2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '08)

July 28–29, 2008
San Jose, California, USA

NEW DIRECTIONS AND REFLECTIONS ON OLD DIRECTIONS

Summarized by Rik Farrow

- ***You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems***
  J. Alex Halderman, Princeton University; Eric Rescorla, RTFM, Inc.; Hovav Shacham, University of California, San Diego; David Wagner, University of California, Berkeley

Eric Rescorla spoke very, very fast about tactics for reducing the risk of using existing electronic voting equipment, such as Election Management Systems (EMSes), Direct Recording Electronic (DRE) machines, and optical scanners. Research has shown that viruses can be spread between management, voting, and voting counting devices, and this work focuses on uncovering data flows and preventing the spread of viruses among devices.

They considered elections as having five phases: device initialization, voting, early reporting, tabulation, and auditing. Device initialization, the writing of ballot definitions to memory cards, can easily spread a virus from the EMS to each DRE. The EMS can itself be infected from a reused memory card, so their advice is never to reuse memory cards, but to preserve used cards as evidence and buy new cards for each election. For commodity cards, this could cost as little as $0.10 per voter, but for proprietary ones (used in Premier/Diebold and some Hart devices), this is out of the question. They propose using a special-purpose initialization device that erases cards without first reading them, installs the ballot definitions, and gets physically reset before initializing the next card.

After voting, early reporting represents the next danger point. They suggest using a sacrificial EMS just for early reporting. During the tabulation phase, they again suggest using a sacrificial EMS and performing a manual audit, comparing the results of EMS tabulation and a random selection of summary tapes. As an alternative, before being passed to the EMS the memory cards would be read on a separate device and the output sanitized so that it can only include election results.

The first questioner mentioned that election officials are "tight on money like you can't believe" and wondered what could be done with a nickel per voter. Eric suggested performing audits first, and replacing memory cards each time, while admitting that replacing cards is infeasible given the budget, but it is the best and safest thing to do. Josh Benaloh then asked, "Why not trust cards you just purchased?" Eric responded that devices from the factory might not be trustworthy, and if the EMS gets compromised, it's game over.

- ***Administrative and Public Verifiability: Can We Have Both?***
  Josh Benaloh, Microsoft Research

Josh described the difference between administrative and public verifiability: The first puts all the trust in some special group of people, whereas the second presents the best solution. But getting the public to believe this, and to participate in verifying the accuracy of elections through the use of cryptographic checks, is difficult. He then described a system that combines features of both types of checking.

Josh's solution relies on changes to optical scanners. Optical scanners tally votes as ballots are fed into them, and he wants scanners to encrypt the results of the scan, save the encrypted result and give a paper receipt to the voter, print the interpretation of the scanner on the ballot with a digital signature, and, finally, allow the voter to cancel and return a ballot. The returned ballot should match the voter's paper

receipt and a published digital signature created when the ballot was scanned. Current optical scanners can return a ballot in the case of an overvote, but not print on ballots.

Barb Simons called his solution simple and eloquent, then asked what happens if she cancels her ballot. Josh answered that she gets to keep that ballot, then vote again on another ballot. Peter Neumann suggested that some election administrator could limit voters to two ballots, then defraud you on the second one. Josh countered that, to the optical scanner, all ballots appear alike (i.e., there are no serial numbers). Another person asked how we know that the cancelled ballots represent a sample of actual ballots that have been cast. Josh replied that this is a simple system by design and that you gain confidence that the system works correctly by checking that recorded yet cancelled votes match the challenges made by voters.

- ***The Case for Networked Remote Voting Precincts***
  Daniel R. Sandler and Dan S. Wallach, Rice University

Dan Wallach began by saying that, as a security person, you never want to see voting on the Internet. You want a physical presence for equipment, witnessing by election officials, and an environment free of coercion. But remote voting, for example, for soldiers overseas, could be made secure, and he used postal voting as an example. Vote by mail relies on the voter marking his or her ballot, sealing it inside an envelope, then adding the voter name/signature to the outside of the envelope, something that gets removed before the vote gets counted. Provisional ballots work similarly, where ballots get a double enclosure, with the voter's info on the outer envelope.

