FUSE - ein Internetwahlsystem für zeitlich unbegrenzt geheime Betriebsratswahlen

Melanie Volkamer, Walter Reinhard, Roland Vogt

melanie.volkamer@dfki.de, walter.reinhard@siemens.com, roland.vogt@dfki.de

Abstract: Die zahlreichen Internetwahlprojekte der vergangenen Jahre haben gezeigt, dass Internetwahlen zu einer realen Möglichkeit geworden sind. Es wurde aber auch deutlich, dass die technischen Schwächen der existierenden Internetwahlsysteme in der zeitlich unbegrenzten Wahrung des Wahlgeheimnisses liegen. Vor diesem Hintergrund wurde das Internetwahlsystem FUSE für den Einsatz bei Betriebsratswahlen in Betrieben, in denen die Mitarbeiter über eine Jobkarte mit PKI-Funktionalität verfügen, entworfen. Es setzt durch eine Kombination verschiedener Sicherheitsmechanismen die zeitlich unbegrenzte geheime Wahl sowie alle weiteren für eine Wahl erforderlichen Sicherheitsziele um. Dazu zählen insbesondere die Nichtbeweisbarkeit des Inhaltes der Stimmabgabe, die Integrität und Authentizität der Stimmen bei der Übertragung, Speicherung und Auszählung sowie die Korrektheit des Wahlergebnisses. Eine Sicherheitsanalyse in Anlehnung an die Common Criteria (CC) zeigt, dass alle geforderten Sicherheitsziele von FUSE erreicht werden.

1 Einleitung

Nach einer Erklärung des Bundesinnenministers Otto Schily vom 29. August 2005 ist die E-Government-Initiative „BundOnline am Ziel“. In seiner Rede auf der gleichnamigen Veranstaltung machte er gleichzeitig deutlich, dass die Modernisierung von Bürgerdiensten und Bürgerbeteiligung damit aber erst an ihrem Anfang steht[1]. Das ist nicht überraschend und trifft insbesondere auf alle Formen demokratischer Prozesse (E-Democracy) zu.

Die vorliegende Arbeit konzentriert sich auf E-Voting und hier insbesondere auf Internetwahlen als dem zentralen Aspekt von E-Democracy. Seit Ende der neunziger Jahre werden weltweit zahlreiche Systementwürfe für die elektronische Stimmabgabe und -auszählung entwickelt und erprobt. Dass das Thema immer noch aktuell ist, zeigen beispielsweise die diesjährige Wahl zum deutschen Bundestag, bei der in zwei Hamburger Wahllokalen ein Experiment mit elektronischen Stiften zur Stimmabgabe durchgeführt wird sowie die Internetwahlen der Gesellschaft für Informatik (GI) und der Initiative D21. Allgemein ist in Deutschland tendenziell eine stufenweise Annäherung an das Thema Internetwahlen festzustellen. Während Gremien- und Vereinsvorstände bereits heute rechtsgültig mit In-

[1] Otto Schily: „Die Modernisierung der öffentlichen Verwaltung ist aber kein statisches Ziel, das einmal erreicht und damit erledigt ist. Der Ausbau und die Ausweitung von E-Government-Leistungen ist eine bleibende Aufgabe, an der wir weiter arbeiten.“

ternetwahlen gewählt werden, fanden im Bereich der Betriebs- und Personalratswahlen als der nächsten Stufe nur einzelne Testwahlen statt. Dies hat in erster Linie soziale und juristische Gründe, welche hier nicht diskutiert werden sollen.

Für die Akzeptanz von Internetwahlen beim Wähler als dem Souverän demokratischer Wahlen ist ein breiter gesellschaftlicher Diskurs über das Verhältnis von Wahlrechtsgrundsätzen und den eingesetzten Internetwahltechnologien notwendig. Ein zentraler Aspekt dieses Diskurses ist die IT-Sicherheit, denn die Stabilität demokratischer Strukturen ist eng verknüpft mit der Verlässlichkeit des Wahlvorgangs.

Im vorliegenden Beitrag wird das Internetwahlsystem FUSE (**f**ree, **u**niversal, **s**ecret, **e**qual) beschrieben. Es ist für den Einsatz bei Betriebsratswahlen konzipiert und ermöglicht die Stimmabgabe vom PC am Arbeitsplatz. Gerade bei Betriebsratswahlen fühlen die Wähler häufig ein fundamentales Misstrauen in Bezug auf die Gefahr von Wahlmanipulationen. Die IT-Sicherheit muss daher höchsten Ansprüchen genügen. Die für FUSE definierten Sicherheitsziele sind direkt aus den Wahlrechtsgrundsätzen abgeleitet. Diese werden ohne wesentlich einschränkende Annahmen erreicht. Das besondere Merkmal von FUSE im Vergleich zu alternativen Systementwürfen ist die zeitlich unbegrenzte Geheimhaltung der Zuordnung von Wähler und Stimme bei gleichzeitig hoher Widerstandsfähigkeit gegen Manipulationsversuche. Insbesondere beruht die dauerhafte Geheimhaltung nicht auf kryptographischen Annahmen sondern auf der Architektur und den Protokollen des Systems. FUSE verwendet einige bekannten und gut untersuchte Ansätze, wie z. B. blinde Signaturen, One-Time-Pad, organisatorische Gewaltenteilung und Mehrfachstimmabgabe. Ihre Kombination führt zu dem ersten Systementwurf für ein Internetwahlsystem, welches den Grundsatz der geheimen Wahl ohne Einschränkung umsetzt und gleichzeitig alle anderen Wahlrechtsgrundsätze respektiert.

