Sicheres elektronisches Abstimmen auf einem unsicheren Gerät

Studiengang: BSc in Informatik | Vertiefung: IT Security
Betreuer: Prof. Dr. Rolf Haenni
Experte: Dr.Andreas Spichiger

Beim Einsatz persönlicher Geräte für elektronische Abstimmungen bieten bestehende kryptographische Protokolle nicht genügend Schutz von Brüchen des Stimmgeheiminisses. Dank eines völlig neuen Ansatzes können aber die Schwachstellen solcher Geräte beseitigt und somit die Möglichkeiten eines Angreifers eingeschränkt werden. In dieser Bachelorarbeit wurde ein erstes Implementierungskonzept dieser Lösung entwickelt, welches die Durchführung eines Wahlereignises ermöglicht.

Ausgangslage

Die Nutzung des Internets für Abstimmungen und Wahlen bringt das Risiko, dass Angreifer die Geräte von Wählern ausnutzen können, um falsche Stimmen abzugeben oder das Stimmgeheimnis zu verletzen. Das erste Problem wurde bereits durch die Implementierung von Prüfcodemechanismen in zahlreichen kryptografischen Protokollen gelöst, die eine Cast-as-intended-Verifizierung gewährleisten. Andererseits hat sich in der Praxis die Sicherstellung der Privatsphäre der Stimme als schwierig erwiesen. Eine neue und innovative Protokollstrategie könnte jedoch helfen, die Angriffsfläche auf dem persönlichen Gerät auf ein Minimum zu reduzieren und die Gefahr potenziell manipulierter Wahlgeräte zu eliminieren. Die dabei eingesetzte Methode hat jedoch im Moment keine praktische Anwendung und existiert daher nur auf dem Papier.

Beispiel für eine einfache Abstimmung mit 3 Wahloptionen und Bestätigung im neuen Protokoll

Ziele

Das Ziel dieses Projekts war ein Art Proof-of-Concept System zu entwickeln, das alle notwendigen Aspekte und Spezifikationen des neuen Protokolls abdeckt. Das Endprodukt muss neben der Implementierung aller verwendeten kryptographischen Algorithmen auch den Benutzern die Möglichkeit geben, an einer Wahlveranstaltung teilzunehmen. Die Idee der Umsetzung ist dabei die Vorteile des Protokolls zu demonstrieren, indem die Wähler für ihre Stimmabgabe statt einer zusätzlichen App den bereits vorinstallierten QR-Code-Scanner auf ihren Geräten verwenden.

Implementation

Der erste Schritt bei der Entwicklung bestand darin, ein vereinfachtes, aber funktionsfähiges System zu schaffen, welches es ermöglicht, den Ablauf des Protokolls anhand von vordefinierten Daten zu simulieren. Die dort eingeführten Annahmen und Vereinfachungen werden allmählich durch die Erfüllung der Protokollanforderungen und Funktionalitäten aufgehoben, was schliesslich in einem Demo-System resultiert.

Resultate

Das realisierte System ist in der Lage die Interaktionen zwischen Komponenten im Protokoll zu unterstützen und auf Benutzeranfragen zu antworten. Ausserdem bekommen die Nutzerinnen und Nutzer als Wähler im System ihre persönliche private Wahlkarten als PDF ausgedruckt, um sich ein realistisches Bild vom Wahlvorgang machen zu können. Am Ende konnte die bereitgestellte Anwendung, selbst unter leicht eingeschränkten Bedingungen, die Eleganz und Effizienz des Protokolls beweisen, insbesondere bei durchgeführten Referenden mit einer geringen Anzahl von Wahloptionen.

Luka Velkov