E-Voting
auf Grundlage eines Instant-Messaging-Systems

Anastasia Meletiadou

Institut für Wirtschafts- und Verwaltungsinformatik
Universität Koblenz-Landau
Universitätsstr. 1
56070 Koblenz
nancy@uni-koblenz.de

Abstract: Zur Zeit werden Instant-Messaging-Systeme (IM-Systeme) vorwiegend für private Zwecke wie Telefonie und Chat genutzt. In diesem Papier zeigen wir, dass solche IM-Systeme auch als Grundlage für sicherheitskritische Anwendungen, wie etwa für die Durchführung von elektronischen Wahlen eingesetzt werden können. Anhand konkreter Szenarien für verschiedene Wahlformen werden Anforderungen für eine Implementation entsprechender Sicherheitsmechanismen (im IM-System oder einer Erweiterung) abgeleitet.

1 Einleitung

Die zunehmende räumliche Verteilung von Projekten hervorgerufen durch Globalisierung und internationale Kollaborationen fordert von den beteiligten Unternehmen den Einsatz von flexibleren Kommunikationsformen. Eine Möglichkeit, dieser Problematik zu begegnen, ist das Forschungsgebiet des Computer-Supported Cooperative Work (CSCW), welches sich mit der IT-Unterstützung von Gruppenarbeit beschäftigt. Eine Unterkategorie von CSCW-Anwendungen sind so genannte Instant-Messaging-Systeme (IM). Dabei interpretieren wir diesen Begriff im weiteren Sinne, d.h. wir beziehen zusätzlich zum reinen Austausch von Textnachrichten (Messaging, Chat) auch erweiterte Funktionalitäten wie Sprachtelefonie, Videokonferenz oder Dateiübertragung mit ein. In diesem Artikel untersuchen wir Gruppenentscheidungsprozesse (inkl. Abstimmung), welche technisch durch eine Kombination aus IM und E-Voting-Anwendung unterstützt werden. Damit soll untersucht werden, inwiefern IM-Systeme nicht nur als Kommunikationsmedium im Unternehmenskontext eingesetzt werden können, sondern auch für sicherheitskritische Anwendungen, wie die Durchführung von elektronischen Wahlen oder geschäftliche Transaktionen, (Vertragsabwicklung, elektronische Zahlung) geeignet sind. Zur Bearbeitung des Themas werden zunächst drei Szenarien für Wahlen in kleinen Gruppen vorgestellt, die mit Hilfe eines erweiterten IM-Systems realisierbar sind (Kapitel 2). Anschließend wird die Realisierung des Kommunikations- und Wahlprozesses mit Hilfe eines erweiterten IM-Systems erläutert (Kapitel 3).

2 Szenarienbeschreibung

In diesem Kapitel werden drei Szenarien vorgestellt, die mindestens einen Abstimmungsprozess und optional eine vorausgehende Diskussion enthalten und entsprechend unterschiedliche Sicherheitsziele (z. B. Anonymität, Nicht-Abstreitbarkeit, Integrität) für eine technische Umsetzung mit sich bringen. Die Szenarien werden funktional beschrieben. Wir abstrahieren also zunächst davon, ob sie in traditioneller Form (mit Anwesenheit der Teilnehmer vor Ort) durchgeführt werden oder mittels eines IM-Systems realisiert werden.