Die Beschreibung und die Sicherheitsanalyse von FUSE erfolgt auf der Grundlage einer systematischen Bedrohungsanalyse. Sie ist an die Struktur und Terminologie der *Common Criteria (CC) for IT Security Evaluation* angelehnt. Mit dieser für Internetwahlen neuartigen Form der Darstellung wird hier eine standardisierte Grundlage für die Diskussion über die Sicherheitseigenschaften von Internetwahlsystemen gegeben.

2 Sicherheitsziele

Internetwahlen zählen zu den sicherheitskritischsten Internetanwendungen und müssen eine Reihe von Sicherheitseigenschaften erfüllen. Diese wurden vielfach untersucht und ergeben sich im Wesentlichen aus den gesetzlich festgelegten Wahlrechtsgrundsätzen, die eine freie, allgemeine, geheime, gleiche und unmittelbare Wahl fordern. Die bekanntesten Zusammenstellungen von Anforderungen an ein Internetwahlsystem sind der Anforderungskatalog für „Online-Wahlen für nicht-parlamentarische Wahlen“ der Physikalisch Technischen Bundesanstalt [PTB04] und die Empfehlungen des Europarates [oE04]. Beide Kataloge umfassen neben den technischen Sicherheitsanforderungen u.a. auch Anforderungen an das Management und die Benutzerfreundlichkeit. Abgeleitet aus den vorhandenen Katalogen betrachten wir die folgenden Sicherheitsziele (Security **O**bjectives):

O1 – Das Internetwahlsystem muss sicherstellen, dass zu keinem Zeitpunkt eine Zuordnung zwischen Wähler und seinem Votum hergestellt werden kann. Die *geheime* Wahl muss also zeitlich uneingeschränkt gewährleistet werden [UKK98]. Es darf weder über den Zeitpunkt der Stimmabgabe noch über die IP-Adresse des Wählers von einer Stimme auf den zugehörigen Wähler geschlossen werden können. Insbesondere muss die geheime Wahl auch dann gewährleistet sein, wenn eine der Komponenten manipuliert ist. **O2** – Im Zusammenhang mit der *freien* und auch *geheimen* Stimmabgabe darf kein Beweis über das Votum des zugehörigen Wählers existieren. **O3** – Um eine *gleiche* Wahl gewährleisten zu können, muss das Internetwahlsystem einen Authentisierungsmechanismus einsetzen, der mindestens so fälschungssicher ist wie die Authentifizierung bei der traditionellen Wahl. **O4** – Außerdem verlangt die *gleiche* Wahl, dass es zu keinem Zeitpunkt möglich sein darf, unbemerkt Stimmen hinzuzufügen, zu verändern oder zu löschen. Dies gilt sowohl bei der Stimmabgabe als auch bei der Übertragung und der Speicherung und auch dann, wenn eine der Komponenten manipuliert ist. **O5** – Schließlich ergibt sich aus der Forderung nach einer *gleichen* Wahl das Ziel der korrekten Ergebnisermittlung. In diesem Zusammenhang wird teilweise auch gefordert, dass der Wähler überprüfen können muss, ob seine Stimme gezählt wurde.

Neben diesen Zielen, die ein Internetwahlsystem erreichen soll, werden folgende Sicherheitsziele an die Umgebung (Security **O**bjectives for the **E**nvironment) betrachtet: **OE1** – Zur Gewährleistung der *allgemeinen* Wahl muss die Verfügbarkeit des Internetwahlsystems sichergestellt werden. **OE2** – Abgeleitet von der Zusammensetzung des Wahlpersonals aus Mitgliedern unterschiedlicher Interessengruppen, besteht eine wichtige Vorgabe darin, nicht einer einzelnen Komponente des Internetwahlsystems vertrauen zu müssen. Daher wird verlangt, dass ein Internetwahlsystem auch dann obige Ziele erreicht, wenn eine seiner Komponenten manipuliert wurde. Entsprechend dieser Forderung an das Wahlsystem muss die Umgebung gewährleisten, dass zu keinem Zeitpunkt der Wahlperiode mehr als eine Komponente manipuliert ist. **OE3** – Das dritte Ziel der Umgebung besteht im Einsatz von derzeit als sicher anerkannten Kryptoalgorithmen.

3 Bedrohungen und Annahmen

Bedrohungen (**T**hreats) für eine Internetwahl können zwei verschiedene Hintergründe haben: **T1** – Die erste Bedrohung ist das Brechen des Wahlgeheimisses. Hierzu kann der Angreifer entweder die Zuordnung von einem bestimmten Wähler zu dessen Stimmzettel während oder nach der Wahl herstellen (O1) oder er erwirbt die Zuordnung von einem Wähler, der ihm seine Stimme verkauft hat (O2). **T2** – Bei der zweiten Bedrohung versucht der Angreifer das Wahlergebnis gezielt durch aktive Eingriffe in den Netzverkehr zu manipulieren. Hierzu kann er versuchen, Stimmen unbemerkt hinzuzufügen, zu löschen oder zu verändern (O4), sich als eine wahlberechtigte Person auszugeben und in deren Namen zu wählen (O3) oder das Auszählmodul zu verändern (O5).