Their design builds on VoteBox (see the paper in the Security proceedings) to include remote electronic voting (RemoteBox). The remote polling place is maintained and monitored by trusted nonpartisan officials who can authenticate voters against a voter database using the same identification systems as used today. The voter gets an electronic ballot on a VoteBox system and then votes, with the encrypted results being broadcast using Auditorium to provide tamper-resistant voting logs. The encrypted ballots are either locally written to a tamper-proof device or sent via a one-way channel (data diode) to a public medium for the posting of provisional ballots.

Someone asked whether Voter Verified Paper Audit Trail (VVPAT) could be used with this system. Dan replied that this system allows the same cast-or-challenge method as Josh's. When a vote gets challenged, it will not be counted, but it will still appear on the public media (encrypted) and can be checked for accuracy. Someone else asked whether the auditing could be local, and Dan said that VVPAT could be added if wanted. Brad Talent, an election official from LA, said that nothing is more odious than comparing signatures on mail-in ballots after an election. What gets lost is the whole face-to-face identification process. Dan responded that this process is digital, and a photograph of the voter could be included with the digital envelope.

PANEL

Summarized by Eric W. Smith (ewsmith@stanford.edu)

- ***How Can Researchers and Election Officials Better Work Together?***
  Moderator: Joseph Lorenzo Hall, University of California, Berkeley

  Panelists: Jeremy Epstein, Software AG and Verified Voting Foundation, Consultant to Kentucky Attorney General on Voting Systems Security; Elaine Ginnold, Registrar of Voters, Marin County, California; Gregory Luke, Strumwasser & Woocher LLP; David Wagner, University of California, Berkeley; Steve Weir, Registrar of Voters, Contra Costa County, California, and President, California Association of Clerks and Election Officials (CACEO)

First each panelist spoke for a few minutes.

Ginnold praised the recent increase in research on election administration (with much funding and many papers published recently), but he cautioned that its impact often depends on collaboration and communication with election officials, which is best achieved when the research is relevant, displays ethics, and is well documented. Relevant research helps election administrators solve real-world problems. For example, officials received complaints about the use of a random number generator to choose precincts for manual tallying. Researchers suggested a better solution, the use of 10-sided dice, which has been implemented in Marin County and ended the complaints. Ethics in research is also needed to foster collaboration. Researchers must remain objective and neutral and be careful not to become spokespeople for other election activists with more political agendas. Protecting confidentiality can also be key. Finally, research should be documented in careful, scientific publications; these can help counteract inaccurate activist claims, help election officials in discussions with their superiors, and lead to policy changes. Since 2000, election officials have been under attack; Ginnold's suggestions can make them more comfortable collaborating with researchers.

Epstein spoke about the need for a common threat model for elections, one that includes low-tech, real-life threats of which researchers might not be aware (e.g., jamming the gears in a lever-voting machine with a pencil lead). He noted that technologists and poll workers are aware of different classes of threats and need to work together instead of talking past each other. Collaboration is particularly important when money is scarce; one must prioritize threats and address those that seem most pressing and most fixable. Finally, researchers need to provide election workers with usable, practical guidance (e.g., explanations of why random numbers should be used instead of pseudo-random numbers).

Weir said that he was critical of the California top-to-bottom review of voting systems. He noted that election officials seemed to be systematically excluded (with no reason given). He also noted that of the three big issues—technology, physical security, and personal security—the review looked only at technology. Also, usability was not addressed, and so the review missed the serious "double bubble" problem that affected tens of thousands of votes in Los Angeles. Weir believes in gathering a lot of data about the elections he runs, but he noted that officials worry that such data may be used against them. Finally, he suggested that each of the seven voting systems in California be assigned to a researcher who would work with the vendor and obtain and analyze any available election data for that machine.

