Schritt für Schritt zum Welt-weites Wählen – das Beispiel der IACR

Christopher Wolf

Horst Görtz Institut für IT-Sicherheit
Fakultät für Mathematik
Ruhr-Universität Bochum
chris@Christopher-Wolf.de oder
Christopher.Wolf@rub.de

Zusammenfassung: Der Welt-Kryptographenverband (IACR – International Association for Cryptologic Research) verwendet seit 2010 ein System für eine Online-Wahl. Die Erfahrungen sind durchweg positiv. Der Einführung ging eine intensive Diskussion innerhalb der Mitgliederschaft voran. Ziel war, möglichst alle Belange zu berücksichtigen und durch einen offenen Prozess von Anfang an Vertrauen in das neue System zu schaffen. Wichtiger Baustein hierzu war eine Demo-Wahl im Jahre 2009, in dem die Mitglieder das System ausprobieren konnten bevor es letztendlich Ende 2010 erstmalig eingesetzt wurde.

1 Einführung

Online-Wahlen können insbesondere für weltweit agierende Organisationen interessant sein: Im Gegensatz zur papier-basierten Variante können Zeit und Kosten gespart werden. In diesem Artikel zeigen wir die Erfahrungen der Welt-Kryptographen-Verbandes IACR (International Association for Cryptologic Research) bei der Umstellung von papierbasiertem zu elektronischem Wählen auf. Insbesondere wegen seiner Verfügbarkeit wurde als „Wahlgerät“ hierbei der heimische Browser gewählt.

Wichtig war bei diesem Prozess das schrittweise Vorgehen, um hierbei alle Interessierten der IACR mitzunehmen und doch zielgerichtet auf ein umsetzbares Verfahren zu zusteuern. Alles in allem gab es kleinere technische Probleme (insbesondere mit der Java-Unterstützung von bestimmten Browsern) – aber insgesamt deutlich weniger als evtl. zu erwarten gewesen wären. Aktuell gibt es innerhalb der IACR keine Stimmen, die zur papierbasierten Wahl zurück kehren wollen. Hierzu hat offensichtlich auch die stark gestiegene Wahlbeteiligung beigetragen (30% bzw. 40% statt wie bislang 20%), die die Legitimität der Wahl insgesamt stärkt.

2 Rechtlicher und Organisatorischer Rahmen

Die IACR hat über 1500 Mitglieder in über 60 Ländern dieser Erde (Stand: 2012). Hierbei sind „Mitglieder“ ausschließlich natürliche Personen. Firmen und Universitäten

mit Forschung im Bereich Kryptologie sind nur „indirekt“ über ihre jeweiligen Mitarbeiter Mitglied. Wichtigste Organe lt. Satzung [Satz] sind der Vorstand (s.u.), 3 Mitgliederversammlungen (eine für jede geographische Region) sowie die Gesamtschaft aller Mitglieder.

Im folgenden geben wir alle Mitglieder an, die durch allgemeine Wahl bestimmt werden. Die übrigen Mitglieder des Vorstands werden auf anderem Wege gewählt und sind für uns an dieser Stelle nicht weiter von Belang.

Der amtierende Vorstand spiegelt gut wieder, wie regional divers die IACR aufgestellt ist. Angegeben sind die/der aktuelle Amtsinhaber/in[1] sowie das Land des aktuellen Wohnsitzes (Quelle: [BoD]).

- Präsident: Bart Preneel (Belgien)
- Vice-Präsident: Christian Cachin (Schweiz)
- Schatzmeister: Greg Rose (USA)
- Schriftführer: Martijn Stam (UK)

Direktoren: Michel Abdalla (Frankreich), Josh Benaloh (USA), Thomas Berson (USA), Shai Halevi (USA), Anna Lysyanskaya (USA), Mitsuru Matsui (Japan), Christof Paar (Deutschland), David Pointcheval (Frankreich), Nigel Smart (UK)

Seit der Gründung im Jahre 1983 hat der Verband damit das Problem, den Vorstand breit legitimiert zu wählen. Damals wurde die Entscheidung getroffen, dies in direkter Wahl aller Mitglieder zu tun. Auf Grund ihrer weltweiten Verstreutheit sowie dem Mangel an einem gemeinsamen, sicheren Kommunikationsmittel blieb damit nur die Briefwahl übrig. Hieran orientiert sich auch die Satzung der IACR:

1. Bis zum 31.5. eines jeden Jahres werden 3 oder mehr Vorstandsmitglieder zur Kandidatenfindungs- und Wahlkommission gewählt
2. Ab dem 15.6. eines jeden Jahres können Kandidaten vorgeschlagen werden
3. Vor dem 1.10. eines jeden Jahres müssen die Wahlunterlagen an alle Mitglieder versandt werden.
4. Bis zum 15.11. müssen die Wahlbriefe beim „Returning Officer“ eingehen. In der Vergangenheit hat der Wahlvorstand die Frist häufiger ausgedehnt (z.B. bis zum 30.11.), um möglichst viele Stimmen berücksichtigen zu können. Zusammen mit zwei weiteren Personen findet dort die Auszählung statt. Bei Stimmengleichheit entscheidet der aktuell amtierende Vorstand
5. Direkt nach der Auszählung wird das Ergebnis allen Mitgliedern zugänglich gemacht.

Die Satzung der IACR legt des Weiteren seit 2008 fest, dass die Wahl entweder per Brief oder elektronisch durchgeführt werden darf. Jede „größere“ Änderung des Wahlmodus muss jedoch vorab von allen Mitgliedern genehmigt werden [Satz, VI, Abschnitt

[1] Im folgenden verwenden wir im Artikel aus Gründen der Lesbarkeit nur noch die männliche Form, meinen damit jedoch explizit auch die weibliche Form.

