07311 Abstracts Collection
Frontiers of Electronic Voting
— Dagstuhl Seminar —

David Chaum[1], Miroslaw Kutyłowski[2], Ronald L. Rivest[3] and Peter Ryan[4]

[1] University of Leuven, BE
david@chaum.com
[2] TU Wroclaw, PL
mirekk@im.pwr.wroc.pl
[3] MIT - Cambridge, USA
rivest@theory.lcs.mit.edu
[4] University of Newcastle, GB
M.D.Ryan@cs.bham.ac.uk

Abstract. From July the 29th to August the 3th, 2007, the Dagstuhl Seminar 07311 "Frontiers of Electronic Voting" was held in the International Conference and Research Center (IBFI), Schloss Dagstuhl. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Voting machine, remote voting, verifiability, foundations of voting algorithms, attacks

07311 Executive Summary – Frontiers of Electronic Voting

This is a short report on Dagstuhl Seminar 07311 - Frontiers of Electronic Voting, 29.07.07 - 03.08.07, organized in The International Conference and Research Center for Computer Science (IBFI, Schloss Dagstuhl).

Keywords: voting machine, remote voting, verifiability, foundations of voting algorithms, attacks

Joint work of: David Chaum, Mirosław Kutyłowski, Ronald Rivest, Peter Y. A. Ryan

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2008/1294

Internet Voting in Estonia

Michael Alvarez (CalTech - Pasadena, USA)

A handful of countries have conducted Internet voting trials over the past decade, including France, the Netherlands, Switzerland, the United Kingdom, and the United States. All of these trials have been conducted at the local and regional levels of government, targeting specific populations of voters. The nation that has advanced the farthest with the deployment of Internet voting has been Estonia, a former Soviet republic on the Baltic Sea and now a full member of the European Union. Since 2000, Estonia has conducted two national elections in which all voters could use Internet voting. The first election, in October 2005, was for local offices and the second election, in March 2007, was for parliamentary elections at the national level. In this paper, we discuss the context for the Estonian experience in deploying Internet voting. We focus on the systematic way in which the Estonians have addressed the legal and technical considerations required to make Internet voting a functioning voting platform, as well as the political and cultural framework that promoted this innovation. Using data from our own qualitative and quantitative studies of the Estonian Internet voting process, we then consider who voted over the Internet in these elections, how Internet voting has been used in Estonian elections and the political implications of the voting platform. Finally, we consider the lessons that other countries can learn from the Estonian experience.

Keywords: Internet voting, remote voting, Estonia

Joint work of: Alvarez, R. Michael; Hall, Thad E.; Trechsel, Alexander H.

Using Incident Reports to Detect Election Anomalies and Irregularities

Michael Alvarez (CalTech - Pasadena, USA)

In this paper we discuss the use of a novel form of data to develop threat assessments for election administration and voting technology. In a primary election on May 2006, Cuyahoga County (Ohio, USA) asked poll workers to complete precinct incident report forms, and Cuyahoga County poll workers reported 6,285 incidents. The incident report forms were not elaborate. Other than asking for average and longest voter wait times, they were essentially blank pieces of paper on which poll workers wrote accounts of the problems they encountered. These verbatim reports were entered into an electronic database, and then coded into specific categories. We begin our analysis with a discussion of vulnerabilities of electronic voting, then turn to a detailed analysis of the precinct incident report data from the March 2006 Cuyahoga primary. We conclude with a discussion of the utility these data for studying election fraud and anomalies, as well as for the development of threat assessment models for voting technologies.

Keywords: Threat assessment, risk analysis, precinct incidents

Joint work of: Kiewiet, D. Roderick; Hall, Thad E.; Alvarez, R. Michael; Katz, Jonathan N.

Can Simple Electronic Voting Be Voter-Verifiable?