Wagner observed that there are no magic answers to the issues of voting, but he noted that working in the trenches of elections can help researchers identify the key issues. He strongly recommended that researchers volunteer as poll workers or election observers to see the election process firsthand. For example, researchers will learn how tiring election work is (and may avoid advocating for complicated procedures to be followed at the end of a 14-hour day). They will also learn the importance of making systems easy to use, even for poll workers with minimal training or who only work once every two years. Wagner also advised that researchers consider working for election officials and suggested that they should maintain an attitude of humility. It's the election officials, not the researchers, who have democratic legitimacy (through appointment or election) and who ultimately make the decisions. Researchers can only give advice. Finally, he advised that someone wanting to do a security review should: (1) call his or her spouse (because the process takes so much time!); (2) call his or her lawyer (since much time will be spent on negotiation, especially to get access to vendor equipment and code); (3) be patient, because, although the work may have a great impact, it may also go slowly.

Luke practices election law in Santa Monica and provides a voice to voters or candidates who want recounts. He suggested attending a recount to see how the process works. Luke repeatedly emphasized the importance of transparency in the election process (a paper audit trail of some sort is key to doing a recount). Indeed, several election machines were decertified in California for being unable to perform meaningful recounts. How was such a fundamental feature left out of the systems? Luke notes that assumptions may not play out in the real world, that there is often a lack of communication between stakeholders, and that participants may be saddled with the poor decisions of their predecessors. Luke noted that it has been difficult and time-consuming for voters to exercise their rights to examine election materials, thus lending the perception of a lack of transparency. Finally, he noted that those working on new solutions should carefully consider the needs of each stakeholder, choose procedures where results are verifiable within the time frame of existing post-election procedures, and prefer procedures that generate evidence which would be admissible in court in the case of a challenge.

Hall noted that Ohio's election review included a panel of election officials, unlike California's.

A questioner noted that the panel represents progress in collaboration between researchers and election administrators but leaves out government elections commissions and, especially, vendors. The real gap may be between researchers and administrators on one side and vendors on the other. The panel noted that vendors want to stay in business and respond to incentives and penalties, so they are making improvements, but new systems take a long time to certify. Also, more explicit specifications (e.g., requiring transparency) should help.

A questioner who had been involved in the top-to-bottom review was saddened at the negative reaction by election officials to the review. He said vendors were producing poor machines that made election officials look bad. But Ginnold noted that the problems were not just with the machines but also with the lack of testing, mistakes in election offices, and poll workers' incorrect use of the machines.

Another questioner noted that election officials are under fire from many corners and asked to what extent they make the distinction between criticism from researchers and from other, more political activists. Ginnold noted that many officials are unaware of the research and that some activists attempt to use researchers to promote their agendas. Hall noted that it can be hard to distinguish good science from bad.

The next questioner, who is involved in a voting rights group in California, objected to the negative comments about some election advocates. He said his group advocated paper-based optical scanners instead of direct-recording electronic (DRE) machines and was complimented for being prepared and polite. He asked Weir how complicated it was to prepare for an election in his county. Weir replied that for two, somewhat overlapping elections, his calendar ran to 79 pages and included 990 critical items, but said that amount was not overwhelming. Hall noted that, prior to one election, election staff had no days off for six weeks.

A questioner noted that researchers tend to find fault and are unlikely to vouch for any system as correct. He wondered what would happen when voting systems are much improved several design cycles from now. Will researchers still be unwilling to vouch for them? He echoed the call for transparency and noted that it is unnatural for a scientist who has analyzed a voting system to ask others to trust his analysis if they cannot repeat it themselves. Ginnold noted that one can distinguish research from activist rhetoric by observing the lack of bias, the straightforward analysis, the consideration of multiple viewpoints, and the lack of fallacious logic. Wagner noted that there is no good outcome when analyzing an already deployed system; indeed, any problems found may not be fixable.