2]. Entsprechend war auch die Einführung der vollelektronischen Wahl durch eine Urwahl genehmigt worden, siehe hierzu Abschnitt 4.3.

3 Prozess zur Einführung der elektronischen Wahl

Die Einführung einer elektronischen Wahl war für die IACR eine delikate Angelegenheit: Als Fachgesellschaft für Kryptologie würde sie viel Ansehen verlieren, wenn ein von ihr verwendetes Online-Wahlsystem gehackt würde. Des Weiteren gibt es einige Vorschläge für solche Systeme von IACR-Mitgliedern. Die Auswahl eines solchen Systems könnte daher von Dritten als Einladung verstanden werden, das selbe System zu verwenden. Alles in allem verwendete die IACR seit 2007 einen mehrstufigen Prozess, bevor es 2010 zur ersten Online-Wahl in der Geschichte der Gesellschaft kam. Dieser Prozess ist öffentlich dokumentiert, siehe [eVot]. Er verlief grob in folgenden Schritten:

1. Vorbereitung & öffentliche Ausschreibung (April 2007 – April 2008)
2. Erste Präsentationsrunde (August 2008)
3. Findung von Evaluationskriterien (August 2009 – April 2009)
4. Zweite Ausschreibung & Präsentation (August 2009)
5. Demo-Wahl (September 2009)
6. Erste vollenektronische Wahl der IACR (September 2010)

Wir beschreiben im Folgenden die verschiedenen Stufen.

3.1 Vorbereitung bis Erste Präsentation

Bis zu diesem Zeitpunkt verwendete die IACR ein reines Briefwahlsystem. Dies war zum einen teuer (mehrere tausend US-Dollar / Jahr). Zum anderen hatte der sog. *„Returning Officer“* sehr starke Möglichkeiten, das Wahlergebnis zu manipulieren: Auf Grund der eher geringen Wahlbereiligung von ca. 20% war es ein leichtes, präparierte Umschläge einzubringen und damit jedes gewünschte Wahlergebnis zu erreichen. Um dies einordnen zu können: In der Geschichte der IACR gab es nie einen Fall, in dem es zu einer solchen Manipulation gekommen wäre (oder einer Anschuldigung einer solchen). Aber allein die Möglichkeit wurde als so schwerwiegend eingestuft, dass nach einem neuen Wahlsystem gesucht wurde. Ziel war damit also insbesondere, ein Wahlsystem zu finden, dass besser als der Status-Quo war. Daher wurde mit einer Satzungsänderung Ende 2008 die Möglichkeit geschaffen, eine elektronische Wahl einzuführen. Da das Thema für die IACR sehr delikat war (siehe oben), wurde hier explizit eine Beteiligung der gesamten Mitgliederschaft vorgeschrieben [Satz, VI, Abschnitt 2]. Auf Grund der möglichen Manipulationsmöglichkeiten wurde ein Ersatzsystem, nicht ein Zusatzsystem zur Briefwahl angestrebt. Des Weiteren bestand die Befürchtung, dass zwei parallele Systeme dazu führen konnten, dass die Menge der Wähler in einem der beiden Systeme so klein wird, dass das Wahlgeheimnis in dieser Gruppe gefährdet wäre. Auch dies sprach dafür, die Briefwahl völlig durch ein vollelektronisches System zu ersetzen.

Um einen möglichst breiten Überblick über mögliche Alternativsysteme zu erhalten wurde eine offene Ausschreibung durchgeführt. „Offen“ bedeutet an dieser Stelle, dass praktisch keine Einschränkungen für das vorzustellende System gemacht wurden und neben alle Mitgliedern auch alle übrigen Personen eingeladen wurden sich zu beteiligen. So wurde der entsprechende Call u.a. auf der Seite der IACR veröffentlicht [eVot]. Da sich in der Mitgliederschaft der IACR eine Reihe von namhaften Forschern befindet, die sich mit elektronischen Wahlsystemen beschäftigen, wurde mit einer entsprechenden Beteiligung gerechnet. Dies war auch der Fall: Auf der Crypto 2008 in Santa Barbara (USA) wurden insgesamt 8 Systeme vorgestellt [Prä08].

Die vorgestellten Systeme und Vorschläge waren sehr unterschiedlich; es sprengt daher den Rahmen dieses Artikels, sie alle vorzustellen. Insbesondere waren sie in einem sehr unterschiedlichen Zustand der Nutzbarkeit: Von Ideenskizzen über teilweise implementierte Protokolle bis hin zu Systemen inkl. Nutzer-Interface war alles vertreten. Es war daher schwer, auf Grund dieser Präsentationen eine sinnvolle Auswahl zu treffen.

3.2 Die Evaluierungskriterien

Die Evaluierungskriterien [Eval] wurden von insgesamt 10 Personen erarbeitet; 6 davon waren vom Vorstand hiermit beauftragt worden – die übrigen 4 arbeiteten zu. Teilweise hatten sie in der ersten Präsentationsrunde Beiträge geliefert. Anbei eine deutsche Übertragung der Kernpunkte von [Eval], teilweise leicht gekürzt. Die Organisation und Reihenfolge der Kriterien folgt dem Orginaldokument. Im Anschluss kommentieren wir diese Kriterien.