Josh Benaloh (Microsoft Research - Redmond, USA)

The technology for verifiable, open-audit elections has advanced substantially since research on this topic began a quarter century ago. Many of the problems are well-understood and have solid solutions. Ballot casting assurance — the problem of ensuring that a programmatically encrypted ballot matches the intentions of an individual human voter — has recently been recognized as perhaps the last substantial obstacle to making this technology fully viable. Several clever schemes have been developed to engage humans in interactive proofs to challenge and check validity of each ballot cast, but such a high standard may be neither practical nor necessary. If done properly, substantial integrity can be obtained by giving voters and observers the *option* to challenge ballot validity without requiring all voters to do so. This option can be made unobtrusive so as to not interfere with the normal process for most voters, but there are numerous risks and subtleties that necessitate a careful examination of the process. This presentation introduces a framework for voter-verifiability in electronic voting, identifies some heretofore unobserved issues with this "simple" method of casting ballots, and describes a detailed process that mitigates all known threats. In doing so, it provides a blueprint for how verifiable, open-audit elections can reasonably be conducted in practice.

Keywords: Voting, elections, voter-verifiable

Full Paper:
http://www.usenix.org/events/evt07/tech/tech.html

Excel Ate My Election!

Ian Brown (Oxford University, GB)

Elections held during May 2007 in England and Scotland for the first time allowed accredited observers access to polling stations and counts. This provided an opportunity for detailed scrutiny of the use of e-voting and e-counting equipment in these elections. This presentation will summarise observations from 10 constituencies and data obtained using Freedom of Information Act requests, interviews with officials, candidates and parties and reports on previous trials. We conclude that inadequate time was available during the procurement process for cross-party consensus to be built around the English e-voting trials or for systems to be fully tested. Design errors meant that a very large number of

Scottish ballots were spoiled, while problems with ballot papers required a large number of votes to be counted manually. Manual recounts found large discrepancies with automated counts, with 56.1% more votes discovered by hand in the Dereham-Humbletoft ward. Laptops used for voting and live electronic registers in Swindon were unreliable, and a lack of usability testing meant that many voters had difficulty using systems. In South Bucks these voters were prevented from voting in person at a polling station, leaving them disenfranchised. Votes initially missed due to an over-wide Excel spreadsheet changed the result in the Highlands and Islands and handed a majority in the Scottish Parliament from the Labour party to the Scottish National Party. These problems raise significant doubts over the outcomes of the May 2007 elections.

Joint work of: Kitcat, Jason; Brown, Ian

Civitas: A Secure Remote Voting System

Michael Clarkson (Cornell University, USA)

Civitas is the first implementation of a coercion-resistant, universally verifiable, remote voting scheme.

This paper describes the design of Civitas, details the cryptographic protocols used in its construction, and illustrates how language-enforced information-flow security policies yield assurance in the implementation. The performance of Civitas scales well in the number of voters and offers reasonable tradeoffs between time, cost, and security. These results suggest that secure electronic voting is achievable.

The name of this system as presented at Dagstuhl was CIVS.

In August 2007, the name was changed to Civitas. For more information, see the Civitas website at http://www.cs.cornell.edu/projects/civitas.

Keywords: Electronic voting, coercion resistance, voter registration, secure bulletin boards, cryptographic protocols

Joint work of: Clarkson, Michael; Chong, Stephen; Myers, Andrew

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1296

Full Paper:
http://www.cs.cornell.edu/people/clarkson/papers/clarkson_civitas_tr.pdf

Information-Theoretic Model of Elections

Benjamin Hosp (George Washington University, USA)

We present an information-theoretic model of a voting system, consisting of (a) definitions of the desirable qualities of integrity, privacy and verifiability, and (b) quantitative measures of how close a system is to being perfect with respect to each of the qualities.

We describe the well-known trade-off between integrity and privacy in this model, and defines a concept of weak privacy, which is traded off with system verifiability. This is an extension of a talk from WOTE 2006, and contains some new applications of the model and arguments for the model's applicability.

Keywords: Information-Theory, Elections, Measurement, Integrity, Privacy, Verifiability

Joint work of: Hosp, Benjamin; Vora, Poorvi

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1298

The Proof of Vote

Catsumi Imamura (IEAv - São José dos Campos, BR)

Election is a complex environment that demands a careful global analysis to design a system architecture. Voters should be identified but kept anonymous regarding to their voting intention. Equipments adopted for collecting, registering and counting the votes should be verified for integrity, consistency, security and transparency by specialist, voters and candidates. And the proof of vote should be set to convince all participants.