Another questioner noted the small number of vendor representatives at the conference (a single attendee out of 70). The panel noted that it is hard to build a relationship with people in whose products you find faults and observed that vendors are often reluctant to talk.

The final questioner suggested attending certification hearings in one's state and noted that putting some election data online helped diffuse the Los Angeles "double bubble" situation (being another call for transparency).

AUDITING AND TALLYING SESSION II

Summarized by Eric W. Smith (ewsmith@stanford.edu)

- ***Pre-Election Testing and Post-Election Audit of Optical Scan Voting Terminal Memory Cards***
  Seda Davtyan, Sotiris Kentros, Aggelos Kiayias, Laurent Michel, Nicolas Nicolaou, Alexander Russell, Andrew See, Narasimha Shashidhar, and Alexander A. Shvartsman, University of Connecticut

In a recent election, the hand-counted and machine-counted precincts had different winners. That may have been for demographic reasons, but how can we trust the machines? This talk described an audit of the Accu-Vote Optical Scan (AV-OS) tabulators that were used in the November 2007 Municipal Elections in Connecticut, done at the request of the Office of the Secretary of the State of Connecticut.

The Accu-Vote system provides a voter-verifiable paper trail but has some known issues, including possible tampering with memory cards or seals, so auditing is desirable. The auditing process described in the talk focused on the memory cards, which include custom software for each district. The audit included integrity checks before and after the election and a post-election check that the cards were in states consistent with election use. The researchers received no assistance or code from the vendor of the AV-OS. They wrote custom firmware to dump data from the cards. The undocumented, built-in dumping procedure made changes to the card and was too slow to use on so many cards. They analyzed the card format, status (e.g., election closed), counters, audit log, etc.

The pre-election tests revealed that poll workers did not always follow proper procedures. They were instructed to test the cards and then randomly choose one (out of four) to be audited. A total of 3.5% of cards contained junk data, which should have been caught in testing. Also, about half of the cards were not in the exact correct state (with most having been tested but not "set for election" as prescribed by the testing procedure). One card contained nonzero counters, indicating that it was not reset after testing, but the issue would probably have been caught in the check for "zero counters" prescribed at the start of the election if that step had not been skipped.

The post-election audit covered 100 cards, only some of which were used in the election. Eight of the cards had junk data (and so must not have been used). One was blank (not programmed for elections). About 40% were used and about 47% were set but unused (with all cards in these last two categories having valid data and software). The authors conclude that both pre-election and post-election tests and audits of memory cards (and similar components) are crucial. Cards not in the proper state (especially the one with nonzero counters before the election) indicate that poll workers didn't follow the election procedures carefully enough. Also, the large numbers of cards with junk data indicate software or hardware problems or a lack of testing; in any case, the rate of cards with junk data was unacceptable. The authors do note that no incorrect ballot data or memory card software was detected in the audit.

- ***Improving the Security, Transparency, and Efficiency of California's 1% Manual Tally Procedures***
  Joseph Lorenzo Hall, University of California, Berkeley

California election law requires a "1% manual tally." The talk discussed work that helped San Mateo County specify exactly what should occur during the tally. The work strove to be general, in order to help other California counties as well.

If one cannot get access and oversight regarding election systems, one can still audit elections by comparing two independent sets of records, if they exist. Although 38 states keep such records, only 17 actually count them. California has had manual tally auditing since 1965, but not many details are prescribed by the law (which specifies that it must be done in 1% of precincts, be random, finish in 28 days, and include all ballot types). A group of researchers set out to improve security, efficiency, and transparency of the process. They proposed interim procedures, which were tested in San Mateo County over a few iterations, and they observed the process in other counties.