Neben obigen Bedrohungen gehen wir von folgenden Annahmen (**A**ssumptions) aus: **A1** – Wir nehmen an, dass der Angreifer keine Angriffe gegen die Verfügbarkeit durchführt. Hintergrund ist, dass Denial-of-Service-Attacken und ähnlichen Angriffen durch orga-

nisatorische Maßnahmen entgegengewirkt werden kann – beispielsweise durch längere Wahlzeiträume. **A2** – Außerdem nehmen wir an, dass es dem Angreifer nicht gelingt, mehr als eine Komponente des Internetwahlsystems unbemerkt zu manipulieren. Dies kann durch ein entsprechendes Security Management (bspw. Aufstellung der Komponenten an unterschiedlichen Orten, Zugriff nur mit 4-Augen-Prinzip, Schutz durch vorgeschaltete Firewalls) gewährleistet werden. **A3** – Als Annahme an die Angreifermächtigkeit setzen wir voraus, dass ein potentieller Angreifer während der Wahl die eingesetzten Verschlüsselungs- und Signierverfahren nicht brechen kann. An dieser Stelle sei darauf hingewiesen, dass wir davon ausgehen müssen, dass ein Angreifer in der Zukunft dazu in der Lage sein wird.

Die Zusammenhänge zwischen den Bedrohungen und Sicherheitszielen sowie zwischen den Annahmen und den Sicherheitszielen für die Umgebung sind in Abbildung 1 veranschaulicht.

	T1	T2	A1	A2	A3
O1	×				
O2	×	×			
O3		×			
O4		×			
O5		×			
OE1			×		
OE2		×		×	
OE3	×	×			×

Abbildung 1: Abbildung der Ziele auf die Bedrohungen und Annahmen

4 Betriebsratswahlen als Anwendungsfeld

Betriebsratswahlen bieten aus vielerlei Hinsicht ein interessantes Einsatzgebiet für Internetwahlen: Zunächst ist die Basis für die Einführung von Internetwahlen gegeben, da jeder Mitarbeiter über einen Rechner verfügt[2] und damit umgehen kann (kein Digital Divide). Weiterhin ist in vielen Betrieben bereits eine Public-Key-Infrastruktur vorhanden oder für die nächsten Jahre angedacht, so dass jeder Angestellte eine Jobkarte mit integrierter Signaturfunktionalität sowie ein entsprechendes Lesegerät am Arbeitsplatz besitzt. Dies ermöglicht den Einsatz von digitalen Signaturen zur Authentisierung der Wähler, ohne dass zusätzliche Kosten entstehen.

Hinzu kommen die Vorzüge des betriebseigenen Intranets und die Administrationspolitik: In der Regel sind die Mitarbeiterrechner zentral verwaltet. Große Betriebe, deren Zweigstellen deutschlandweit verstreut sind und die daher ein besonders hohes Interesse an der Einführung einer Internetwahl haben, verfügen meist über ihr eigenes sicheres Rechenzen-

[2] In Betrieben, in denen dies nicht der Fall ist, können zusätzlich Wahlterminals aufgestellt werden.

trum mit geschützten Servern, redundanten Systemen und Maßnahmen gegen Angriffe.

Trotz dieser technischen Vorzüge darf nicht außer Acht gelassen werden, dass für rechtsgültige Internetwahlen in Betrieben das Betriebsverfassungsgesetz [BMW01] geändert werden muss. Insbesondere ist derzeit die Präsenzwahl der Regelfall und die Briefwahl (als Form der Distanzwahl) nur als Ausnahmeregelung zugelassen. Aus verschiedenen Gründen wie Einfachheit, Kostenersparnis, Wählermobilität und Zeitersparnis erscheint die Internetwahl vom Arbeitsplatzrechner die zukunftsweisende Form der Internetwahl zu sein. Damit stößt man aber zwangsläufig auf die Probleme der Distanzwahl und die Gründe, warum die Briefwahl nur in Ausnahmefällen erlaubt ist, nämlich die Sicherstellung der geheimen und freien Stimmabgabe im privaten Umfeld [KV05]. Hier ist eine gesellschaftliche Diskussion zur Akzeptanz erforderlich. Aber auch technisch muss diesem Problem begegnet werden.

Ein Schwachpunkt in Betrieben ist die Möglichkeit des Systemadministrators, die Kommunikation mitzulesen und über IP-Adresstabellen sogar einzelnen Angestellten zuordnen zu können. Dies führt bei einer Reihe von bekannten Internetwahlsystemen zu einem Widerspruch mit dem Sicherheitsziel der zeitlich unbegrenzt geheimen Wahl. Hier ist ein zusätzlicher Mechanismus erforderlich.

5 FUSE - Sicherheitsprinzipien

Der Systementwurf von FUSE basiert auf den nachfolgend beschriebenen Prinzipien. Sie stellen die zentralen Aspekte seiner Sicherheitspolitik dar.

Der Architekturentwurf setzt das Prinzip der Gewaltenteilung so weitgehend durch, dass die Manipulation einer einzelnen Komponente nicht ausreicht, um die geheime Wahl zu brechen (**T1**) oder unbemerkt das Wahlergebnis gezielt zu manipulieren (**T2**). Dies bedeutet insbesondere, dass alle Komponenten von unterschiedlichen Betreibern gehostet werden und der Zugriff nur über ein Vier-Augen-Prinzip möglich ist. Den Problemen bzgl. der Stimmabgabe im ‚ungesicherten' Arbeitsplatzumfeld begegnen wir analog zu [Ins02] mit dem Konzept der Mehrfachstimmabgabe, bei der nur die zuletzt abgegebene Stimme zählt. Insbesondere Wähler, die bei der Stimmabgabe beeinflusst oder gar genötigt wurden, können ihre Stimme erneut abgeben. Auf diese Weise wird auch dem Stimmenhandel entgegen gewirkt. Selbst wenn der Wähler einen Nachweis vom System über seine Stimmabgabe erhält, kann er gegenüber Dritten nicht beweisen, dass dieser Nachweis auch zu der Stimme gehört, die letztlich gezählt wird.