A.) Nutzer-Perspektive

1. Existierendes System & Open-Source
2. Nutzerfreundlichkeit für den Durchschnittsnutzer
3. Einfacher Betrieb für Freiwillige

B.) Sicherheit und Verfügbarkeit

4. Jeder Wähler kann exakt einmal wählen
5. Eine einzelne Stimme muss geheim bleiben; insbesondere darf sie nicht zum jeweiligen Wähler zurück verfolgt werden können
6. Es muss möglich sein, das Gesamtergebnis zu verifizieren. Jeder Wähler kann feststellen, dass seine Stimme gezählt wurde und nur gültige Stimmen in das Endergebnis mit ein gingen
7. Das System muss verfügbar & zuverlässig sein; ggf. kann es auf einen anderen Server verschoben werden

C.) Weitere Überlegungen

8. Denial-of-Service-Angriffe sollten nach Möglichkeit ausgeschlossen bzw. einfach behebbar sein. Kein IACR-Mitglied sollte an einen bestimmten Rechner für seine Stimmabgabe gebunden sein
9. Sicherheit gegen Viren und Trojaner

10. Möglichst sparsame Annahmen über die Sicherheit von Einzelkomponenten des Systems – z.B. keinen zentralen Vertrauensanker, von dem die Gesamtsicherheit des Ergebnisses abhängt. Z.B. durch die Verwendung eines Secret-Sharing-Schemas
11. Möglichkeit, „Dummy-Wahlzettel“ einzubringen
12. Unabhängigkeit der Stimmen für verschiedene Wahlen, die zur gleichen Zeit statt finden (z.B. Präsident und Direktoren)

D.) Explit augeschlossene Kriterien

13. Verhinderung von Stimmenkauf / -verkauf: Dies ist durch Kriterium C.11 hinreichend berücksichtig

14. Vollständige Verfügbarkeit des Wahlsystems: Notfalls kann die Wahlperiode verlängert werden (Kriterium B.7)

15. Verifizierbarkeit auf Papier

3.3 Kommentare zu den Kriterien

Wenngleich die Kriterien sicher interessant sind und für sich selbst stehen können ist es vermutlich jedoch sinnvoll, sie teilweise in den Kontext der IACR einzubetten. Hierzu muss man zunächst wissen, dass die IACR über keinerlei hauptamtliche Kräfte verfügt; Kriterium A.3 (Betrieb durch Freiwillige) war daher eine schlichte Notwendigkeit. Analog ist A.1 aus der Geschichte zu verstehen: Eine Reihe der auf der ersten Präsentation (siehe Abschnitt 3.1) vorgestellten Systeme war sicher interessant – aber leider (noch) nicht existent. Diese mussten in den Evaluationskriterien daher explizit ausgeschlossen werden. Insbesondere sah die IACR sich außerstande, mit eigenen Ressourcen ein solches System zu programmieren, zu verifizieren und zu testen.

Kriterium B.6 (Verifizierbarkeit der Wahl) geht sicher über die Möglichkeiten einer Briefwahl hinaus. Auf der anderen Seite hat eine Wahl ja zwei Ziele – nämlich eine Auswahl unter möglichen Kandidaten zu treffen und das Ergebnis dieser Auswahl auf eine allgemein anerkannte Basis zu stellen (=Legitimität). Die Anforderungen von B.6 sind sicherlich sehr streng. Aufgrund der ersten Präsentationsrunde war jedoch klar, dass es in der Praxis Systeme gab, die dieses Kriterium auch erreichen konnten.

Kriterium C.11 wirkt sehr technisch. Praktisch verhindert es aber schön, dass ein Wähler zu einer bestimmten Wahl gezwungen werden kann: Im Falle eines Falles kann er seine Stimmabgabe einfach wiederholen. Es hängt hier jedoch stark von der Ausgestaltung und dem Angreifermodell ab, ob C.11 trägt: Wenn wir annehmen, dass ein Wähler seine Wahl-Credentials direkt an den Angreifer abliefert geht C.11 ins Leere (siehe z.B. D.13). Unter der Annahme, dass der Angreifer den ausgefüllten Wahlzettel nicht direkt, sondern nur „geblindet“ sieht, funktioniert dies.

Interessant sind auch die *„Explizit ausgeschlossenen Kriterien“* (Abschnitt 3.2.D). Man hätte diesen Abschnitt auch mit *„Grenzen des Wahlsystems“* bezeichnen können:

Wenngleich alle diese Kriterien sicherlich sinnvoll sind – so sind sie für eine vergleichsweise kleine Organisation wie die IACR sicherlich übertrieben. Auf der anderen Seite bedeutet dies, dass das von der IACR verwendete Wahlsystem sich vermutlich nicht für eine öffentliche Wahl eigenen wird. Dies wurde seitens der IACR nochmals durch zwei gleichlautende Beschlüsse auf den Mitgliederversammlungen in Europa (Eurocrypt 2010) und den USA (Crypto 2010) festgestellt [eVot]; zu diesem Zeitpunkt war bereits bekannt, dass die IACR Helios verwenden würde (siehe hierzu Abschnitt 3.4). Ihr Wortlaut (Englisch):

> The IACR adopts the Helios remote e-voting system for future IACR elections (including 2010). At the same time, the IACR clearly publishes a statement that its use of this system does not constitute an endorsement of this or other remote-voting systems for public-sector elections.

Dieses Statement wurde in die offizielle eVoting-Seite der IACR aufgenommen.

3.4 Zweite Ausschreibung bis Demo-Wahl und Entscheidung

Aufgrund der Evaluationskriterien aus Abschnitt 3.2 wurde eine zweite Ausschreibung durchgeführt. Hierzu meldeten sich nur noch 2 Kandidaten – nämlich Vertreter der Systeme Helios sowie Punchscan. Beide erfüllten nach Ansicht der IACR-Vorstandes alle Kriterien und wurden zu einer Präsentation auf der Vorstandssitzung im August 2009 eingeladen. Um letztendlich beurteilen zu können, ob beide Systeme die Kriterien auch in der Praxis erfüllten, wurde eine „Demo-Wahl“ durchgeführt. Beide Systeme wurden hierzu eingeladen; letztendlich sah sich jedoch nur das Helios-Team dazu in der Lage, eine solche Demo-Wahl zu organisieren. Seitens Punchscan liegen leider keine Gründe vor, warum diese nicht an der Demo-Wahl teilnahmen.