This talk addresses the proof of vote mechanism we adopted in Brazil during the election systems maturity life cycle since 1996 elections.

Keywords: Voting machine, proof

Code Voting? A Simple Way to Prevent Automatic Vote Manipulation at Voter's Computer

Rui Joaquim (Polytechnic Institute of Lisbon/INESC-ID - Lisboa, P)

One of the major problems that prevent the widespread of Internet voting is the vulnerability of the voter's computer. A computer connected to the Internet is exposed to virus, worms, spyware, malware and other threats that can endanger the election's integrity. For instance, it is possible to write virus that changes the voter's vote to one predefined vote on election's day.

It is possible to write such a virus so that the voter wouldn't notice anything wrong with the voting application. This attack is very frightening because it may pass undetected. To prevent such attack it is necessary to prevent automatic vote manipulation at voter's computer. Here we present Code Voting, a solution to this problem that is simple enough to be successfully used by the voter and, at the same time, allows the use of cryptographic voting protocols that protect the integrity of the election at the server side of the voting application.

Keywords: Internet voting, automatic vote manipulation, privacy

CodeVoting: Protecting Against Malicious Vote Manipulation at the Voter's PC

Rui Joaquim (Polytechnic Institute of Lisbon/INESC-ID - Lisboa, P)

Voting in uncontrolled environments, such as the Internet comes with a price, the price of having to trust in uncontrolled machines the collection of voter's vote. An uncontrolled machine, e.g. the voter's PC, may be infected with a virus or other malicious program that may try to change the voter's vote without her knowledge. Here we present CodeVoting, a technique to create a secure communication channel to a smart card that prevents vote manipulation by the voter's PC, while at the same time allows the use of any cryptographic voting protocol to cast the vote.

Keywords: Internet voting, vote manipulation

Joint work of: Joaquim, Rui; Ribeiro, Carlos

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2008/1299

Frontiers in Modern Verification for e-Voting

Joseph R. Kiniry (University College - Dublin, IRL)

Constructing a modern e-voting application necessitates using best practices in software engineering. The only way to achieve the system and software quality level demanded by many researchers in the voting research community, and by few individuals and groups in the public, is to use modern verification technology based upon applied formal methods. Recent advancements in verification theory and technology enable, for the first time, the ability to formally design and develop applications on the order of the size and complexity of modern voting computers. This talk summarizes some of those advancements that are particularly apropos to this problem domain, and highlights some of the open research challenges in connecting the research in e-voting systems design to e-voting systems engineering, from the point of view of an applied formal methods researcher who also happens to be an e-voting activist, security analyst, and system architect.

Keywords: Applied formal methods, e-voting, verification, technology, tools

Introduction bullet points and questions/issues for seminar

Joseph R. Kiniry (University College - Dublin, IRL)

Joe Kiniry is a Lecturer in the School of Computer Science and Informatics (http://www.csi.ucd.ie/) at University College Dublin (http://www.ucd.ie/) in Dublin, Ireland.

o He leads the KindSoftware Research Group (http://secure.ucd.ie/) and co-founded and co-leads the Systems Research Group (http://srg.cs.ucd.ie/) which consists of over 40 researchers in fields ranging from pervasive systems' software and hardware (design, implementation, visualization, etc.) to applied formal methods.

o While a Postdoctoral Scholar at Radboud University Nijmegen he led several efforts focusing on the security analysis of modern computing systems that impact upon society including smart cards and e-voting systems.

o He led the (unauthorized by the Dutch government) security hack of the Dutch remote voting system (KOA).

o He led the (authorized) external systems security analysis of the KOA system.

o He was the core verification expert in the design and development of the (partially) formally verified KOA ballot count system.

o He has participated in various ways in the Irish Commission on Electronic Voting (including assisting in the evaluation of the correctness of the PowerVote software, being invited to and uninvited from various panels for asking the wrong questions, etc.).

o He has led the design and development of a verified implementation of an Irish STV-based ballot counting system.

o He leads the development of the GPL-based Open Source re-release of the KOAv2 system.

o Questions/issues for the seminar: - Is e-voting a critical enough application domain to warrant the use of software and hardware verification? - If so, are academic and volunteer e-voting researchers willing to learn and use the concepts, tools, techniques, and process necessary to perform verification. If not, what quality level is necessary, how it is best achieved, and why is verification unimportant?