A blue-ribbon panel concluded that "margin-dependent audits with a floor" are best, but what about the low-level details? The procedures described by the talk touch on many of the issues. The steps of the tally include retrieval of materials, seal verification, sorting of ballots into piles, tallying involving four people (a caller, a witness, and two talliers who stay in sync every 10 ballots), and reconciliation of all discrepancies between the hand tally and the electronic results. The procedures specify that selection and tallying take place after ballots are counted (lest attackers decide to change results that they know were not selected for tallying), that tallying then happen quickly (short attack window), and that counters be "blind" (lest they subconsciously reach the "expected" result) but not too blind (e.g., to reconcile discrepancies they may have to work backward from the expected results to find subtle oval-filling mistakes).

Hall noted that some procedural changes need to be reviewed by experts. For example, choosing precinct numbers

digit by digit can be a problem. For example, with 1204 precincts, choosing each digit separately gives equal weight to the small group of precincts from 1000 to 1204 and the larger group with a "0" in the thousands place. He advised making the tally process transparent by giving public notice in advance, publishing procedures and useful data, and having clear lines of communication and clear procedures. He described several ways to save time, since in large counties the tallying process can take all 28 days, including the use of a spreadsheet to "bin" random numbers (thereby saving many dice rolls) and prefilling the tally sheets. He also suggested using RFID tags to help with chain-of-custody issues.

A questioner noted that election officials and staff also spent a lot of time on this effort to improve their processes. A commenter from Ohio noted that the procedures, including audio and video resources, were very helpful.

The procedures are on the Web at http://josephhall.org/procedures/ca_tally_procedures-2008.pdf.

- ***Comparing the Auditability of Optical Scan, Voter Verified Paper Audit Trail (VVPAT) and Video (VVVAT) Ballot Systems***
  Stephen N. Goggin and Michael D. Byrne, Rice University; Juan E. Gilbert, Gregory Rogers, and Jerome McClendon, Auburn University

Auditing should be a secure, accurate check on vote counts. But how accurate are the counts? That is, how well do humans count the ballots? Goggin compared the accuracy of counts from a Voter Verified Paper Audit Trail (VVPAT) system, an optical scan system, and a prototype Voter Verified Video Audit Trail (VVVAT) system.

The study used only a single human counter (not the usual group) but used ballots in perfect condition (thereby eliminating the difficult interpretations of voter intent or heat-damaged thermal paper). The metrics were accuracy of the count, efficiency (time to count), and satisfaction (the subjective experience of the counter). For accuracy, the most important metric, only 65.0%, 45.0%, and 23.7% of participants provided the correct vote counts for the optical scan, VVPAT, and video systems, respectively. Only the difference of the video system from the other two was statistically significant. The video system tended to have undercounts. For close races, statistically significant results regarding the number of perfectly counted races indicated that optical scan was better than VVPAT, which was in turn better than VVVAT. The results for lopsided races were not statistically significant.

In terms of efficiency, the first count of the VVPAT ballots was slow (owing to the need to physically separate the ballots from the spool). Subsequent VVPAT counts and counts done with other technologies all took about the same amount of time: 10–15 minutes for one person to count 120 ballots. In terms of satisfaction, no reliable difference among the technologies was observed.

The authors concluded that although the optical scan system fared best, no technology was great, and so redundant, group, or error-correcting counting is needed, but group counting has its own set of issues. Furthermore, human counting should not be considered the "gold standard" of accuracy unless such safety measures are in place.

A questioner noted that counting using the video technology was fast but inaccurate, whereas one might think it would be slow (with much fast-forwarding and rewinding, etc.). In fact, the video counting was done with a series of screen captures.

A questioner asked how much instruction was given to the counters. They were given 10–15 minutes of instruction and told to be accurate, not fast (and yet they still made many errors).

