

Joint Standing Committee on Electoral Matters
Submission No. 187
Date Received 12/8/05
Secretary SD

BARCODING

FOR

SIMPLE, QUICK, CHEAP, SAFE
ELECTIONS

BUT

PRESERVING

MANUAL COUNTING

by Dr. Amy McGrath OAM
amy.mcgrath@optusnet.com.au

12

12

12

12

12

12

12

12

12

12

12

12

12

12

12

12

12

Barcoding for simple, quick, cheap, safe elections but preserving manual counting

by Dr. Amy McGrath OAM 12.8.2005

Barcoding will place responsibility where the Commonwealth Electoral Act intended, on the elector. The elector should only be issued a ballot paper for the address where he/she has lived for one month. Any other address renders the vote invalid. At present the 'nanny-state' role of the AEC requires it to encourage or enforce voter responsibility, which only encourages illegal voting it cannot enforce.

A solution to shift responsibility from a 'nanny-state' has to be simpler, quicker, cheaper, safer and more accurate at all levels of process. A bar-coding solution succeeds. Computerisation does not.

The AEC and the NSW and Queensland Electoral Commissions have already been moving in this direction. All have sent barcoded letters to be presented at polling booths – the AEC in Victorian Council elections. My bar-coding solution takes this a step further. All voters will have a simple alpha-numeric barcoded voting card sent to them in the AEC mail-out after the close of the rolls.

This voting card will be surrendered in proof I have attended the polling booth, the barcode reader will record it. I will be given a ballot paper, and even sign for it on a simple read-only barcode reader. This signal will be despatched by mobile telephone technology to the Divisional Returning Office, which can cover 98.3% of voters – the balance by wireless technology.

No legislative change, and few to the Divisional Operations Manual, will be required.

Division-wide voting will facilitate the solution of the problems it created

1. giant roll – now of 860,000 voters on all tables in all booths
2. multiple voting in the same name
3. multiple voting in different names
4. transport costs including to and from scanning centres

Some Advantages of a barcoding system in elections

Time:

- Less queues
- Finding names in bulky rolls – especially foreign names – in tiny telephone book fonts
- Absent voting by identifying the correct division.
- Postal voting far quicker by scanning in further scrutiny
- Less provisional votes to check (after initial election as voters accept the change)

Accuracy:

- Absent votes no longer informal as often by official error at present
- Voting cards from booths or declaration votes scanned for non-voter & polling statistics.
- Bar coding error one in millions compared to manual mark-up mistakes in crowded rolls.

Savings

- Printing of over 25,000 certified lists of nearly 90,000 names (down to 1 per booth)
- 1-2 less staff in booths. Reduction of 2-3 days in scrutiny of declaration votes = \$450,000
- OPR scanners unnecessary – staff, transport of above lists to and from DRO offices
- Printing declaration forms (voting card enclosed on return)



Glossary

4-State Barcode

The barcode symbology used by Australia Post. The symbology enables the delivery destination and other information to be designated on a piece of mail in a barcode format. The name derives from the fact that the codes are made of four types (states) of bars.

Alphanumeric

A character set containing letters, numbers, and other characters.

ASCII

The character set and code described in the American National Standard Code for Information Interchange, ANSI X3.4-1977.

Bar

A single vertical printed line that forms a part of a barcode. The length of the bar may vary, depending on the value of the bar.

Barcode

A series of bars organised according to specific rules into various symbols. The symbols represent letters, numerals, and other human readable characters.

The characters represented by the bars are a further set of codes, representing a range of sorting rules and other information.

Bar Density

The number of characters that a barcode can represent in a length of 25.4 mm.

Barcode Symbol

A group of bars that represent characters or data elements in a particular symbology.

Bar Format Encoded

Any information string that has been converted from the original alpha or numeric representation to a bar by bar representation. In case of the 4-State barcode it would be a string of 0, 1, 2 or 3's in the appropriate order to represent the information required.

Character

An individual letter, number, or other symbol represented by a group of bars.

Character Set

Characters available for encoding within a barcode.

Contrast

The difference in reflectance between the bars and paper or other material the barcode is printed on.

Customer Barcode

A barcode that can be printed on mail items by Australia Post customers.

Customer Information Field

A part of the barcode that is set aside for an Australia Post customer to use to store their own information. The data contained in the Customer Information Field must comply to the format published for the barcode being used.

Delivery Point Identifier (DPID)

An eight digit number that uniquely identifies a physical point to which Australia Post delivers mail.

Font

A specific size and style of type used by printers.

Format

The physical arrangement specified for a particular barcode symbol.

Format Control Code (FCC)

A two digit number encoded in all barcodes that identifies the fields/Encoding Tables used in the barcode. The FCC provides the 'recipe' for the barcode, enabling the barcode to be decoded.