2.1 Szenario 1: keine Diskussion, geheime Abstimmung

Das erste Szenario beschreibt eine Wahl ohne Diskussion, mit geheimer Abstimmung. Eine solche Wahl wird beispielsweise bei der Besetzung von universitären Gremien durchgeführt. Solche Wahlen laufen ähnlich einer politischen Wahl ab. Aus den rechtlichen Rahmenbedingungen [La03, Un06] ergeben sich entsprechende Sicherheitsziele: Die *Anonymität* ist durch das Vertrauensmodel der Wahlkommission gegeben. Der Wähler ist im Wählerverzeichnis registriert und erhält nach Vorlage seines Ausweises und Wahlberechtigung einen Stimmzettel, den er unter Ausschluss der Öffentlichkeit ausfüllt. Es gibt zu keinem Zeitpunkt eine Verbindung zwischen seinem Namen und seiner Stimme. Die *Nicht-Abstreitbarkeit* kann in zwei Formen auftreten. Erstens, wenn der Wählende nicht abstreiten kann, *dass* er gewählt hat (Teilnahme nachweisbar) und zweitens, wenn der Wählende nicht abstreiten kann, *wie* er gewählt hat (Stimme nachweisbar). Die erstere Form ist zwar eventuell durch die Beobachtung der Öffentlichkeit und ein „Abhaken“ im Wählerverzeichnis gegeben, hat aber bei diesem Szenario keine größere Relevanz. Die zweite Form ist in diesem Szenario (geheime Wahl) ausdrücklich auszuschließen. Eine dritte Eigenschaft ist die *Integrität* des Ergebnisses. Wenn ein Wähler die korrekte Erfassung der Stimmen anzweifelt, kann er basierend auf dem Öffentlichkeitsprinzip die Wahl mitverfolgen und eine Nachzählung verlangen. Weiterhin gilt hier, dass die *Festlegung der Wahlberechtigten* in einem vorherigen Schritt erfolgt. Die *Authentizität* der Wahlberechtigen beim Wahlvorgang wird durch das Vorzeigen eines Ausweises überprüft. Das *Ergebnis* wird dann von der Wahlkommission durch Auszählung der anonymen Stimmzettel ermittelt und veröffentlicht.

2.2 Szenario 2: offene Diskussion, offene (namentliche) Abstimmung

Ein Universitätssenat könnte auf einer Sitzung z.B. über die Erweiterung des Curriculums um einen weiteren Studiengang abstimmen wollen. Die Mitglieder unterhalten sich zunächst über alle denkbaren Möglichkeiten, auch vertrauliche Kommunikation zwischen zwei Beteiligten („Flüstern“) ist erlaubt. Hier finden sowohl die Diskussion als auch die Abstimmung (einfaches Handzeichen) offen statt (*keine Anonymität*). Das Ergebnis kann von jedem Anwesenden durch Abzählen der Handzeichen nachvollzogen werden (*Nicht-Abstreitbarkeit* der Stimmen und die *Integrität des Ergebnisses*). Ebenso, wie im vorigen Szenario, erfolgt die *Festlegung der Wahlberechtigten* zu einem früheren Zeitpunkt. Die *Authentifikation der Wahlberechtigen* erfolgt in der Regel auf Grund

persönlicher Bekanntschaft ohne Vorlage von Ausweisen oder anderer technischer Identifikationsmerkmale. Das *Ergebnis* wird in Form eines Protokolls während der Sitzung festgehalten.

2.3 Szenario 3: offene Diskussion, geheime Abstimmung

Eine Kombination der ersten beiden Szenarien ist eine Wahl mit einer offenen Diskussion und einer geheimen Wahl. Eine solche Wahl kann beispielsweise bei Personalentscheidungen im Senat einer Universität auftreten. Die Teilnehmer unterhalten sich zunächst offen über die Besetzung der Stelle. Dann erfolgt in einer geheimen Abstimmung die Entscheidung. In diesem Szenario ist *Anonymität* nur während der Wahl gewünscht, es gelten die gleichen Aussagen wie im Szenario 1. Diese Anonymität heisst im Umkehrschluß, dass *Nicht-Abstreitbarkeit* ausdrücklich nicht gewünscht ist. Allerdings kann durch die vorherige Kommunikation eine Tendenz der Teilnehmer erkennbar sein. Ähnliches gilt für die Nachweisbarkeit der *Integrität* der Ergebnisse. Ein Teilnehmer kann das Ergebnis anzweifeln, was zu einer Nachzählung führt. Die *Authentifikation* basiert wie im vorherigen Szenario auf der sozialen Interaktion der Teilnehmer. Das *Ergebnis* wird in Form eines Protokolls während der Sitzung festgehalten [La03, Un06].

