunkt t.b.d.) Stunden vor Kolloquium
- Abgabe pünktlich, muss eindeutig(!) im GIT erkenntlich sein

Kolloquium

- Teil der Prüfungsleistung (Vortrag und Fragerunde)
- Wichtig: Anwesenheit ist Teil der Prüfungsleistung

Gewichtung

Pflichtenheft 10%, Entwurf 30%, Implementierung 30%, Qualitätssicherung 20%, Abschlusspräsentation 10%

Werkzeuge für Software

Werkzeug-gestützte SW-Entwicklung

Verwendung von

- GIT-Repository
- Issues Tracker
- Continuous Integration
- Build-Skripte (Maven, Ant, ...)

Den Betreuern ist Zugriff zu gewähren. Überprüfung von Commits.

1. Phase: Pflichtenheft

Pflichtenheft

Artefakt: Pflichtenheft im Umfang: ca. 40 Seiten

Inhalte:

- Systemmodell und -umgebung
- Zielbestimmungen (Muss-, Wunsch- und Abgrenzungskriterien)
- Vollständige funktionale Anforderungen; Qualitätsanforderungen
- GUI-Entwürfe
- Ausführliche Testfallszenarien
- Phasenverantwortliche

Wie geht es weiter

- Austausch der Kontaktinformationen
- Anlegen des Repository
- Festlegung der Phasenverantwortlichen
- Ausprobieren von ElectionGuard (`https://electionguard.vote/`) und Helios (`https://vote.heliosvoting.org/`)
- Einlesen in E-Voting und Ende-zu-Ende-Verifizierbarkeit

Bis zum nächsten Treffen!

Fragen und Antworten

Vielen Dank

für die Aufmerksamkeit!

Karlsruher Institut für Technologie

Vielen Dank

für die Aufmerksamkeit!

Gibt es Fragen?