Opacity

The relative ability of paper or other material to prevent light showing through. Opacity affects the ability of the reader devices to scan barcodes.

Print Contrast

Comparison of reflectivity between bars and spaces.

Pre-sorting

The process of a customer sorting their mail to defined sorting breaks prior to lodgement into the Australia Post network.

Quiet Zone

A zone defined by the distance immediately preceding the first Start Bar, and following the last Stop Bar, and the distances above and below the barcode. This zone must be kept clear of other printing to assist barcode reading.

Reed Solomon Error Correction

A process used to protect a barcode from errors and erasures.

Reflectance

The amount of light reflected back from a surface.

Start/Stop Bars

A pair of bars used for the beginning or end of a barcode that allow the barcode scanner to identify if the printed barcode is upside down.

This prevents the barcode scanner from reading the barcode in the wrong direction. If the scanner identifies the orientation of the barcode by checking the Start/Stop Bars it can then attempt to read the barcode in the correct direction.



“e-Voting: Risks and Opportunities.”

Professor William J (Bill) Caelli, AO
 Asst Dean – Strategy & Innovation and
 Research Leader – Information Security Institute (ISI)
 Faculty of Information Technology
 Queensland University of Technology (QUT)
 Brisbane. Qld.

Phone: 07-3864 2752

Fax: 07-3864 1907

Email: w.caelli@qut.edu.au



6 Mar 2005

Presentation to the H.S. Chapman Society Inc.
 Annual General Meeting and Forum 26, Sunday 6 March 2005
 NSW Leagues Club, 165 Phillip Street, Sydney, NSW, Australia

W. Caelli (QUT)

1

Professor William J (Bill) Caelli, AO

BSc (Hons) N'cle, PhD (ANU), FACS, FTICA, CISM, Sen. MIEEE

Prof Caelli is the **Assistant Dean – Strategy and Innovation** in the **Faculty of Information Technology** at the **Queensland University of Technology (QUT)**, Brisbane, Queensland, Australia. He co-leads the **cyber law and policy** research group in the Information Security Institute (ISI) at QUT which incorporated the **Information Security Research Centre (ISRC)**, a research centre of which he was the **Founding Director** in 1988. He is a member of both the **“IT Security”** and **“Futures”** Expert Advisory Groups (EAG) to Australia's Critical Infrastructure Advisory Committee (**CIAC**) established under its Federal Government sponsored Trusted Information Sharing Network (**TISN**). He has over 42 years of experience in the IT industry, with some 30 years involvement in information security and cryptography. He founded **ERACOM Pty Ltd** in 1979, a company that develops and markets advanced, integrated cryptographic systems and information security products around the world, having started with the creation of secure high performance micro-computer systems based upon the Stanford University Network (SUN) workstation architecture. These products and systems particularly address the needs of the banking and finance industries worldwide. He worked with both **Hewlett-Packard** and **Control Data Corporation** in the 1970s both in Australia and in the USA. He received his PhD in Nuclear Physics from the **Australian National University (ANU)** in 1972.

He is a Fellow of the Australian Computer Society and the Institute for Combinatorics as well as being a Senior Member of the IEEE. In 2002 he was presented with the **Kristian Beckman Award** by Technical Committee 11 of IFIP, the International Federation for Information Processing based in Vienna, Austria, for his international work in information security and received the **Pearcey Medal** in September 2002 for his lifelong work in and contributions to the IT industry. He is a Board Member of the USA's **Colloquium for Information Systems Security Education (CISSE)**. Computerworld Australia has designated him as a **“Computer Pioneer”**. In September 2003 he was made an Honorary CISM by **ISACA**, the international information security association. He was made an **Officer in the Order of Australia (AO)** in the January 2003 Australia Day honours list.

Professor Caelli's research and education interests lie in trusted computer systems and networks, cryptography and its integration into systems as well as in the legal, social and political implications of information security and related matters.

“e-Voting: Risks and Opportunities.”

Professor William J (Bill) Caelli, AO
Asst Dean – Strategy & Innovation and
Research Leader – Information Security Institute (ISI)
Faculty of Information Technology
Queensland University of Technology (QUT)
Brisbane. Qld.