3 E-Voting über Instant-Messaging

In diesem Kapitel soll nun erläutert werden, wie die Szenarien mit Hilfe eines erweiterten IM-Systems realisiert werden können. Die grundsätzlichen Abläufe und geforderten Sicherheitsziele sollen gleich zu den Vorort-Varianten bleiben. Jedoch werden die einzelnen Schritte der Abläufe durch technische Mechanismen ergänzt oder ersetzt.

3.1 Phase 0 – Vorbereitung

Jeder Teilnehmer installiert den gewählten IM-Client, registriert sich mit einer Kennung beim Server und kann jederzeit mit anderen Teilnehmern kommunizieren. Jeder dieser Clients verfügt über die üblichen Funktionen eines IM-Systems (Chat, Voice-over-IP, Video-IP). Abbildung 1 zeigt eine Architektur für ein entsprechendes System bestehend aus einem existierenden IM-System (helle Symbole), wie etwa Skype [Sk08] oder Spark [Ig08], erweitert um ein anwendungsspezifisches Add-On (dunkle Symbole). Dieses Add-on übernimmt sowohl Aufgaben der Authentifizierung als auch die e-Voting-Funktionen wie Erstellung und Verteilung von Stimmzetteln und die Durchführung und Auswertung der Wahl.

3.2 Phase 1 - Authentifikation

Die Authentifikation der Wahlberechtigten findet durch das Anlegen einer Kennung statt. Diese Identifikation wird über den Authentifikationsserver des IM-Systems abgewickelt. Hier ist jedoch zu beachten, dass aktuelle IM-Systeme die Zuordnung von echten Personen zu gewählten Kennungen nicht überprüfen und damit einen Angriffspunkt

anbieten. Jeder darf eine Kennung anlegen und den entsprechenden Namen frei wählen (soweit dieser noch nicht vergeben ist). Es ist somit möglich, dass sich ein Andreas Maier eine Kennung mit Namen „Peter Müller“ erstellt. Um die registrierten Teilnehmer auszuwählen, gibt es zwei Wege: Die erste Möglichkeit ist die Verwendung der Suchfunktion des IM-Systems, zum Beispiel durch Eingabe des Namens oder Wohnortes des gesuchten Benutzers. Diese Vorgehensweise ist jedoch problematisch, da die Suchergebnisse aufgrund des oben genannten Sachverhalts nicht eindeutig sind. So könnte ein Angreifer absichtlich ein passendes, gefälschtes Profil anlegt, um selbst „gefunden“ zu werden. Eine zweite Möglichkeit ist die Weitergabe der genauen Benutzerkennung über ein anderes Medium (persönliche Mitteilung, E-Mail, Telefon, Visitenkarte, Briefkopf).

In beiden Fällen kann die Authentizität des Nutzers nicht ohne weiteres garantiert werden. Ein Mechanismus, um dies gewährleisten zu können, ist es die persönliche „Wiedererkennung“ von bekannten Personen über dem Videokanal (siehe Abschnitt 3.5.) ähnlich wie in einem Treffen vor Ort (Kapitel 2).

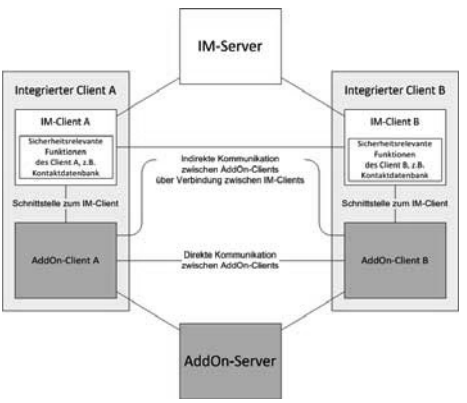

Abbildung 1: Architektur eines erweiterten IM-Systems mit AddOn

3.3 Phase 2 - Diskussion

Nachdem alle Teilnehmer in eine Konferenz eingeladen sind, kann eine Diskussion beginnen. Wichtige Anforderungen für diesen Teil der Kommunikation ist die Vertraulichkeit der Diskussion (Schutz gegen Abhören oder Manipulation der Diskussion) sowie die Möglichkeit der Protokollierung eines Diskussionsabschnittes, so dass beispielsweise zu einem späteren Zeitpunkt die Erstellung des Stimmzettels nachverfolgt werden kann („aber ich hatte doch auch Herrn Müller vorgeschlagen“).