Die einzige Möglichkeit, das Wählervotum zeitlich unbegrenzt geheim zu halten, ist der Einsatz einer One-Time-Pad Verschlüsselung. Eine benutzerfreundliche Umsetzung dieses Verfahrens ist der *Vote Scrambling Algorithm (VSA)* [FZ05]. Die Idee des VSA-Ansatzes ist, dass jeder Wähler seinen eigenen *Wählerstimmzettel* erhält, auf dem jedem Kandidaten eine spezifische Nummer – die Kandidatennummer *KN* – zugeordnet ist. Diese gibt der Wähler bei der Stimmabgabe ein (statt der Markierung). Ausgangspunkt für die Berechnung der einzelnen Wählerstimmzettel und damit der Nummer jedes Kandidaten ist der

originale Stimmzettel, auf dem alle Kandidaten[3] in einer festen Reihenfolge gelistet sind. Auf diese Weise erhält jeder Kandidat eine Ausgangsnummer (*aNr*). Nun wird für jeden Wählerstimmzettel eine Zufallszahl (*r*) modulo der Anzahl der Kandidaten (*k*) berechnet. Der Wert (*KN*) jedes Kandidaten auf dem entsprechenden Wählerstimmzettel wird dann durch eine einfache Modulooperation $KN = r + aNr \bmod k$ berechnet. Jeder Wählerstimmzettel ist damit eine zyklische Verschiebung des ursprünglichen Stimmzettels. Die One-Time-Pad Eigenschaften sind gegeben, da die Zufallszahl für jeden Stimmzettel zufällig neu bestimmt wird und genauso lang wie die Nachricht selbst ist. Die Geheimhaltung des One-Time-Pads (*r*) erfolgt organisatorisch.

Die Jobkarte als sichere Komponente erhält neben der Authentifizierung des Wählers noch eine weitere Funktionalität: Sie erzeugt und speichert Wahlberechtigungsinformationen zur anonymen Stimmabgabe. Enscheidend ist dabei, dass es nicht möglich ist, diese Token von der Karte auszulesen. So wird verhindert, dass diese Tokens zur berechtigten Stimmabgabe an unberechtigte Personen weitergegeben wird.

Zur Steigerung des Wählervertrauens hat der Wähler nach der Wahl die Möglichkeit, mit seiner Jobkarte zum Wahlvorstand zu gehen und zu prüfen, ob und wie seine Stimme gezählt wurde (Auditing).

6 FUSE – Systembeschreibung

In diesem Kapitel erläutern wir die Gesamtarchitektur von FUSE und beschreiben die einzelnen Phasen des Wahlablaufs (Wahlvorbereitung, Wahlberechtigungsprüfung, Stimmabgabe und Wahlende), um anschließend zeigen zu können, dass die Sicherheitsmechanismen von FUSE die geforderten Sicherheitsziele abdecken.

FUSE besteht aus vier Servern (WVZ-1, WVZ-2, CA und Urne), den PCs der Wähler, einem Auszählungsrechner (RC) und einem externen Provider (EP) (vgl. Abbildung 2). Der externe Provider erzeugt die VSA-Wählerstimmzettel, die beiden Server WVZ-1 und WVZ-2 dienen zur Wahlberechtigungsprüfung, die Aufgabe des Urnenservers ist die Speicherung der Stimmen während der Wahlperiode und auf dem Auszählungsrechner ist die Auszählfunktionalität realisiert. Die Zertifizierungsstelle (CA) informiert die beide Wahlberechtigungsserver, wenn Wähler während der Wahl ihre Karte sperren lassen, damit mit der entsprechenden Karte nicht mehr gewählt werden kann.

Wahlvorbereitung Im Vorfeld der Wahl lädt die Wahlleitung das Wählerverzeichnis und die öffentlichen Schlüssel der Wähler auf die beiden Server WVZ-1 und WVZ-2. Der externe Provider (EP) wird damit beauftragt, die Wählerstimmzettel zu erzeugen. Er generiert die zufälligen und gleich verteilten One-Time-Pads (*r*), berechnet die entsprechenden Kandidatennummern (*KN*) und versieht jeden Wählerstimmzettel mit einer eindeutigen Kennzahl (*KZ*). Dies ist erforderlich, um bei der Auszählung die Ausgangsnummer (*aNr*) jedes Kandidaten wieder extrahieren zu können. Zusätzlich fertigt der EP eine Tabelle aus Kennzahlen (*KZ*) und zugehörigen One-Time-Pads (*r*) an, die er verschlüsselt aufbewahrt.

[3] Falls nötig, enthält der Stimmzettel auch eine Möglichkeit zur ungültigen Stimmabgabe.