Phone: 07-3864 2752 Fax: 07-3864 1907
Email: w.caelli@qut.edu.au



Presentation to the H.S. Chapman Society Inc.
Annual General Meeting and Forum 26, Sunday 6 March 2005
NSW Leagues Club, 165 Phillip Street, Sydney, NSW, Australia

6 Mar 2005

W. Caelli (QUT)

1

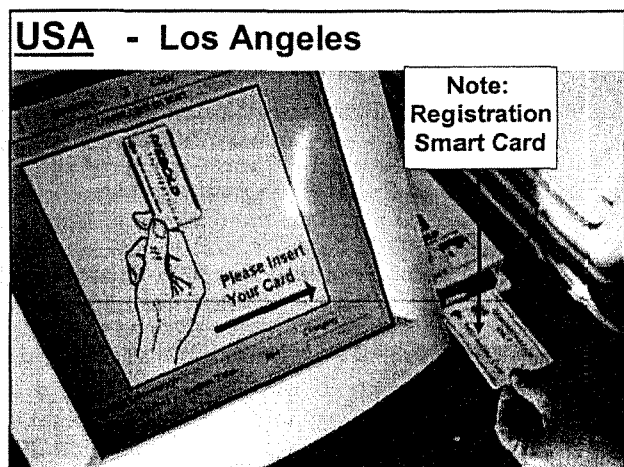
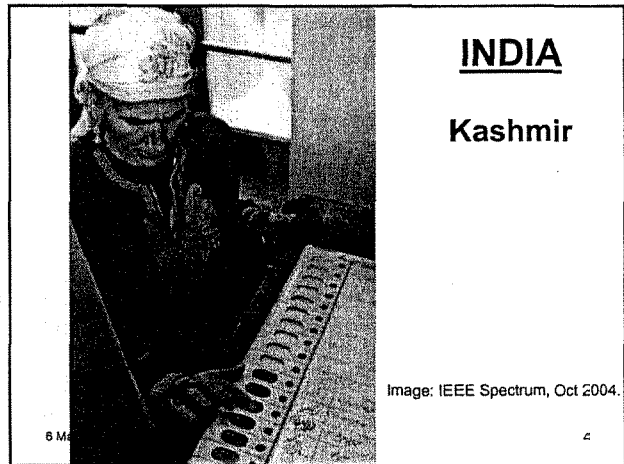
“e-Voting: Risks and Opportunities.”

- Overview – It’s happening!
- Case Study – India
- Voting Considerations for E-Voting Systems
- Developments in E-Voting
- ISI at QUT
- Summary and Conclusions

6 Mar 2005

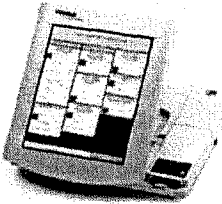
W. Caelli (QUT)

2



Australia


eVACS system used since 2001



6 Mar 2005 W. Caelli (QUT) 7

"... for the first time in history, more than 25 percent of U.S. ballots will be cast using equipment that directly records votes only on electronic media, such as chips, cartridges, or disks, with no paper or other tangible form of backup Twenty-five years in the making, electronic voting is finally being widely adopted in the United States."


Cherry, S : "The Perils of Polling"
IEEE Spectrum, October 2004



6 Mar 2005 W. Caelli (QUT) 8

"... in their hurry to eliminate paper and avoid another Florida-style fiasco, some equipment makers and election officials are rushing to deploy systems that have known flaws or that have been poorly tested – or not tested at all. Much the same story is playing out not only in the United States but also in Australia, Brazil, India, the United Kingdom, Venezuela, and elsewhere."

Cherry, S : "The Perils of Polling"
IEEE Spectrum, October 2004.



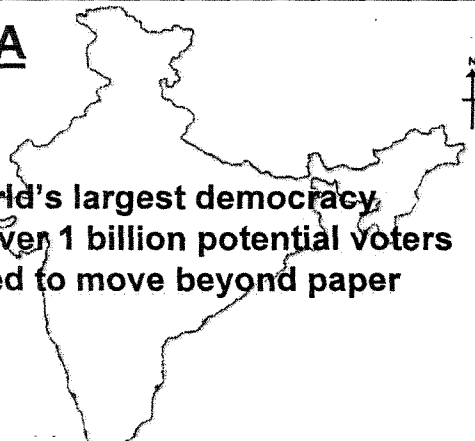
6 Mar 2005 W. Caelli (QUT) 9

Case Study

India
February 2005.

6 Mar 2005 W. Caelli (QUT) 10

INDIA





- world's largest democracy
- over 1 billion potential voters
- need to move beyond paper

Objectives

- Not Changing the Basic Logistics of the existing Election process.
- Reasonably enough administrative procedure in place to avoid Machine based tampering
- No Invalid Vote
- PAPER LESS
- Reusable
- Deterrence for Booth Capture

India

Top: Ballot paper awaiting despatch
Bottom: EVMs in store room

Genesis and Evaluation of Voting Machine

- Concept of Electronic voting conceived in 1976 in ECIL.
- Development of prototype model in 1978.
- Trial of EVM in 1980 in ECIL for office bearer elections.
- Demonstration of the machine to the Election Commission & political parties.
- Trial Election by Election Commission of India in 1982 in Parur, Kerala in 10 polling stations (Subsequent Court Case demanded legal bill for EVM from Parliament).