A Scientist's Guide to Talking with the Media

Joseph R. Kiniry (University College - Dublin, IRL)

The book that I suggested in Monday's panel session is called "A Scientist's Guide to Talking with the Media" by Richard Hayes and Daniel Grossman. You can order it from standard outlets such as Amazon, or, perhaps even better, you can join the Union of Concerned Scientists (of which I am an active member) and order it from them at a reduced rate. See http://www.ucsusa.org/publications/scientist-media-guide.html for more details.

Keywords: Scientist, media, panel

Remote Electronic Voting in Practise - A Review

Robert Krimmer (E-Voting.CC - Viennna, A)

Democracy and elections have more than 2,500 years of tradition. Technology has always influenced and shaped the ways elections were held. Since the ermergence of the Internet there has been the idea of conducting remote electronic elections. In this paper we reviewed 104 elections with remote e-voting possibility based on research articles, working papers and also press releases. Our findings show that remote e-voting has arrived on the international stage, but in small numbers and less sophisticated technology than expected.

Keywords: State of the Art, Technology, Elections

Kleptographic Attacks on E-Voting Schemes

Przemysław Kubiak (Institute of Mathematics & Informatics/TU Wroclaw, PL)

We analyze electronic voting schemes and show that in many cases it is quite easy to implement a kleptographic channel, which is a profound danger for electronic voting systems. We show serious problems with Neff's scheme.

There are also attacks on Chaum's visual voting scheme and some related schemes, which work at least when implementation is not careful enough.

Keywords: Kleptography, electronic voting, receipt voting, coercion, election integrity, verifiable pseudo-randomness

Joint work of: Gogolewski, Marcin; Klonowski, Marek; Kubiak, Przemysław; Kutyłowski, Mirosław; Lauks, Anna; Zagórski, Filip

Full Paper:
http://www.springerlink.com/content/p4702j7847312673/

Provable Unlinkability in Voting Processes

Mirosław Kutyłowski (Institute of Mathematics & Informatics/TU Wroclaw, PL)

Multistage decryption and mixing of votes must be controlled in some way in order to avoid dishonest vote counting.

Methods like radomized partial checking have been designed for this purpose.

We analyze mathematically how much information is revealed by such control procedures and determine the number of mixes necessary to reach high level security.

We also present some related results concerning ThreeBallot scheme.

Keywords: Anonymity, randomized partial checking, ThreeBallot

Full Paper:
http://springerlink.metapress.com/content/x2ja9609xdgl/

See also: Rapid Mixing and Security of Chaum's Visual Electronic Voting, Provable Anonymity for Networks of Mixes

Component Based Electronic Voting Systems

David Lundin (University of Surrey, GB)

An electronic voting system may be said to be composed by a number of components, each of which has a number of properties. One of the most attractive effects of this way of thinking is that each component may have an attached in-depth threat analysis and verification strategy. Furthermore, the need to include the full system when making changes to a component is minimised and a model at this level can be turned into a lower-level implementation model where changes made can cascade to as few parts of the actual implementation as possible.

Keywords: Component based electronic voting systems

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1300

Receipt-Free Universally-Verifiable Voting With Everlasting Privacy

Tal Moran (Weizmann Inst. - Rehovot, IL)

We present the first receipt-free voting scheme that gives voters "everlasting privacy": even an adversary with unbounded computational power will be unable to learn anything about the voters' votes (beyond what is revealed by the final tally). Our voting protocol is designed to be used in a traditional setting, in which voters cast their ballots in a private voting booth. Following in the footsteps of Chaum and Neff, our protocol ensures that the integrity of an election cannot be compromised even if the computers running it are all corrupt .

We present the protocol using physical metaphors (weights and scales), in a way that can be understood even by people that do not have a computer-science background.