CONVENTIONAL E-VOTING SYSTEMS

Summarized by Eric Cronin (ecronin@cis.upenn.edu)

- ***Modeling and Analysis of Procedural Security in (e)Voting: The Trentino's Approach and Experiences***
  Komminist Weldemariam, Fondazione Bruno Kessler and University of Trento; Adolfo Villafiorita, Fondazione Bruno Kessler

Komminist Weldemariam presented the results of a security evaluation on the electronic voting system being adopted in the autonomous region Trentino of Italy. The evaluation was based on traditional software modeling and evaluation approaches, but the models were constructed in a way that also captured the procedural aspects of voting. The tools in particular look for "procedural threats": actions that can modify assets in ways that go undetected by election procedures.

In addition to the rich procedural environment, elections also have a number of other unusual and unavoidable aspects when compared to commonly modeled systems: highly mobile assets (intrinsic to elections), asset evolution (the same devices contain both ballot definitions and election results at different points in time), number of instances, and presence of nondigital assets. All these characteristics are modeled using UML diagrams, and then automated analysis is performed by injecting attacks at any point in the model and checking for undetected changes to assets or denial-of-service states.

The authors' results show that by formally modeling the procedural aspects of a system, a richer analysis of security threats is possible through automation. A member of the audience raised the question of how to model the lack of infallibility in the human aspect of elections, and how to identify which procedures are more critical to be performed correctly. The speaker answered that they were aware of the issue of poll worker reliability: one possible approach is to treat them as untrusted for the analysis. Two other areas of future work asked about were detecting subtle insider

attacks and cost analysis of threats identified by the automated tools.

- ***Security Evaluation of ES&S Voting Machines and Election Management System***
  Adam Aviv, Pavol Cerny, Sandy Clark, Eric Cronin, Gaurav Shah, Micah Sherr, and Matt Blaze, University of Pennsylvania

Micah Sherr presented the first of two papers on the results of Ohio's EVEREST (Evaluation & Validation of Election-Related Equipment, Standards and Testing) project. Sherr was part of a team that performed a source-code analysis of the Election Systems and Software (ES&S) voting system. (The authors worked closely with a "red team" at WebWise Security, who also analyzed the ES&S system.) Unlike the two other vendors examined in EVEREST, no in-depth analysis of ES&S had been performed. The analysis examined 670,000 lines of source code in 12 programming languages, targeting five hardware platforms. Both touch screen and optical scan hardware were evaluated, as well as the back-end software used to design ballots, program voting hardware, and tabulate results.

Scherr began with an overview of the ES&S voting system and its hardware and software components. He then went on to discuss the methodology used by the researchers and some of the major results of their study. Because of the time constraints faced (ten weeks from receipt of source code and hardware to delivery of final report), an ad hoc triage approach focusing on the areas of most strategic importance to the attacker was employed. Analysis concentrated on crypto, media processing, access control, and key distribution. This approach differed greatly from the checklist-like approach used by the official Independent Testing Authorities (ITAs).

The authors found that all data integrity and authenticity mechanisms were circumventable; attacks could be carried out by single poll workers or sometimes single voters; unexpected interaction between components led to systematic vulnerabilities; attacks could spread virally from one component to another, forming a closed loop. Specific attacks shown included common physical keying of all hardware in all locations, unprotected access to the audit printer (which is the legal record in Ohio) allowing arbitrary output to be printed, unauthenticated loading of firmware on both optical scanners, and initialization and reprogramming of touchscreen terminals by using a magnet and PDA. The presentation concluded with some observations. The evaluators found that although the ITA evaluation led to syntactically good code (well commented, standard naming conventions, etc.), design failures were evident throughout, and common automated security tools (e.g., Fortify) had clearly not been used. Additionally, the complex design makes it extremely hard to defend procedurally or technically, and the authors could not offer any quick fixes.