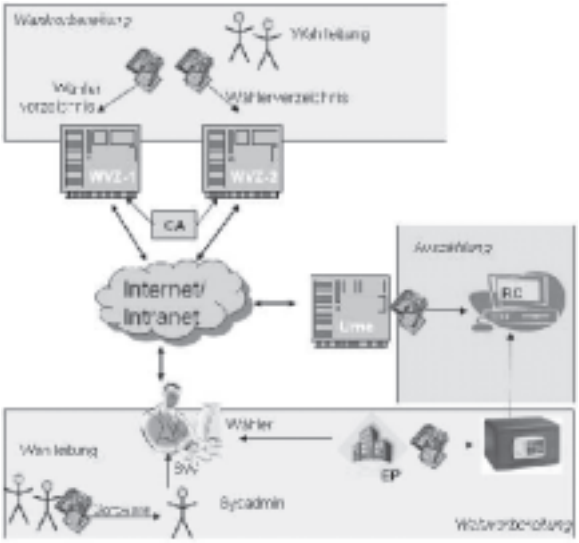

Abbildung 2: Systemarchitektur

Die Wählerstimmzettel werden anonym an die Wähler verteilt, so dass keine Zuordnung zwischen Stimmzettel und Wähler besteht. Eine Möglichkeit zur anonymen Verteilung ist das Ziehen des Wählerstimmzettels aus einer Trommel. Eine persönliche Zustellung ist weder erforderlich noch geeignet, da ein Wähler auch mehr als einen Wählerstimmzettel erhalten kann (Mehrfachstimmabgabe). Für die Komponenten Urne, RC, WVZ-1 und WVZ-2 werden Schlüsselpaare erzeugt und der Administrator installiert die FUSE-Wählersoftware inklusive der öffentlichen Schlüssel aller Komponenten auf den PCs der Wähler. Außerdem wird der öffentliche Schlüssel der beiden Server VWZ-1 und WVZ-2 auf den Urnenserver und den Auszählungsrechner geladen und der öffentliche Schlüssel der Urne auf dem Auszählungsrechner installiert. Abschließend werden alle Serverkomponenten konfiguriert und frei geschaltet. Der Ablauf der Wahl ist dann für alle Wähler gleich. Die einzelnen Schritte sind als Sequenzdiagramme in Abb. 3 und 4 dargestellt.

Wahlberechtigungsprüfung Die Wahlberechtigungsprüfung beginnt, wenn der Wähler die FUSE-Wählersoftware auf seinem PC startet: Zunächst prüft die Software, ob ein Kartenlesegerät angeschlossen und eine Jobkarte eingesteckt ist. Anschließend wird die Wahlfunktionalität der Karte angestoßen, um ein zufälliges Token t zu erzeugen und es mit einem zufälligen Faktor b zu ‚blinden' *(1)*. Nach Aktivierung der Jobkarte *(2, 3)* wird der so erhaltene Wert $b*t$ damit vom Wähler (W) signiert. Das Ergebnis[4] $sig(W, b*t)$und $b*t$ werden anschließend an die FUSE-Wählersoftware übergeben *(4)*, die eine Wahlberechtigungsanfrage an WVZ-1 versendet *(5)*. WVZ-1 überprüft nun anhand der erhalten-

[4]Notation: *Operation(Schlüsselinhaber, Nachricht)*. Ob der öffentliche oder der geheime Schlüssel des Inhabers verwendet wird, hängt davon ab, ob die Nachricht verschlüsselt (*ver*) oder signiert (*sig*) wird. Eine Signatur beinhaltet nur den Hashwert der Nachricht. Teile von Nachrichten werden durch das Zeichen # verbunden.

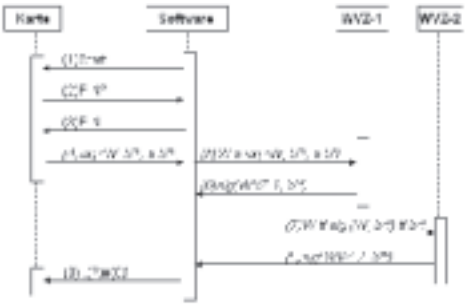

Abbildung 3: Wahlberechtigungsprüfung

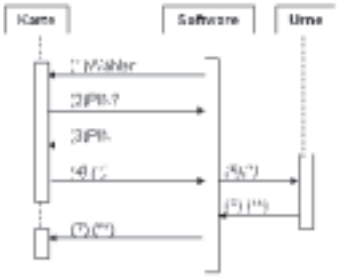

Abbildung 4: Stimmabgabe

den Daten zunächst, ob der Wähler im Wählerverzeichnis aufgelistet ist, anschließend, ob die Signatur korrekt ist und gültig ist und zuletzt, ob der Wähler bereits eine Wahlberechtigungsanfrage geschickt hat. Falls alle Überprüfungen zu einem positiven Ergebnis führen, registriert WVZ-1 die Anfrage und schickt dem Wähler einen Berechtigungsnachweis $sig(WVZ\text{-}1, b*t)$ *(6)*. Parallel findet die gleiche Anfrage an WVZ-2 statt *(7)*. WVZ-2 schickt entsprechend $sig(WVZ\text{-}2, b*t)$ zurück *(8)*. Die Wahlsoftware verifiziert die Signaturen von WVZ-1 bzw. WVZ-2 und gibt die Daten an die Karte weiter *(9)*. Die Karte entfernt nun den jeweiligen Blindungsfaktor und erhält: $sig(WVZ\text{-}1, t)$ und entsprechend $sig(WVZ\text{-}2, t)$. Damit ist die Wahlberechtigungsüberprüfung abgeschlossen.