Diese Wahl fand im September 2009 statt (vgl. Abschnitt 4.3). Da die Demo-Wahl letztendlich zeigte, dass alle im Abschnitt 3.2 genannten Kriterien erfüllt waren und sich die Wahl mit akzeptablen Aufwand durch den Wahlausschuss durchführen ließ, wurde Helios ab 2010 für die jährlich statt findenden Wahlen der IACR verwendet.

3.5 Kommentare zur Einführung

Der Prozess der IACR war alles in allem sowohl sehr gründlich wie auch sehr offen: Alle Teams hatten die Chance, ein System zu erstellen, das den Kriterien aus Abschnitt 3.2 genügt. Alle Teams hatten die Chance, eine Demo-Wahl zu organisieren. Dass sich letztendlich nur ein Team hierzu in der Lage sah, zeigt wie groß der Unterschied zwischen einem theoretisch umsetzbaren System und einem praktisch einsetzbaren System tatsächlich ist.

Ein Frage, die sich ein Außenstehender vielleicht stellen mag ist die vergleichsweise lange Zeitspanne (über 3½ Jahre), die zwischen den ersten Ideen für eine Online-Wahl und der tatsächlichen Umsetzung liegt. Auf der anderen Seite muss man hier im Hinterkopf behalten, dass die Briefwahl seit 1983 ja zufriedenstellend funktionierte; es

gab weder aus organisatorischer noch aus finanzieller Sicht die Notwendigkeit, schnell auf eine Online-Wahl umzusteigen. Zum zweiten wird die IACR von Freiwilligen getragen, die sich i.d.R. nur zweimal im Jahr treffen – einmal bei der Eurocrypt- und einmal bei der Crypto-Konferenz (jeweils im April/Mai und August eines Jahres). Dies hat im vorliegenden Prozess auch klar die Taktung vorgegeben: Auf Sitzung X wurde ein Auftrag erteilt. Dieser wurde bis Sitzung X+1 erledigt. Es wurde aufgrund der neuen Fakten entschieden etc. Dies ist jedoch mehr ein organisatorisches als ein technisches Problem. In anderen Organisationen oder bei gegebener Notwendigkeit hätte dies ggf. schneller realisiert werden können.

Alles in allem verlief die Einführung der Online-Wahl problemfrei. Das Verfahren war mehrfach von allen hieran Interessierten diskutiert worden, die Entscheidungskriterien und alle entsprechenden Dokumente sind öffentlich. Dies führte letztendlich zu einer großen Akzeptanz der Entscheidung. Es gab einzelne Kritik an technischen Bausteinen, wie z.B. der Wahl von Java als Implementierungssprache für die „Wahl-Kabine“ (siehe Abschnitt 4.3)

4 Die eigentliche Wahl

In diesem Abschnitt beschreiben wir die wesentlichen Funktionen des Helios-Systems aus Sicht des Wahlvorstands und eines einzelnen Wählers. Die Sicht eines Administrators bleibt hierbei außen vor. Zum Thema Usability verweisen wir insbesondere auf [WH09].

4.1 Helios

Das Helios-Wahlsystem liegt derzeit in Version 3 vor. Es ist Open-Source unter GLP v3. Alle Sourcen finden sich sich auf github [Hgit]. Entsprechend der technischen Spezifikation ist die Struktur von Helios ist wie folgt [Hv3d]:

1. Wahl-Server
2. Wahl-Kabine („booth“)
3. Verifikatoren

Der Wahl-Server teilt sich dabei in ein Web-Tool zum Erstellen einer neuen Wahl und einer „elektronischen Pinwand“ oder „gläsernen Wahlurne“, um alle bisher abgegebenen (verschlüsselten!) Stimmzettel zu sehen. Damit kann sich jeder Wähler davon überzeugen, dass seine Stimme auch vom Server angenommen wurde. Der Wahl-Server macht es für die Wahlkommission vergleichsweise einfach, eine eigene Wahl durchführen. Zur Zeit der Demo-Wahl 2009 war das einzige User-Interface der Internet-Browser des jeweiligen Nutzers; inzwischen gibt es auch ein Interface via Smartphone.

Helios kann dabei in zwei Modi verwendet werden: Direkt von den Sourcen. In diesem Fall installiert man Helios auf einem beliebigen Server. Oder analog zum Easychair Reviewing System, das physikalisch auf dem Server eines Third-Party-Providers läuft

und jeweils Instanzen für jede Konferenz (bei Helios: Wahl) erzeugt. Die IACR verwendet letzteres, da es administrativ einfacher ist und durch entsprechende kryptographische Protokolle ausgeschlossen ist, dass der Betreiber des entsprechenden Systems das Wahlergebnis beeinflussen kann. Außerdem trennt es (administrativ) den Systembetreiber von der Wahlkommission; letzteres ist zumindest psychologisch relevant.

Die Wahl-Kabine befindet sich im Internet-Browser des jeweiligen Benutzers; alle Daten werden dort verschlüsselt. Der Nutzer hat die Chance, seine Stimme entweder abzugeben oder zu verifizieren (s.u.). Um die Stimme abzugeben benötigt der Nutzer ein Login und ein Passwort, das ihm auf beliebigem Wege zugestellt werden kann. Per se kann die Wahl-Kabine durch eine andere Software ersetzt werden, da die Spezifikationen von Helios öffentlich sind. Der Wahl-Server kommuniziert dabei mit jeder Software, die die Spezifikation erfüllt. Aktuell gibt es auch eine Implementierung von Helios auf Smartphones.