Keywords: Voting, cryptographic, receipt-free, everlasting privacy

Joint work of: Moran, Tal; Naor, Moni

Full Paper:
http://www.wisdom.weizmann.ac.il/~Etalm/

See also: Crypto 2006, LNCS vol. 4117, pg. 373-392

Scantegrity

Stefan Popoveniuc (George Washington University, USA)

Scantegrity is an integrity assurance add-on for any conventional optical-scan voting system. It gives voters the ability to verify that their votes are recorded and tallied correctly without altering the basic form of the ballot or how voters use it.

Scantegrity borrows its clockwork from the Punchscan voting system. But instead of being a complete voting system, Scantegrity aims to provide a low-footprint audit companion solution for any current optical scan voting system. Its special audit symbols are included unobtrusively in the ballot printing, out of the way of what voters need to do-vote.

Keywords: Optical scan voting, E2E

Full Paper:
http://scantegrity.org/papers/whitepaper.pdf

Verifying Electronic Voting Protocols in the Applied Pi Calculus (5 minute talk)

Mark D. Ryan (University of Birmingham, GB)

This is a 5-minute advert for my talk, of the same title. I outline our approach to verification of voting protocol properties, and give the essential results.

Keywords: Automatic verification

Joint work of: Ryan, Mark D.; Delaune, Stephanie; Kremer, Steve

Pret a Voter with Human-Readable Paper Audit Trail

Peter Ryan (University of Newcastle, GB)

The Prêt à Voter election scheme allows voters to confirm that their vote is accurately counted whilst maintaining ballot secrecy. Initial analysis indicates that the scheme is highly trustworthy, due to the high degree of transparency and auditability. However, the assurance arguments are subtle and involve some understanding of the role of cryptography. As a result, there remain challenges regarding public understanding and trust. It is essential that a voting system be not only trustworthy but also widely trusted.

In this note, I propose a simple mechanism to generate a conventional paper audit trail that can be invoked should the outcome of the cryptographic count be called into question. It is hoped that having such a familiar mechanism as a safety net will encourage public confidence.

Care has to be taken to ensure that the mechanism does not undermine the carefully crafted integrity and privacy assurances of the original scheme.

Keywords: Verifiable voting, paper audit trail

On SVIS project

Kazue Sako (NEC - Kawasaki, J)

With the experince of developing a binding voting system based on mix-nets for private organization with 17000 elgible voters and running it almost every other months for more than 3 years, we're planning to provide a system for in academic symposiums involving general participants. The first target is Symposium on Cryptography and Information Security (SCIS) which is an annual symposium held in Japan collecting more than 600 participatants. There is SCIS award for young researchers based on a paper-voting from participants. In the presentation I will talk about our effort in SVIS project (Secure Voting in Symposiums) to bring a remote electronic voting system in the next SCIS in January 2008. I will talk about a new privacy requirement in voting protocol which I faced in this project and ideas to meet the requirement.

Client/Server Trade-Offs in Universally Verifiable Elections

Berry Schoenmakers (TU Eindhoven, NL)

Verifiable computation of the election result is commonly done by using either homomorphic techniques or mixing techniques. Homomorphic tallying is fast but the encrypted votes are accompanied by a noninteractive zeroknowledge proof, which may be costly. Mix-based tallying allows for simple, constant-size encrypted votes but sequential mixing and final tallying are relatively slow.

In this talk we give a trade-off in which the work for the voting client is minimized (same effort as in mix-based case) and homomorphic tallying it still possible. Thus, compared to Damgaard-Jurik's result (PKC '02), we reduce the work even further by eliminating the interval proof needed in their case. By using the protocol for binary conversion of Paillier encrypted values by Schoenmakers-Tuyls (Eurocrypt '06), the servers can check the validity of any encrypted vote. The transformation (incl. binary conversion) of the encrypted votes into suitably homomorphically encrypted votes can be done during the election, possibly even before acknowledging receipt of the vote to the voter. Once the election is closed, the election result can be produced quickly using homomorphic tallying.

