Frontiers of Electronic Voting - Dagstuhl Seminar 07311 Executive Summary

David Chaum[1], Mirosław Kutyłowski[2], Ronald Rivest[3], Peter Y. A. Ryan[4]

[1] Institute of Author1, Department of Author1
Address ZIP, Town, Street, Country
david@chaum.com

[2] Wrocław University of Technology, Institute of Mathematics and Computer Science
50-370 Wrocław, Wybrzeże Wyspiańskiego, Poland
miroslaw.kutylowski@im.pwr.wroc.pl

[3] MIT, Department of Electrical Engineering and Computer Science
MA 02139-4307, Cambridge, 77 Massachusetts Avenue, USA
rivest@mit.edu

[4] University of Newcastle upon Tyne, School of Computing Science
NE1 7RU, Newcastle upon Tyne, United Kingdom
peter.ryan ncl.ac.uk

Abstract. 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

1 Introduction

Democracy and voting systems have received considerable attention of late, with the validity of many elections around the world being called into question. The US experience demonstrates that simply deploying technological "solutions" does not solve the problem and can easily exacerbate it. Nevertheless, many other countries are either deploying e-voting and e-counting systems or planning to do it.

The aim of the seminar was to present and discuss promising technologies, schemes, and cryptographic protocols to achieve high assurance of accuracy and privacy in the casting and counting of votes. Special attention was given to attacks and dangers that emerge for electronic voting systems.

The challenge is highly socio-technical in nature: requires an excellent understanding of the potentialities and dangers of technological approaches as well as an appreciation of the social, legal and political impact. The seminar thus aimed to bring together researchers and practitioners from academia and industry, whose work relates to electronic voting systems, to evaluate the state of the

Dagstuhl Seminar Proceedings 07311
Frontiers of Electronic Voting
http://drops.dagstuhl.de/opus/volltexte/2008/1294

art, to share practical experiences, and to look for possible enhancements. The overall aim then was to stimulate discourse between the various stakeholders and enhance the understanding of voting technologies and practices.

2 Workshop Formula

The workshop consisted of the following parts:

Introductory Session. During this time each participant described his research profile, specific interests in voting procedures, her or his expectations as well as major challenges from own point of view. During this part each participant was assigned a 5 minute slot.

General Discussions. Two sessions have been devoted to major problems concerning practical implementation of e-voting systems. The main goal of this part of the seminar was to find a common agreement on the major issues concerning requirements, design goals and implementation of modern voting systems.

Voting Machines and End-to-End Paper Based Methods. Technologies which require presence of the voter in a poll station were grouped in this section. Both electronic and non-electronic methods were concerned, the main focus was on end-to-end designs, where no assumption on system security is necessary.

Verifiability. This section concerned methods for achieving secure design of voting protocols and dependable implementations.

Internet Voting. Methods which enable to vote remotely where discussed in this section. The main focus was on Internet based methods. The main problem concerned was what security level is achievable.

Foundations. Various technologies that are components of voting protocols have been discussed in this part.

Voting Systems. This session was devoted to practical presentation and discussion of the voting systems.

Threats. Diverse issues concerning dangers inherent in voting procedures, both potential and existing ones, were topic of this session.

Additionally, further issues, like analyzing anomalies, implementation experiences, and political districting were presented.

3 Talks

Michael Alvarez: Using Incident Reports to Detect Election Anomalies and Irregularities.

Josh Benaloh: Can Simple Electronic Voting Be Voter-Verifiable?

Michael Clarkson: Civitas: A Secure Remote Voting System.

Rop Gonggrijp: Hacking the Nedap (practical presenatation).