Statt eine Stimme abzugeben kann ein Wähler auch verifizieren, ob sie korrekt ist. Hierzu werden Verifikatoren von verschiedenen Autoren angeboten. Damit kann jeder Wähler sich den Autor (oder die Autoren) heraus suchen, denen er am meisten vertraut. Dies dient insbesondere dem Schutz vor Malware, die ggf. die elektronische Wahl-Kabine korrumpiert haben könnte. Da die Malware nicht weiß, wann der Nutzer seine Stimme verifizieren wird, besteht bei einer Wahl eine vergleichsweise große Chance, dass mindestens ein Nutzer die Veränderung seines Stimmzettels bemerkt; der Stimmzettel kann auch exportiert und dann auf einem anderen Gerät (z.B. Smartphone) verifiziert werden. Die Trennung in Stimmen in solche, die verifiziert worden sind und solcher, die auch ins Endergebnis mit eingehen erschwert den Stimmenkauf. Dies ist natürlich nicht perfekt. Insbesondere kann sich ein Angreifer die Wahl-Credentials (Login & Passwort) verschaffen und damit sicher eine bestimmte Stimme abgeben.

In einem letzten Schritt werden alle Stimmzettel und Audit-Trails der Wahl auf dem Wahl-Server veröffentlicht, so dass jeder Wähler das Ergebnis der Wahl nachvollziehen kann. Auch hierfür gibt es (quelloffene) Software. Da diese dezentral ausgelegt ist kann leider nicht angegeben werden, wie viele Nutzer davon praktisch Gebrauch machen; allerdings reicht theoretisch ein einziger Nuzter aus, der hier einen Fehler findet, um die Legitimität der Wahl in Frage zu stellen. Wie bereits für die Stimmabgabe ist das entsprechende Nutzerinterface rein web-basiert.

Rein technisch verwendet Helios homomorphe Verschlüsselung, d.h. es wird die Tatsache ausgenutzt, dass für mache Verschlüsselungssysteme gilt

$$E(a) * E(b) = E(a+b).$$

Es können also Stimmzettel zusammen gezählt werden ohne die einzelnen Stimmzettel entschlüsseln zu müssen. Erst das Endergebnis wird entschlüsselt und veröffentlicht. Die exakten technischen Details finden sich in [Hv3d]. Für Version 4 soll dieses System beibehalten werden, für Version 5 könnten evlt. (auch) Mix-Netze unterstützt werden. Dies ist derzeit noch nicht völlig klar.

Die vollständige Darstellung von Helios würde diesen Artikel sprengen. Wir verweisen insbesondere für Fragen der Sicherheit daher auf [Aid08, CK12]]

Eine ausführliche Analyse von Helios aus Nutzersicht findet sich unter [HW09].

4.2 Instanzierung durch die IACR

Seitens der IACR bestand ein starkes Interesse, dass kein Mitglied der Wahlkommission allein das Ergebnis beeinflussen kann bzw. dass allein der Anschein entsteht, dass dies möglich wäre. Daher ist der Schlüssel der Wahl zwischen allen Mitgliedern der Wahlkommission geteilt (secret sharing scheme). Nur gemeinsam können sie das Ergebnis berechnen. Dies ist kryptographisch bewiesen und aus Sicht der IACR daher zielführend.

Die Logins sind anonymisiert, konkret wurden „V1, V2, …, V1600“ verwendet. Damit ist es nicht möglich festzustellen, wer gewählt hat. Nur, wie viele Mitglieder insgesamt an der Wahl teilgenommen haben. Innerhalb der Mitgliederschaft der IACR war diese Entscheidung umstritten. Konkret handelte es sich um eine kulturelle Differenz zwischen Ländern (insbesondere in Europa), in denen die Wählerlisten für andere Wahlen nicht nach der Wahl veröffentlicht werden und Ländern (z.B. die USA), in denen dies der Fall ist. Das Hauptargument ist die bessere Nachvollziehbarkeit der Wahl; so würde es bemerkt werden, wenn ganze Friedhöfe geschlossen zur Wahl antreten, wie dies z.B. bei einigen (Kommunal-)Wahlen in der Vergangenheit der Fall gewesen war. Letztendlich entschied sich die IACR dafür, der Anonymität ihrer Mitglieder mehr Gewicht zu geben als der Auditierbarkeit der Wahl.

Ebenfalls bewusst in Kauf genommen wird die Tatsache, dass Login & Passwort per eMail an alle Mitglieder versandt wurden. Zum einen gab es bei der Briefwahl immer wieder Beschwerden von Mitgliedern, denen innerhalb der 6 Wochen keine Unterlagen zugekommen waren. Zum zweiten sollte ein Medienbruch vermieden werden. Und zum dritten wurde argumentiert, dass kein Angreifer so große Teile des Internets in seine Gewalt bringen könnte, dass er die Wahl damit effektiv beeinflussen würde. Abschließend würde so ein Angriff von mindestens einem Mitglied bemerkt werden – nämlich dann, wenn seine Stimme ersetzt wurde bzw. bereits eine Stimme abgegeben wurde, obwohl er noch gar nicht gewählt hatte.

4.3 Demo-Wahl Ende 2009

Wenngleich es sich bei der Demo-Wahl Ende 2009 nicht um eine richtige Wahl handelte, war es der erste Testlauf des Systems innerhalb der IACR. Insbesondere wurde in dieser Online-Wahl die Frage geklärt, ob die IACR in Zukunft auf Online-Wahlen umstellen soll. Insgesamt wurden 379 Stimmen abgegeben. Bei 1542 Teilnahmeberechtigten entspricht dies einer Beteiligungsquote von 24,6%. Die wichtigsten Ergebnisse im Einzelnen [eVot]:

- Soll die IACR statt des bisherigen Briefwahl-Systems eine Online-Wahl durchführen?
    - Online-Wahl: 344 (91,5%)
    - Briefwahl: 32 (8,5%)

- Soll die IACR für eine evtl. Online-Wahl das Helios-System nutzen?
    - Ja: 293 (88,3%)
    - Nein: 39 (11,7%)

Zum Vergleich: An den (Brief-)Wahlen im selben Jahr nahmen 325 Mitglieder teil, ein Jahr zuvor waren es 312 Mitglieder gewesen [VotAll]; die Mitgliederzahl in beiden Jahren war vergleichbar.