- ***Systemic Issues in the Hart InterCivic and Premier Voting Systems: Reflections on Project EVEREST***
  Kevin Butler and William Enck, The Pennsylvania State University; Harri Hursti; Stephen McLaughlin, The Pennsylvania State University; Patrick Traynor, Georgia Institute of Technology; Patrick McDaniel, The Pennsylvania State University

William Enck was part of the team that evaluated the voting systems manufactured by Hart InterCivic and Premier Voting Systems (formerly Diebold). Unlike the ES&S system, these two systems were evaluated in the 2007 California Top to Bottom review. The focus was therefore on evaluating the impact of the earlier reviews on Ohio elections. Whereas the public reports from earlier studies were available, accessing the private reports (containing the detailed information needed to reproduce earlier attacks) proved mostly futile.

The analysis confirmed the vulnerabilities from earlier reports, as well as discovering numerous new vulnerabilities in the process. Additionally, the EVEREST study had access to Premier equipment not studied in California, and the researchers had access to hardware and source code simultaneously, which was not the case for the California review. As with the ES&S study, they found failures to protect data integrity, failures to protect against malicious insiders, failure to provide trustworthy auditing, and the presence of unsafe features and practices. Specific vulnerabilities found included firmware replacement, recovery of erased files violating voter privacy, password bypasses, management interface access, back-end security software circumvention, forgeable audit logs, and testing functionality included in production equipment.

Enck finished the presentation with lessons their team had taken away from the study. These included the importance of performing sanctioned, open studies of voting systems and the difficulties faced in doing so in the current political climate; the importance of time to perform the studies (since the rate of discovery was increasing when the study came to an end); the helpfulness of independent confirmation of earlier studies; and need for simultaneous access to source code and the equipment to run it on. The key takeaways for the audience were that having a specific list of vulnerabilities in current systems is not enough, more understanding of how the systems are broken is needed to protect against future failures, and the situation is worse than previously thought. There were several questions from the audience about the differences between the EVEREST report and the earlier California study and the amount of access to confidential material provided to follow-up studies. An author from the ES&S team commented that the confidential annex to their report could be reproduced in far less time than would be needed to obtain it.

CRYPTOGRAPHIC VOTING SYSTEMS

Summarized by Eric Cronin (ecronin@cis.upenn.edu)

- ***Analysis, Improvement, and Simplification of Prêt à Voter with Paillier Encryption***
  Zhe Xia, Steve A. Schneider, and James Heather, University of Surrey, U.K.; Jacques Traoré, France Telecom, Orange Lab

The second session began with a talk on an improved cryptographic voting scheme that solves an information leakage problem in an earlier version of the scheme, Prêt à Voter with Paillier Encryption (PAV-Paillier). The authors introduce a model for an information leakage and analysis approach. The modified PAV-Paillier has the additional advantage of being simpler without degrading any of the security properties. Instead of going into the cryptographic details of their solution, the talk instead focused on the information leakage model and its application.

The information leakage attacks that the authors are interested in modeling are those that allow for coercion. The model comprises transitive relationships between voter and results and any intermediate items such as ballots or receipts. If a transitive link between voter and result can be established, then information leakage exists. An example given was that, for a simple handwritten ballot, there is a relationship voter => ballot, through recognizable handwriting, and then ballot => result, again through the handwriting.

Under this model, there are several interesting cases: voting machines can always create ballot => result, so it is crucial to prevent voter => ballot. Similarly, if a receipt exists, then receipt => ballot must be prevented, since voter => receipt is always possible. It is this second case for which several attacks to the PAV-Paillier scheme are identified. In addition to preventing receipts from being linkable to ballots and the aforementioned simplification, the proposed improvement also fixes shortcomings in PAV-Pallier such as the inability to alphabetize candidates on the ballot or hold ranked elections.