3.4 Phase 3 – Wahl

Einige Mitglieder (z.B. der Vorsitzende) sind berechtigt, den Stimmzettel zu erstellen und die Abstimmung zu starten. Jeder Wahlberechtigte kann über sein IMAdd-On den

Wahlzettel anzeigen und seine Stimme abgeben. Der Koordinator wird mit Hilfe des Systems und je nach Szenario die Stimmen auszählen und das Ergebnis verkünden. Bei Nutzung eines IM-Systems als Grundlage und Kommunikationsmedium ist die Gefahr der Manipulation der Ergebnisse gegeben. So könnte beispielsweise der Koordinator den Auswertungsmechanismus manipulieren. Ebenso ist bei elektronischer „Verkündung" der Ergebnisse, etwa durch ein Posting auf einer Webseite, eine Manipulation denkbar.

3.5 Implementierung durch IM-System und Add-On

Für eine Realisierung einer sicherheitskritischen Anwendung mit Hilfe eines IM-Systems gibt es prinzipiell zwei Möglichkeiten:

Variante „Unified Security / Sicherheit im IM-Client" – Für die integrierte Anwendung (d.h. den IM-Client mit Erweiterungen) kann man fordern, dass (a) die Registrierungs- und Authentifikationsmechanismen eines geeigneten IM-Clients verwenden müssen und (b) Erweiterungsfunktionalitäten (elektronischen Abstimmung sowie die Integration mit den Funktionen des IM-Systems z.B. Wahlzettel an Benutzer mit der Kennung <x> senden) nur über den eventuell existierenden sicheren Kommunikationskanal zwischen den IM-Clients kommunizieren darf.

Variante „Vertraue Niemandem / Sicherheit im Add-On" – Das Add-On vertraut niemandem, nicht mal den Sicherheitsmechanismen des IM-Clients. In Bezug auf Signatur bedeutet das, dass Add-On A seine Nachrichten an Add-On B selber signiert.

Wir haben für den Ansatz, den wir zur Zeit entwickeln, eine Mischform gewählt. Als Grundlage sollen die eingebauten Mechanismen des IM-System zur Registrierung und Authentifikation verwendet werden, um Vorteile wie Nutzung des IM-System auch als übliche Kommunikationsmittel, keine Existenz einer mächtigen zentralen Instanz und die Beliebtheit solcher Systeme (also kein weiterer Account nötig) nutzen zu können. Allerdings beabsichtigen wir, eine der Schwächen der existierenden Systeme mittels der Erweiterung zu lösen, nämlich die fehlende gegenseitige Authentifizierung der Teilnehmer (Kapitel 3.1). Um dieses Problem zu beheben, führen wir zusätzlich zu den vorhandenen Sicherheitsfunktionen des IM-Systems einen weiteren Authentifikationsmechanismus ein. Unser Ansatz basiert auf einer Kombination aus (1) Wiedererkennung durch die anderen Beteiligten (z.B. in einem Videobild) und (2) einer Absicherung des dabei verwendeten Übertragungskanals mit Hilfe eines Diffie-Hellman-Verfahrens (DH). Dazu bauen die Teilnehmer eine Video-Konferenz untereinander auf. Dann berechnet jeder Client mit Hilfe des DH-Verfahrens einen gemeinsamen Schlüssel. Der jeweilige Teilnehmer liest den Hashwert dieses Schlüssels über die Videoübertragung vor [DVW92]. Durch Vergleich der Hashwerte kann die Integrität der Verbindung überprüft werden. Einen ähnlichen Ansatz verfolgt auch [Zi07]. Der Unterschied zum Ansatz von Zimmermann liegt darin, dass bei dem hier betrachteten Anwendungsfall Verfahren für mehr als zwei Teilnehmer notwendig sind, z.B. für die Generierung von gemeinsamen Schlüsseln. Weiterhin soll mit Hilfe eines Add-ons ein Wahlprotokoll für kleinen Gruppe ohne zentrale Instanz wie [BM86] oder [DLM82] realisiert werden, welches den im Kapitel 2 beschriebenen Szenarien entspricht.