Alles in allem wurden damit sowohl die Online-Wahl wie auch das Helios-System mit großer Mehrheit angenommen.

Die Demo-Wahl selbst verlief ziemlich reibungslos – so berichtet es zumindest offizielle der offizielle IACR Bericht über die Demo-Wahl [HSH10]. Es gab lediglich grundsätzliche Erwägungen zur Online-Wahl, Probleme mit der Java-Version des jeweils verwendeten Browsers sowie der Unterstützung aller Plattformen. Dies betraf aber nur einen kleinen Teil der Mitglieder; er ist im obigen Bericht leider nicht quantifiziert. Es werden allerdings von zwei Nutzern dezidierte (anonymisierte) Kommentate zur Java-Problematik veröffentlicht. Ärgerlicher war aus Sicht der Wahlkommission allerdings, dass das Web-Interface für die Wahl-Administration nicht fehlerfrei lief. Alles in allem waren es nach Ansicht der Wahlkommission kleinere technische Fehler, die alle bis zur ersten „richtigen“ IACR-Wahl gelöst werden konnten.

Briefwahl			**Legende**	**Online-Wahl**		
2006[¶]	2008	2009	**Jahr**	2010	2011	2012
324	312	325	**Wähler**	475	612	518
nicht verfügbar		1542	**Berechtigte**	1555	1484	1530
		21,1%	**Beteiligung**	30,5%	41,2%	33,9%

Tabelle 1: Wahlbeteiligung an der IACR-Wahl im Falle der Online- und der Briefwahl. Die Jahre der Briefwahl sind seitens der IACR leider nicht völlständig dokumentiert.

[¶] Die Zahlen von 2007 sind auf der IACR-Seite nicht verfügbar.

4.3 Weitere Wahlen seit 2010

Entsprechend dem Mitglieder-Votum (siehe vorheriger Abschnitt) führt die IACR seit 2010 alle ihre Wahlen mittels Helios durch. In dieser Zeit entwuchs Helios den Kinderschuhen und bietet z.B. sehr viel mehr Unterstützung für verschiedene Browser und Systeme, wodurch auch die oben beschriebenen Probleme weniger wurden bzw. ganz entfielen. Inzwischen ist Helios innerhalb der IACR als Wahlsystem etabliert. Hierzu trug vermutlich auch der sehr offene Umgang von Helios mit evtl. Sicherheitslücken bei, siehe hierzu insbesondere [Had]. Interessanter Weise stieg die Wahlbeteiligung signifikant, siehe hierzu Tabelle 1 (Zahlen von [VotAll]).

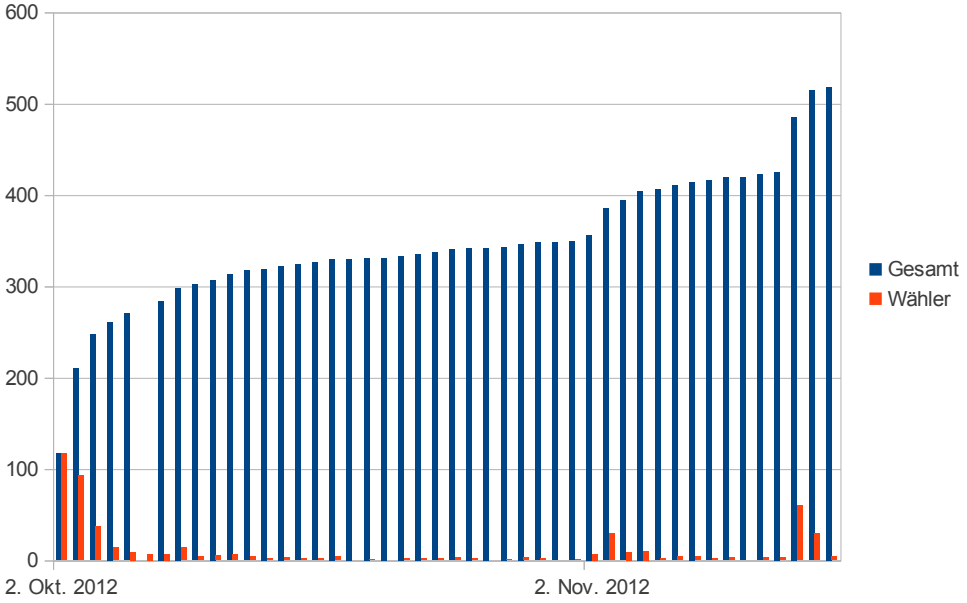

Abbildung 2: Anzahl Wähler pro Tag. Rot („Wähler“) sind die Wähler des jeweiligen Tages, blau („Gesamt“) die Gesamtsumme bis dahin. Die exakten Zahlen befinden sich im Anhang.

Leider sind die Zahlen auf [VotAll] nicht vollständig – damit ist es schwer exakt zu quantifizieren, wie stark die Wahlbeteiligung durch die Einführung der Online-Wahl gestiegen ist. Alles in allem gab es aber wohl auf jeden Fall einen messbaren Anstieg, insbesondere, da die Mitgliederzahlen der IACR in den letzten Jahren ziemlich konstant waren. Das Jahr 2011 sticht mit einer Beteiligung von über 40% klar hervor. In diesem Jahr wurden schlicht mehr Erinnerungsmails versandt als in den übrigen Jahren (4 statt der üblichen 2). Diese Entwicklung lässt sich ebenfalls gut an den Daten für 2012 ablesen, für die eine taggenaue Wahlbeteiligung vorliegt (Abbildung 2). Die Daten

wurden auf Grund der aktuellen Stimmlisten auf Helios generiert und jeweils um 23:07 (UTC) gemessen. Für den 1.10. und 7.10. liegen auf Grund eines technischen Defekts leider keine Daten vor.