Weighted Voronoi Region Algorithms for Political Districting

Bruno Simeone (University of Rome "La Sapienza", I)

Automated political districting shares with electronic voting the aim of preventing electoral manipulation and pursuing an impartial electoral mechanism. Political districting can be modelled as multiobjective partitioning of a graph into connected components, where population equality and compactness must hold if a majority voting rule is adopted. This leads to the formulation of combinatorial optimization problems that are extremely hard to solve exactly. We propose a class of heuristics, based on discrete weighted Voronoi regions, for obtaining compact and balanced districts, and discuss some formal properties of these algorithms. Their performance has been tested on randomly generated rectangular grids, as well as on real-life benchmarks; for the latter instances the resulting district maps are compared with the institutional ones adopted in the Italian political elections from 1994 to 2001.

Keywords: Political districting, weighted Voronoi regions, graph partitioning, heuristics

Joint work of: Simeone, Bruno; Ricca, Federica; Scozzari, Andrea

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1302

Coercion-Resistant Tallying for STV Voting

Vanessa Teague (University of Melbourne, AU)

There are many advantages to voting schemes where voters rank all candidates in order, rather than just choosing their favourite. However, these schemes inherently suffer from a coercion problem when there are many candidates, because a coercer can demand a certain permutation from a voter and then check whether that permutation appears during tallying. Existing coercion-resistant cryptographic voting schemes do not address this problem. In this paper, we solve this problem for the popular STV system, by constructing an algorithm for the verifiable tallying of encrypted votes.

Keywords: Electronic voting, coercion, Italian attack, STV, preferential voting, Australian voting

On Coercion-Resistant Electronic Schemes with Linear Work

Jacques Traore (France Telecom R&D - Caen, F)

Remote electronic elections are a promising concept to afford convenience to voters and to increase election turnouts.

Problems related to coercion and to vote-selling, though, impede the realization of these elections in large scale. Recently, Juels, Catalano and Jakobsson proposed a scheme that considers real-world threats and that is more realistic for remote electronic elections. Their scheme, though, has quadratic work factors and thereby is not efficient for large elections. Based on the work of Juels et al., Smith proposed an efficient scheme that has linear work factors. In this talk we first show that Smith's scheme is not coercion resistant. Then we present a new coercion-resistant scheme with linear work factor that overcomes this and other flaws of the Smith' proposal. Our solution is based on a variant of Boneh, Boyen, Sacham group signature scheme (Cryptoť04).

Joint work of: Traore, Jacques; Araujo, Roberto; Foulle, Sébastien

A practical and secure coercion-resistant scheme for remote elections

Jacques Traore (France Telecom R& D - Caen, F)

Juels, Catalano, and Jakobsson (JCJ) proposed at WPES 2005 the first scheme that considers real-world threats and that is more realistic for remote elections. Their scheme, though, has quadratic work factor and thereby is not efficient for large scale elections. Based on the work of JCJ, Smith proposed an efficient scheme that has linear work factor. In this paper we first show that the Smith's scheme is insecure. Then we present a new coercion-resistant election scheme with linear work factor that overcomes this and other flaws of the Smith's proposal. Our solution is based on the group signature scheme of Camenisch and Lysyanskaya (Crypto 2004).

Keywords: Election schemes, coercion-resistance, security

Joint work of: Araujo, Roberto; Foulle, Sebastien ; Traore, Jacques

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2008/1295

Standardized Basic Requirements and Evaluation Techniques for Remote Electronic Voting

Melanie Volkamer (Universität Passau, D)

In the past, election officials have invited security experts to check the e-voting systems for vulnerabilities. In general, each group of experts used their own set of requirements on different levels of detail and the evaluation methods as well as the evaluation depth varied a lot. This leads to judgments about e-voting systems which are hardly comprehensible by third parties. Thus, standardized requirements and evaluation procedures are essential to successfully introduce electronic voting.

This talk provides a solution based on the internationally agreed certification standard Common Criteria by presenting our Protection Profile (PP) for remote electronic voting. The Protection Profile Project was supported by the German Federal Office for Information Security (BSI) and discussed with the e-voting expert round of the German scientific association of informatics (GI) and experts of other organisations including universities, ministries, administrations, product developers and data protection authorities. The certified PP serves as a contribution to the international community and can be used for certification of remote electronic voting systems in any country around the world that has adopted the Common Criteria.

The developed Protection Profile for remote electronic voting defines only a basic set of required security requirements based on a couple of assumptions which needs to be extended depending on the particular election the system should be used for.