Stimmabgabe Die FUSE-Wählersoftware leitet den Wähler automatisch zur Stimmabgabe weiter. Hier wird eine Eingabemaske für die Kandidatennummer *KN* und die Kennzahl *KZ* angezeigt. Nachdem der Wähler die entsprechenden Daten eingegeben hat, werden diese zusammen mit dem öffentlichen Schlüssel des Urnenservers (Urne) und des Auszählungsrechners (RC), sowie einem Zeitstempel *time* eines verläßlichen Zeitservers an die Karte weitergeleitet *(1)*. Diese berechnet nach Eingabe der korrekten PIN durch den Wähler *(2, 3)* den Stimmdatensatz

$$ver(Urne,time\#sig(WVZ\text{-}1, t)\#t\#ver(RC,KN\#KZ\#sig(WVZ\text{-}2, t)\#t)) \quad (*)$$

und gibt ihn an die Wählersoftware zurück *(4)*, die die Daten an den Urnenserver schickt *(5)*. Dieser entfernt mit dem eigenen geheimen Schlüssel die äußere Verschlüsselungs und prüft die Signatur des Wählerverzeichnis WVZ-1 auf dem Token t. Der hintere Teil der Nachricht ($ver(RC,KN\#KZ\#sig(WVZ\text{-}2, t)\#t)$) ist für den Auszählungsrechner verschlüsselt und wird zusammen mit dem Token t und der Zeit *time* in der Urne abgespeichert. Falls zu dem gleichen Token zu einem späteren Zeitpunkt eine weitere Stimme eingeht, wird die alte durch die neue ersetzt. Zur Bestätigung der Stimmabgabe schickt der Urnenserver die Signatur des hinteren Teils des Stimmdatensatzes

$$sig(Urne, ver(RC,KN\#KZ\#sig(WVZ\text{-}2, t)\#t)) \quad (**)$$

an den Wähler zurück *(6)*. Die FUSE-Wählersoftware schickt die erhaltene Nachricht zur Verifikation der Signatur des Urnenservers und zur Speicherung an die Jobkarte *(7)*. Ab-

schließend signalisiert eine Rückmeldung an die Wahlsoftware dem Wähler, dass seine Stimmabgabe erfolgreich abgeschlossen wurde.

Die Wahlberechtigungsprüfung und die Stimmabgabe können auch zu unterschiedlichen Zeitpunkten und von verschiedenen Rechner stattfinden, da die zur Stimmabgabe benötigten Daten auf der Jobkarte gespeichert sind. Möchte ein Wähler ein zweites Mal seine Stimme abgeben, so wiederholt er die Stimmabgabephase mit den auf der Karte bereits gespeicherten signierten Tokens. Da der Wähler nun erneut eine Kennzahl eingeben muss, hat er auch die Möglichkeit, einen neuen Wählerstimmzettel zu verwenden.

Wahlende Nach dem Ende der Wahlperiode werden alle Server vom Netz getrennt. Die gespeicherten Stimmdatensätze (inkl. der Tokens) werden vom Urnenserver auf den Auszählungsrechner (beispielsweise mittels CD) übertragen. Gleiches geschieht mit der Liste der signierten blinden Token $b*t$ der beiden Server WVZ-1 und WVZ-2. Schließlich übergibt der externe Provider (EP) der Wahlleitung die verschlüsselte Zuordnungsliste (Kennzahl KZ – One-Time-Pad r). Diese lädt die Liste und aktiviert die Auszählprozedur. Hierbei wird bei jeder Stimme geprüft, ob das Token t korrekt signiert ist und noch nicht vorkam. Weiterhin wird das Token mit den Einträgen $b*t$ aus den Wählerverzeichnissen verglichen, um sicher zu stellen, dass das signierte Token der Form $sig(WVZ\text{-}2, t)$ ist und nicht etwa $sig(WVZ\text{-}2, b*t)$ (im zweiten Fall wurde die Stimme nicht von der entsprechenden Jobkarte sondern aus abgefangenen Kommunikationsdaten erzeugt)[5]. Außerdem wird sichergestellt, dass das entschlüsselte Token mit dem übereinstimmt, welches der Urnenserver angegeben hat. Abschließend wird das tatsächliche Votum extrahiert und separat gespeichert. Nachdem dies für alle Stimmdatensätze geschehen ist, wird das Ergebnis berechnet und veröffentlicht. Die Auszählung erfolgt offline, um nachträglichen Manipulationen vorzubeugen. Da die Schnittstellenbeschreibung öffentlich ist, kann auch jede andere Software zur Auszählung verwendet werden, um so sicherzustellen, dass das Ergebnis korrekt berechnet wird.

7 Sicherheitsanalyse

O1: Unbegrenzt geheime Wahl Die geheime Stimmabgabe wird durch die Gewaltenteilung und den VSA-Ansatz realisiert. Dadurch kennen die jeweiligen Komponenten nur Teilinformationen, die alleine aber nicht ausreichen, um eine Zuordnung zwischen Wähler und Votum herzustellen. Die beiden Server WVZ-1 und WVZ-2 wissen nur, welche Wähler ein Token erfragt haben. Die Urne kann zwar über die Zuordnung von Wähler und IP-Adresse auch die Zuordnung zwischen Wähler und verschlüsseltem Datensatz ermitteln, aber es fehlt ihr die Zuordnung zwischen Kennzahl und Wahlstimmzettel. Dem Auszählungsrechner fehlt jede Information über die Wähler, um eine Zuordnung herstellen zu können. Das Abhören des Netzwerkes führt auch nicht zum Brechen des Wahlgeheimnisses, weil dem Angreifer die Zuordnung der Kennzahl zum Wählerstimmzettel fehlt. Damit ein Angriff durch den externen Provider ausgeschlossen werden kann, ist eine weitere

[5] t und b müssen groß genug gewählt werden, damit die Wahrscheinlichkeit, dass $t = t'$ oder $t = t' * b$ vernachlässigbar klein ist.