Insbesondere am roten „Wähler"-Balken des jeweiligen Tages sieht man sehr schön den Effekt der beiden Erinnerungsmails vom 2. November sowie 13. November. Auf der anderen Seite brachte die lange Wahlperiode vermutlich nicht sehr viel – es gab einzelne Tage (z.B. den 11.11.), an dem kein einziges Mitglied gewählt hatte. Die Wahlperiode ist allerdings in der Satzung festgelegt und kann daher nicht so einfach verkürzt werden.

Als Faustformel kann man aber festhalten, dass die IACR durch die Einführung einer elektronischen Wahl eine ca. 10%-Punkte höhere Wahlbeteiligung bekommen hat. Mit verantwortlich dürfte sein, dass ein Klick immer noch einfacher ist als einen Brief zur Post zu bringen.

Fazit

Die IACR verwendet seit inzwischen 3 Jahres das System Helios für die Wahl seines Vorstandes. Nach anfänglichen, kleineren Kinderkrankheiten läuft das System inzwischen stabil. Der Einführung der Online-Wahl ging eine intensive Diskussion innerhalb des Verbandes voraus.

Hauptvorteil ist zum einen die einfachere Handhabung des Systems durch die Ehrenamtlichen, die die Wahl organisieren müssen. Vorher mussten sie sich darum kümmern, Wahlzettel aus Papier zu allen 1500 Mitgliedern zu senden und diese auch zu zählen. Dies war vergleichsweise zeitintensiv. Aktuell beschränkt sich der Aufwand auf den Export der Wählerliste (eMail-Adressen) aus der Mitgliederdatenbank sowie dem Entschlüsseln des Wahlergebnisses. Das System wird innerhalb der Mitgliederschaft akzeptiert. Interessanter Weise war es vergleichsweise einfach, die Wahlbeteiligung von vorher ca. 20% der Mitglieder auf über 40% anzuheben (2011). Ohne weitere Maßnahmen scheint die Wahlbeteiligung stabil über 30% zu bleiben (2010, 2012). Störend ist allein die lange Wahlperiode; eine Verkürzung auf z.B. 10 Tage wäre vermutlich sinnvoll. Aufgrund bestehender Regelungen in der Satzung ist dies allerdings nicht möglich.

Alles in allen ist die Erfahrung der IACR positiv. Es gibt weder Stimmen, auf die alte Briefwahl zurück zu greifen noch ein anderes Tool als Helios zu verwenden. Die größte dem Autor bekannte Wahl mit Helios ist die Präsidenten/Rektor-Wahl an der französischsprachigen Université catholique de Louvain (Belgien) mit ca. 30.000 Studierenden und 5000 Mitarbeitern. Aktuell berichtet Helios auf seiner Homepage, dass der (Teil-)AStA für Bachelor-Studierende in Princton (USA) Helios verwendet.

Helios ist sicherlich nicht die Lösung für alle Wahlprobleme dieser Welt. Zum einen versteckt es große Teile der Technik vor seinen Benutzern. Damit muss der Benutzer jeweils mindestens einem Endgerät (Wahl-Kabine oder Auditsoftware) trauen um sicher zu sein, dass seine Stimmabgabe auch wirklich (korrekt) erfolgt ist. Wurden beide

korrumpiert, ist die Sicherheit von Helios dahin. Bei größeren Wahlen (z.B. Bundestagswahl) gäbe es ein ausreichend großes Angriffsziel um die entsprechende Schadsoftware zu erstellen und in Umlauf zu bringen. Insbesondere in unsicheren Wahlkreisen kann schon ein kleiner Anteil gefälschter Wahlzettel das Ergebnis nachhaltig beeinflussen. Zum anderen ist die Nutzerauthentifizierung nicht sicher gelöst: Alle dem Autor bisher bekannten Verfahren Helios zu instanzieren setzen auf Login/Passwort-Paare, die zumindest theoretisch einfach abgefangen werden können. Letzteres um so mehr als wenn sie per eMail verschickt werden. Interessanter Weise scheint Helios hier keine Probleme zu sehen – so bewirbt es aktuell „Vowee“, bei dem man mittels Twitter-Account (!) eine Wahl aufsetzen und verwalten kann.

Auf der anderen Seite ist dies vielleicht eine Stärke von Helios: Menschen, die Technik einfach nur benutzen wollen können dies bei Helios einfach tun. Die Frage, ob das Verfahren sicher ist oder nicht müssen sie in diesem Fall allerdings an Spezialisten delegieren. Inwieweit dies für eine bestimmte Wahl ein Problem darstellt muss jede Organisation für sich selbst beantworten. Daher war es sehr sinnvoll, dass die IACR die Online-Wahl in kleinen, überschaubaren Schritten eingeführt hat und auf allen Ebenen versucht hat, die Mitgliederschaft „mitzunehmen“. Hilfreich war allerdings, dass die technischen Spezifikationen allen Mitgliedern zugänglich waren und (zumindest theoretisch) auch hätten verstanden werden können.

Literaturverzeichnis

[Aid08] Ben Adida: Helios: Web-based Open-Audit Voting, USENIX Security 2008, Seiten 335-348, USENIX.

[BoD] International Association of Cryptologic Research: Board of Directors (2013), http://www.iacr.org/bod.html.