The talk will first sketch the current situation, give a short introduction to the CC, including the advantages compared to existing approaches to scrutinize electronic voting system and proposes the Protection Profile including its restrictions in the current version and the mainly discussed topics in the development process.

Electronic Vote-Verification Receipts

Poorvi Vora (George Washington University, USA)

Recently proposed voter-verifiable protocols provide encrypted paper receipts to voters, who may later check that these receipts are in the electronic ballot box. This paper describes an enhancement that allows the voter to electronically transmit, from the polling booth, her encrypted receipt to an external verifier of her choice, who may perform the check on her behalf. It uses a short-lived human-verifiable digital signature - whose security depends on the hardness of an AI problem - to enable the voter, without access to trusted computation, to be certain that the receipt has been securely deposited with the external verifier. This approach presents the advantage of being easily extensible for those with visual disabilities.

Keywords: Human-verifiable, digital signature, voting

Joint work of: Vora, Poorvi; Simha, Rahul

Full Paper:
http://www.seas.gwu.edu/∼Epoorvi/CaptchasWOTE07.pdf

See also: initial version at WOTE 2007

Casting Votes in the Auditorium

Dan Wallach (Rice University, USA)

In elections employing electronic voting machines, we have observed that poor procedures, equipment failures, and honest mistakes pose a real threat to the accuracy of the final tally. The event logs kept by these machines can give auditors clues as to the causes of anomalies and inconsistencies; however, each voting machine is trusted to keep its own audit and ballot data, making the record unreliable. If a machine is damaged, accidentally erased, or otherwise compromised during the election, we have no way to detect tampering or loss of auditing records and cast votes.

We see a need for voting systems in which event logs can serve as robust forensic documents, describing a provable timeline of events leading up to and transpiring on election day. To this end, we propose an auditing infrastructure that draws on ideas from distributed systems and secure logging to provide a verifiable, global picture of critical election-day events, one which can survive individual machine malfunction or malice. Our system, the Auditorium, joins the voting machines in a polling place together in a private broadcast network in which all election events are logged redundantly by every machine.

Each event is irrevocably tied to the originating machine by a digital signature, and to earlier events from other machines via hash chaining.

In this paper we describe in detail how to conduct an election in the Auditorium. We demonstrate our system's robustness to benign failures and malicious attacks, resulting in a believable audit trail and vote count, with acceptable overhead for a network the size of a polling place.

Joint work of: Sandler, Daniel; Wallach, Dan

Full Paper:
http://www.usenix.org/events/evt07/tech/full_papers/sandler/sandler.pdf

See also: 2007 USENIX/ACCURATE Electronic Voting Technology Workshop

Verifiable Internet Voting for Unsecure Platform

Filip Zagórski (Wroclaw University of Technology, PL)

We present a voter verifiable Internet voting scheme which provides anonymity and eliminates the danger of vote selling even if the computer used by the voter cannot be fully trusted.

The ballots cast remain anonymous - even the machine does not know the choice of the voter. It makes no sense to buy votes - the voter can cheat the buyer even if his machine cooperates with the buyer.

Nevertheless, the voter can verity that his vote has been counted.

Joint work of: Zagórski, Filip; Kutyłowski, Mirosław

Simulation-Based Analysis of E2E Voting Systems

Olivier de Marneffe (University of Louvain, B)

End-to-end auditable voting systems are expected to guarantee very interesting, and often sophisticated security properties, including correctness, privacy, fairness, receipt-freeness, ... However, for many well-known protocols, these properties have never been analyzed in a systematic way.

In this paper, we investigate the use of techniques from the simulation-based security tradition for the analysis of these protocols, through a case-study on the ThreeBallot protocol.

Our analysis shows that the ThreeBallot protocol fails to emulate some natural voting functionality, reflecting the lack of election fairness guarantee from this protocol. Guided by the reasons that make our security proof fail, we propose a simple variant of the ThreeBallot protocol and show that this variant emulates our functionality.

Keywords: UC framework, simulatability, security proof, ThreeBallot

Joint work of: de Marneffe, Olivier; Pereira, Olivier; Quisquater, Jean-Jacques

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1297