4 Ausblick

In diesem Papier haben wir die mögliche Kombination von Instant-Messaging und sicherheitsrelevanten Anwendungen aufgezeigt. Als Beispiel haben wir Gruppenprozesse gewählt, die aus einer Diskussion mit anschließender (Gruppen-) Entscheidung bestehen. Diese können mit Hilfe einer Kombination von IM- und E-Voting-System realisiert werden. Die Vorteile solcher Systeme sind die spontane Nutzung und die leichte Handhabung ohne größeren Administrationsaufwand. Dadurch sind sie prädestiniert für ortsunabhängige Entscheidungsfindungen in Gruppen. Anderseits sind *je nach Fall* (Typ der Wahl, vorgeschriebene Abläufe) *unterschiedliche* Sicherheitsziele zu verfolgen und durch das technische System zu realisieren. Im entsprechenden Projekt wird an einer Referenzarchitektur gearbeitet, welche – abhängig von den Sicherheitszielen des jeweiligen Szenarios – geeignete Komponenten und Sicherheitsmechanismen anbietet, um die Sicherheitsanforderungen einer solchen komplexen Kommunikation erfüllen zu können. Die Herausforderungen dabei sind die Echtzeit dieser Applikationen, die Integration der unterschiedlichen Kommunikationskanäle in den E-Voting Prozess, die unterschiedlichen Kommunikationsabläufe bei den unterschiedlichen Typen von elektronischen Wahlen und das Fehlen einer einheitlichen Administration der Systeme, in welchen die Wahlberechtigten agieren.

Literaturverzeichnis

[BM86] Benaloh, J. C. Yung, M.: "Distributing the power of a government to enhance the privacy of voters," in Proceedings of the fifth annual ACM symposium on Principles of distributed computing, Calgary, Alberta, Canada, 1986, Seite 52 - 62

[DLM82] DeMillo, R. A.; Lynch, N. A., et al.: "Cryptographic Protocols," in Proceedings 14th ACM Symposium. on the Theory of Computing, 1982, Seite 383-400.

[DVW92] Diffie, W.; van Oorschot, P. C., et al.: "Authentication and Authenticated Key Exchanges - Designs, Codes and Cryptography 2." vol. 2: Kluwer Academic Publishers, 1992, Seite 107-125.

[Ig08] Igniterealtime: Spark - a jive software community, http://www.igniterealtime.org/, [Zugriff am 2008-03-28]

[La03] Land Rheinland-Pfalz: " 223-41 Hochschulgesetz (HochSchG) Rheinland-Pfalz" 2003, https://www.uni-koblenz.de/gesetze/dateien/rlp/hochschg_20030721.pdf, [Zugriff am 2008-03-22].

[Sk08] Skype Technologies S.A: Skype - take a deep breath, www.skype.com, [Zugriff am 2008-03-28]

[Un06] Universität Koblenz-Landau: "Grundordnung der Universität Koblenz-Landau," Universität Koblenz-Landau 2006, https://www.uni-koblenz.de/gesetze/dateien/uni/uni_grundo_20060323.pdf, [Zugriff am 2008-27-22].

[Zi07] Zimmermann, P.: "ZRTP: Media Path Key Agreement for Secure RTP," 2007, http://www.zfoneproject.com/docs/ietf/draft-zimmermann-avt-zrtp-04.pdf [Zugriff am 2008-05-15].