[CK12] Véronique Cortier and Steve Kremer: D4.3 Results on a real life case study: Helios 2.0, 116 Seiten, abgerufen am 28.6.2013, http://www.lsv.ens-cachan.fr/Projects/anr-avote/RAPPORTS/deliv4-3.pdf

[Eval] Yvo Desmedt, Stuart Haber, Shai Halevi, James Hughes, Antoine Joux, and Jean-Jacques Quisquater, Josh Benaloh, Ron Rivest, David Wagner, and Moti Yung: E-Voting Systems for the IACR: Requirements and Evaluation Criteria, http://www.iacr.org/elections/eVoting/requirements.html, abgerufen am 9.5.2013.

[Had] Helios Voting System – Attacks and Defences, http://documentation.heliosvoting.org/attacks-and-defenses, abgerufen am 10.5.2013.

[HBH10] Stuart Haber Josh Benaloh Shai Halevi: The Helios e-Voting Demo for the IACR, http://www.iacr.org/elections/eVoting/heliosDemo.pdf, 7 Seiten, 24. Mai 2010.

[Hgit] Ben Adida et al.: Helios Voting System – Sourcen: https://github.com/benadida/helios-server, abgerufen am 10.5.2013

[Hv3d] Ben Adida et al.: Helios Voting System version 3 – technical documentation: http://documentation.heliosvoting.org/verification-specs/helios-v3-verification-specs, abgerufen am 10.5.2013.

[M12] Bart Preneel: Membership Meeting at Crypto 2012, http://www.iacr.org/docs/minutes/c2012mem-slides.pdf, abgerufen am 10.5.2013.

[eVot] International Association of Cryptologic Research: Should the IACR use e-voting for its elections?, https://www.iacr.org/elections/eVoting/, abgerufen am 2.5.2013.

[VotAll] International Association of Cryptologic Research: IACR Elections, http://www.iacr.org/elections/, abgerufen im Mai 2013.

[Prä08] International Association of Cryptologic Research: Board Meeting on E-Voting, Tuesday, August 19, 2008, Santa Babara, CA, USA, http://www.iacr.org/elections/eVoting/presentations.html, abgerufen am 9.5.2013.Urs Hengartner

[WH09] Janna-Lynn Weber and Urs Hengartner: Usability Study of the Open Audit Voting System Helios, elektronische Version: http://www.jannaweber.com/wp-content/uploads/2009/09/858Helios.pdf

[Satz] International Association of Cryptologic Research: Bylaws in der Version vom 22. Dezember 2008, http://www.iacr.org/docs/bylaws.html, abgerufen am 2.5.2013.

Anhang – Wahlbeteiligung in 2012 nach Tagen

Tue October 2, 2012	117 of 1530 (7.6%)		Fri October 26, 2012	342 of 1530 (22.4%)
Wed October 3, 2012	210 of 1530 (13.7%)		Sat October 27, 2012	342 of 1530 (22.4%)
Thu October 4, 2012	247 of 1530 (16.1%)		Sun October 28, 2012	343 of 1530 (22.4%)
Fri October 5, 2012	261 of 1530 (17.1%)		Mon October 29, 2012	346 of 1530 (22.6%)
Sat October 6, 2012	270 of 1530 (17.6%)		Tue October 30, 2012	348 of 1530 (22.7%)
Mon October 8, 2012	284 of 1530 (18.6%)		Wed October 31, 2012	348 of 1530 (22.7%)
Tue October 9, 2012	298 of 1530 (19.5%)		Thu November 1, 2012	349 of 1530 (22.8%)
Wed October 10, 2012	302 of 1530 (19.7%)		Fri November 2, 2012	356 of 1530 (23.3%)
Thu October 11, 2012	307 of 1530 (20.1%)		Sat November 3, 2012	385 of 1530 (25.2%)
Fri October 12, 2012	313 of 1530 (20.5%)		Sun November 4, 2012	394 of 1530 (25.8%)
Sat October 13, 2012	317 of 1530 (20.7%)		Mon November 5, 2012	404 of 1530 (26.4%)
Sun October 14, 2012	319 of 1530 (20.8%)		Tue November 6, 2012	406 of 1530 (26.5%)
Mon October 15, 2012	322 of 1530 (21.0%)		Wed November 7, 2012	410 of 1530 (26.8%)
Tue October 16, 2012	324 of 1530 (21.2%)		Thu November 8, 2012	414 of 1530 (27.1%)
Wed October 17, 2012	326 of 1530 (21.3%)		Fri November 9, 2012	416 of 1530 (27.2%)
Thu October 18, 2012	330 of 1530 (21.6%)		Sat November 10, 2012	419 of 1530 (27.4%)
Fri October 19, 2012	330 of 1530 (21.6%)		Sun November 11, 2012	419 of 1530 (27.4%)
Sat October 20, 2012	331 of 1530 (21.6%)		Mon November 12, 2012	422 of 1530 (27.6%)
Sun October 21, 2012	331 of 1530 (21.6%)		Tue November 13, 2012	425 of 1530 (27.8%)
Mon October 22, 2012	333 of 1530 (21.8%)		Wed November 14, 2012	485 of 1530 (31.7%)
Tue October 23, 2012	335 of 1530 (21.9%)		Thu November 15, 2012	514 of 1530 (33.6%)
Wed October 24, 2012	337 of 1530 (22.0%)		Fri November 16, 2012	518 of 1530 (33.9%)
Thu October 25, 2012	340 of 1530 (22.2%)			

Alle Werte wurden jeweils um 23:07 (UTC) eines jeden Tages auf Grund der Zahl der auf Helios registrierten Wahlzettel ermittelt. Auf Grund eines technischen Defekts begann die Messung erst am 2.10. Aus den selben Gründen sind für den 7.10. keine Zahlen verfügbar.