- ***Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes***
  David Chaum; Richard Carback, University of Maryland, Baltimore County; Jeremy Clark, University of Waterloo; Aleksander Essex, University of Ottawa; Stefan Popoveniuc, The George Washington University; Ronald L. Rivest, Massachusetts Institute of Technology; Peter Y.A. Ryan, University of Newcastle upon Tyne; Emily Shen, Massachusetts Institute of Technology; Alan T. Sherman, University of Maryland, Baltimore County

Aleksander Essex presented the Scantegrity II voting system. Currently, election verification focuses on two places: the casting of ballots and the counting of ballots ("collected as cast, counted as collected"). Missing from that equation is verification of the integrity of ballots during the time between casting and counting. Scantegrity II is a system to provide end-to-end verification for elections using traditional optical scan ballots. Scantegrity II allows a voter to verify that his or her ballot has been included in the set of tallied ballots and that the vote marked on the ballot matches the vote made in the polling booth.

A powerful feature of Scantegrity II is that its only impact on the existing optical scan election workflow is the use of specially printed ballots. The casting of votes, tallying ballots, and tabulating the results are all orthogonal to the Scantegrity II verification. This is accomplished by printing a unique confirmation code inside each optical scan bubble, using invisible ink. If the user wants the option of verifying his or her vote later, a special marker can be used to fill in the bubble and, in the process, reveal the code. The code is then written down along with the serial number of the ballot and taken home by the voter as a receipt. The other confirmation codes for candidates not selected remain invisible, which makes disputed votes simpler to handle.

Verification of the voter receipt is enabled by the election officials publishing the verification codes corresponding to the candidate tallied for each ballot. Verification of the count is enabled by publishing a table with a column for each candidate and a protected mapping from each confirmation code to a cell in the table. The cells whose confirmation codes were voted are marked, and the sum of each candidate's column is the vote tally. Finally, using randomized partial checking makes it possible to statistically verify that the confirmation codes verified by the receipts are correctly reflected in the results table.

Questions from the audience focused on the chemical properties of the invisible ink and possible attacks on it. The speaker clarified that the only harm that comes from knowing multiple valid confirmation codes for a ballot is that malicious "denial of confidence" challenges are harder for the elections official to discard quickly. The randomized partial checking would still verify that the ballots were correctly tallied.

- ***Coercion-Resistant Tallying for STV Voting***
  Vanessa Teague, Kim Ramchen, and Lee Naish, The University of Melbourne

The final talk of the cryptographic voting systems session was presented by Vanessa Teague, about an encrypted tallying technique for single transferable vote (STV) elections. STV is the rather complicated scheme used by Australia and Ireland as well as a few other locations. Unlike, for example, the first-past-the-post voting system used in the United States, in STV preferential voting is performed by ranking the candidates in each race in order of preference. Tallying is then performed iteratively, redistributing a ballot's votes as candidates are eliminated from the running.

In common STV elections, having 70 candidates in a race is not uncommon, leading to 70! ($1.1978571 \times 10^{100}$) possible orderings on a voted ballot. Because of this, it is possible to encode a unique fingerprint on a ballot by using a specific ordering of least-preferred candidates (known as the "Italian Attack"). If ballots are made public after the election for

verification, a coercer would be able to check that the ballot with a given fingerprint showed the correct—coerced—votes.

The solution taken to this attack has been to encrypt the votes in such a way that the tally can be performed without decrypting. Previous schemes exist that address most coercion attacks on single-race ballots, but the scheme presented works with multi-race ballots and against stronger coercion attacks.

Each ballot is first transformed into a square matrix with a row and column for each candidate. Each cell in the matrix represents a pairwise preference of the row candidate to the column candidate. A value of –1 indicates that the row candidate is preferred, whereas a 0 indicates the column candidate is preferred. By summing the column for a candidate and multiplying by –1, you can recover the rank from the traditional ballot. Additionally, by adding an eliminated row to the column sums the votes are automatically redistributed to reflect the new ordering. The final step is to take this matrix and encrypt it using something such as exponential ElGamal, which has the property of additive homomorphism. Tallying then takes place using the encrypted matrices for each ballot instead of the cleartext votes. The authors have implemented this scheme and said that for a 30-candidate election and one million voters it required 10,000 PC hours to tally the election and produced a 400 GB audit log of the encrypted ballots.