Gewaltenteilung erforderlich. Einer der externen Provider kennt die Zuordnung zwischen One-Time-Pads und Pseudonymen und der andere die Zuordnung zwischen diesen Pseudonymen und den Kennzahlen.

O2: Keine Beweiskraft für eigenes Votum FUSE liefert dem Wähler wegen der Möglichkeit zur erneuten Stimmabgabe während der Wahl keinen Beweis für sein Votum. Auch nach der Wahl kann der Wähler keinen solchen Beweis erhalten, weil dafür die versendete Bestätigung mit dem endgültigen Inhalt der Urne abgeglichen werden muss.

O3: Angemessen sichere Authentifizierungstechnik Der Einsatz der Jobkarte zur Authentifizierung gegenüber den Wahlverzeichnisservern und den signierten Tokens, die die Jobkarte nur verschlüsselt verlassen, ist so sicher wie das bewährte Authentifizierungsverfahren mittels Personalausweis[6]. Eine Weitergabe der Jobkarte zusammen mit der PIN kann ausgeschlossen werden, da an die Karte weitere Funktionalitäten gebunden sind. Insbesondere wäre der Stimmenkäufer in der Lage jedes beliebige Dokument unwiderruflich im Namen des Karteninhabers zu signieren. Das Verfahren stellt ebenfalls sicher, dass die von den Wählerverzeichnissen erhaltenen blind signierten Token nicht weitergeben werden können, da nur die Karte, die die Wahlberechtigungsanfrage verschickt hat, im zweiten Schritt einen gültigen Stimmdatensatz erzeugen kann.

O4: Integrität und Authentizität der Stimmen Dieses Ziel wird durch unterschiedliche Mechanismen für den PC des Wählers, die Kommunikation und die Server erreicht: Der VSA-Ansatz hat neben der Sicherstellung der geheimen Wahl noch einen zweiten Effekt. Falls es einem Angreifer gelingen sollte, einen Wähler-PC zu manipulieren, um Einfluss auf das Ergebnis zu nehmen, so gelingt ihm dies nicht gezielt, da er das zugehörige One-Time-Pad r nicht kennt. Darüber hinaus ist ungewiss, ob dies die Stimme ist, die gezählt wird oder ob der Wähler zu einem späteren Zeitpunkt erneut von einem anderen PC aus seine Stimme abgibt. Ein Angreifer kann auch durch die Manipulation des PCs verhindern, dass die Stimme verschickt wird. Gleichzeitig spielt er dem Wähler aber vor, seinen Wahlvorgang erfolgreich beendet zu haben. Dies fällt auf, wenn der Wähler seine Stimmwahl nach Wahlende überprüft. Eine weitere Möglichkeit des Angreifers, Stimmen hinzuzufügen oder zu löschen besteht darin, das Wählerverzeichnis während der Wahl zu manipulieren. Da zur Stimmabgabe eine gültige Signatur beider Wählerverzeichnisse erforderlich ist, genügt die Manipulationen eines der WVZ nicht, um eine unberechtigte Person zur Wahl zuzulassen Schließlich ist es für einen Angreifer nicht möglich, auf dem Kommunikationsweg oder bei der Speicherung in der Urne neue Stimmen zu erzeugen oder vorhandene unbemerkt zu verändern, da die Signaturen der beiden Wählerverzeichnisse nicht während der Wahlperiode ohne den geheimen Schlüssel erzeugt werden können. Auch das einfache Kopieren von vorhandenen Stimmen fällt bei der Auszählung auf. Die Urne kann Stimmen löschen, da ein Abgleich mit der Anzahl der Wähler, die ein Token erhalten haben nicht aussagekräftig ist (nicht jeder der die Wahlberechtigungsanfrage durchgeführt hat, hat zwingend seine Stimme abgegeben). Sie kann auf diese Weise

[6] Da bei der Ausgabe der Jobkarte die Identität und Authentizität mittels Personalausweis überprüft wurde, ist das bisherige Authentisierungsverfahren lediglich vorgelagert.

das Ergebnis aber nicht gezielt verändern, da sie den Inhalt der gelöschten Stimmen nicht kennt. Darüber hinaus fällt diese Manipulation auf, wenn die entsprechenden Wähler ihre Stimmabgabe beim Wahlveranstalter prüfen lassen.

O5: Korrektheit des Ergebnisses Dieses Ziel ist erreicht, da zum einen die Schnittstellen zum Auszählungsrechner öffentlich sind und jede beliebige Software einsetzbar ist und zum anderen die Auszählung offline erfolgt und die Software zuvor geprüft wurde (diese minimale Funktionalität könnte auch in Form eines Hardware Security Module realisiert sein). Außerdem bietet das System dem Wähler nach der Wahl die Möglichkeit zu verifizieren, ob seine Stimme auch tatsächlich ausgezählt wurde.