J. Alex Halderman and Dan Wallach: The California Secrectary of State's *top-to-bottom* Report.

Benjamin Hosp: Information-Theoretic Model of Elections.
Catsumi Imamura: Elections in Brazil.
Rui Joaquim: CodeVoting: A Simple Way to Prevent Automatic Vote Manipulation at Voter's Computer.
John Kelsey: Hacking Paper: Some Random Attacks on Paper-Based E2E System.
Aggelos Kiayias: Security Vulnerabilities in the Diebold OS and TSx Terminals and the Adder Voting System.
Joseph R. Kiniry: Frontiers in Modern Verification for e-Voting.
Robert Krimmer: Remote Electronic Voting in Practise - A Review.
Przemysław Kubiak: Kleptographic Attacks on E-Voting Schemes.
Mirosław Kutyłowski: Provable Unlinkability in Voting Processes.
David Lundin: Component Based Electronic Voting Systems.
Tal Moran: Receipt-Free Universally-Verifiable Voting With Everlasting Privacy.
Stefan Popoveniuc: Scantegrity.
Ronald Rivest: ThreeBallot, VAV, and Twin.
Michael Roe: Threats to an Election.
Mark D. Ryan: Verification of Electronic Voting Protocols.
Peter Ryan: Prêt à Voter with Human-Readable Paper Audit Trail.
Kazue Sako: On SVIS project.
Roberto Samarone Araujo: On Coercion-Resistant Electronic Schemes with Linear Work.
Berry Schoenmakers: Client/Server Trade-Offs in Universally Verifiable Elections.
Bruno Simeone: Weighted Voronoi Region Algorithms for Political Districting.
Vanessa Teague: Coercion-Resistant Tallying for STV Voting.
Jacques Traore: A Practical and Secure Coercion-Resistant Scheme for Remote Elections.
Poorvi Vora: Electronic Vote-Verification Receipts.
Dan Wallach: Casting Votes in the Auditorium.
Filip Zagórski: Verifiable Internet Voting for Unsecure Platform.
Olivier de Marneffe: Simulation-based Analysis of E2E Voting Systems.

4 Follow-up Publications

A number of papers have been contributed to these Dagstuhl proceedings. Some number of papers directly related to Dagstuhl presentations, or resulting from work done during the seminar are planned to be included in a special volume of LNCS Series devoted to e-voting technology, edited by David Chaum.

5 Dagstuhl Accord

During discussions in Dagstuhl, a draft of a common opinion on major current problems of e-voting has been prepared. Further editorial work has been carried on by the organizers of the workshop. Finally, the following version of Dagstuhl Accord has been agreed by the organizers and presented to the participants for signing. In the next stage, the organizers will enable general public to join the Dagstuhl Accord by signing a supporting declaration.

Dagstuhl Accord on Electronic Voting

Participants of the 2007 Dagstuhl Conference on Frontiers of E-Voting agree that:
Taking advantage of technology to improve large-scale elections has recently captured the interest of researchers coming from a number of disciplines. The basic requirements pose an apparently irreconcilable challenge: while voter confidence hinges on transparently ensuring integrity of the outcome, ballot secrecy must also be ensured. Current systems can only address these essential requirements by relying on trust in those conducting the election or by trust in the machines and software they use. Some promising new systems dramatically reduce the need for such trust. What are called "end-to-end" voting systems, for example, allow each voter to ensure that his or her vote cast in the booth is recorded correctly. They then allow anyone to verify that all such recorded votes are included in the final tally correctly. Surprisingly, through use of encryption typically, these systems can also provide privacy of votes. They do this without introducing any danger of "improper influence" of voters, as in vote buying and coercion. Moreover, such systems offer all these properties without relying on trust in particular persons, manual processes, devices, or software.
Care must still be taken to ensure proper implementation and education of voters in order to avoid misuse or incorrect perceptions. Some are also concerned that the level of understandability and observability of hand-counting of paper ballots in polling places will not be matched by electronic systems. The challenge for governments and civil society should be to find ways to foster development and testing of new election paradigms in general and to allow them to be assessed and expeditiously rise to meet their potential to improve elections.
The challenges for the technical research community now forming around election technology includes further exploration and refinement of these new types of systems. Particularly promising and important areas include analysis, formal modeling, and rigorous proofs regarding systems and potential threats. Initial deployments of these systems are starting to provide valuable real-world experience, but effective ways to communicate and expose their workings may also be important. The goal is systems that increase transparency regarding the correctness of the election results and yet maintain secrecy of individual votes. Improved voter confidence may follow.
Voting over electronic networks has various attractions, is starting to be deployed, and is regarded by some as inevitable. No solution, how-

> *ever, has been proposed that provides safeguards adequate against various known threats. Problems include attacks against the security of the computers used as well as attacks that impede communication over the network. Improper influence of remote voters is also a significant problem, although it is tolerated with vote by mail in numerous jurisdictions. Securing network voting is clearly an important research challenge. We cannot, however, prudently recommend any but unavoidable use of online voting systems in elections of significant consequence until effective means are developed to address these vulnerabilities.*

The text of the Dagstuhl Accord and the list of signees are available on the webpage http://dagstuhlaccord.org/