8 Vergleich mit anderen Arbeiten

Teilweise werden die Ansätze des FUSE-Systems bereits in anderen Internetwahlsystemen eingesetzt: So wurde die Mehrfachstimmabgabe durch die Bestrebungen in Estland populär. Das estnische System stellt ein Abbild der Briefwahl dar. Die Stimme wird zunächst verschlüsselt (also in einen Umschlag getan) und anschließend signiert (dies entspricht der eidesstattlichen Erklärung) [Maa04]. Die dort gewählten Ansätze genügen aber den von uns definierten Sicherheitszielen nicht. Ein Ansatz, der auf unterschiedlichste Weise in anderen Wahlsystemen zum Einsatz kommt, ist die blinde Signatur. Das bekannteste deutsche System, welches diesen Mechanismus verwendet, ist das i-vote System [OK03]. Die blinde Signatur wird dort für den Stimmzettel verwendet und dient ausschließlich zur offenbar zeitlich begrenzten Sicherung der geheimen Wahl. Im Projekt eVoting.at wurde die Speicherung bestimmter Daten (Wahltoken) auf der Signaturkarte vorgeschlagen [KKPU04]. Hintergrund dort ist die Aufteilung des Wahlprozesses in zwei Phasen: Der Wähler authentifiziert sich in der ersten Phase als Wahlberechtigter mittels einer von ihm signierten Nachricht und erhält ein Wahltoken, welches er auf der Karte speichert und mit dem er später anonym seine Stimme abgeben kann. Das Polyas System von Micromata [Gbm05] ist ein Beispiel für ein System welches die Gewaltenteilung ähnlich konsequent wie FUSE umsetzt. Zur Sicherung der zeitlich unbegrenzt geheimen Wahl existieren weitere Ansätze. So schlägt [vA04] vor, dass jeder Wähler vor der Wahl ein Geheimnis – etwa einen Tiernamen – als One-Time-Pad registriert. Wenn der Wähler nun seine Stimme abgibt, kann er mit dem One-Time-Pad steuern, ob seine Stimme gezählt wird oder nicht.

9 Fazit

Die an die Struktur und Terminologie der Common Criteria (CC) for IT Security Evaluation angelehnte Sicherheitsanalyse hat gezeigt, dass die Wahlrechtsgrundsätze (frei, allgemein, geheim und gleich) vom FUSE-Systementwurf sichergestellt werden. Alle definierten Sicherheitsziele werden erfüllt. Insbesondere ist die zeitlich unbegrenzt geheime Wahl selbst dann gewährleistet, wenn die eingesetzten Kryptoverfahren nach der Wahl gebro-

chen werden oder es einem Angreifer gelingt, eine der Komponenten zu manipulieren.

FUSE kann nicht nur auf Mitarbeiter-PCs, sondern auch auf Kiosksystemen mit den gleichen Sicherheitseigenschaften eingesetzt werden, denn mit dem Konzept der Mehrfachstimmabgabe ist das Wahlgeheimnis im Unterschied zu vielen alternativen Internetwahlsystemen auch bei Beobachtung der Stimmabgabe grundsätzlich geschützt.

Relativ zu den abgewehrten Bedrohungen spricht somit aus technischer Sicht alles für einen Einsatz von FUSE bei Betriebsratswahlen. Derzeit wird an einer prototypischen Implementierung von FUSE gearbeitet, um anschließend Erfahrung mit der Mehrfachstimmabgabe und der Eingabe einer Kandidatennummer sammeln zu können.

Literatur

[BMW01] Bundesministerium fuer Wirtschaft und Arbeit BMWA. Betriebsverfassungsgesetz (BetrVG). *http://bundesrecht.juris.de/bundesrecht/betrvg/inhalt.html (Abrufdatum: 30.08.2005)*, 25.09.2001.

[FZ05] G. Fischer und W. Zuser. *The Vote Scrambling Algorithm*. Schweighofer E., Augeneder, S., Liebwald, D., Menzel, T. - Boorbergverlag, 2005.

[Gbm05] Micromata GbmH. Online-Wahlen für Verbände und Vereine. *http://www.micromata.de/produkte/documents/polyas_broschuere_72dpi.pdf*, 2005.

[Ins02] Internet Policy Institute. Report of the National Workshop on Internet Voting - Issues and Research Agenda. *http://news.findlaw.com/hdocs/docs/election2000/nsfevoterprt.pdf*, 26.07.2002.

[KKPU04] Robert Kofler, Robert Krimmer, Alexander Prosser und Martin Karl Unger. The Role of Digital Signature Cards in Electronic Voting. In *HICSS*, 2004.

[KV05] Robert Krimmer und Melanie Volkamer. Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In *EGOV (Workshops and Posters)*, Seiten 225–232, 2005.

[Maa04] Epp Maaten. Towards Remote E-Voting: Estonian case. In *Electronic Voting in Europe*, Seiten 83–100, 2004.

[oE04] Council of Europe. Legal, operational and technical standards for e-voting. *Recommundation Rec(2004)11 and explanatory memorandum*, 2004.

[OK03] Dieter Otten und Jürgen Küntzler. Über die Herstellung von Anonymität bei elektronischen Wahlen. *Datenschutz und Datensicherheit*, 27(5), 2003.

[PTB04] Physikalisch-Technische Bundesanstalt Braunscheig und Berlin PTB. Online-Wahlsystem für nicht-parlamentarischen Wahlen: Anforderungskatalog. *http://www.berlin.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf (Abrufdatum: 30.08.2005)*, 8.5.2004.

[UKK98] Markus Ullmann, Frank Koob und Harald Kelter. Anonyme Online-Wahlen - Lösungsansätze für die Realsisierung von Online-Wahlen. *DUD * Datenschutz und Datensicherheit 22*, 1998. V2.6.

[vA04] Bernard van Acker. Remote e-Voting and Coercion: a Risk-Assessment Model and Solutions. In *Electronic Voting in Europe*, Seiten 53–62, 2004.