Top: Ballot box being carried to the polling station
Bottom: EVMs being carried to the polling station

6 Mar 2005

W. Caelli (QUT)

13

Genesis and Evaluation of Voting Machine

- Revised the specifications based on feedback in trial election.
- Successful deployment of EVMs in Shadnagar Legislative Assembly, Andhra Pradesh election held in 1983.
- Final SRS for bulk production of the machines with following criteria was taken up.



Voters waiting to cast their vote

6 Mar 2005

W. Caelli (QUT)

14

Genesis and Evaluation of Voting Machine

- Final SRS for bulk production of the machines with following criteria was taken up.
 - Ruggedness and reliability of the design
 - Manufacturability of the design
 - Low power consumption as the unit is battery powered.
 - Ease of installation, operation and understanding by various polling officials.
 - Tamper-proof
 - Use of state-of-art components and technology
 - Prof. Indiresan committee to review technical aspects
 - Committee cleared for bulk production



Voting the Ballot box way



Voting the EVM way

6 Mar 2005

W. Caelli (QUT)

15

Genesis and Evaluation of Voting Machine

- First lot of 75,000 machines were produced in 1989-1990
- Legislative amendment to use election gadget in general elections
- Deployment of machines for bye elections and state elections during 1994-1999.
- Improvements incorporated in the design like dual memory
- Procurement of total machines required for the country 1999-2004
- Deployment of machines in general elections through out the entire country (one million machines) in 2004



EVM being demonstrated to VTPs



EVM being demonstrated to the press

6 Mar 2005

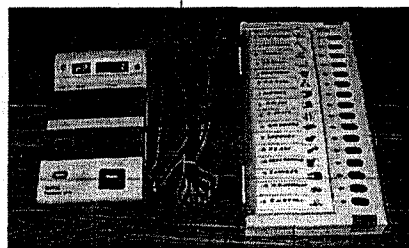
W. Caelli (QUT)

16

EVM (Electronic Voting Machine)

India

Interconnecting Cable



Control Unit

Balloting Unit

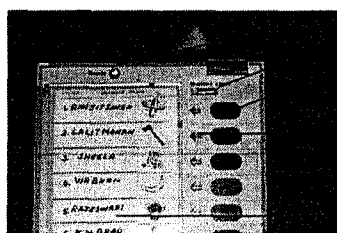
6 Mar 2005

W. Caelli (QUT)

17

Balloting Unit - Details

India



Ready Lamp
Slide Switch Window
Candidate's Button

Candidate's Lamp

Ballot Paper Screen

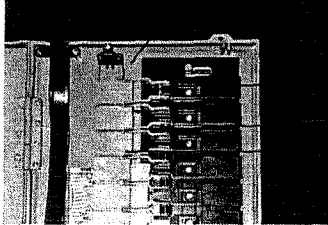
6 Mar 2005

Description

W. Caelli (QUT)

18


Balloting Unit - Internal parts



- Ready Lamp
- Slide Switch
- Candidate's Button
- Masking Tab

6 Mar 2005 Description W. Caelli (QUT) 19

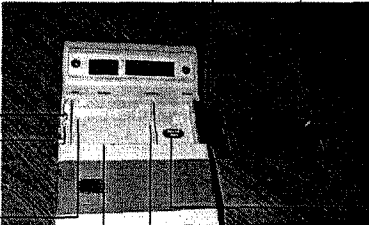
Control Unit



- ON Lamp
- Display Section
- Ballot Section
- Total Button
- Busy Lamp
- Candidate Set Section
- Result Section
- Ballot Button

6 Mar 2005 Description W. Caelli (QUT) 20

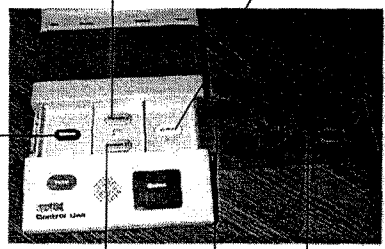
Control Unit - Candidate Set Section



- Candidate set section inner door
- Candidate set section outer door
- Provision for thread seal
- Latch
- Power pack compartment
- Plug for power pack
- Provision for Thread seal
- Candidate set button

6 Mar 2005 W. Caelli (QUT) 21

Control Unit - Result Section



- Result I button
- Clear button
- Close button
- Result II button
- inner latches
- Frames for Paper seal

6 Mar 2005 W. Caelli (QUT) 22

Intrinsic Security Weaknesses

- Concerns about the people behind the machines
- Doubts about the accuracy and integrity of e-voting equipment
 - Hackers could enter Vote Database using third-party applications and change votes without leaving a trace
 - Possibility of Data transfer and altering the memory data

6 Mar 2005 W. Caelli (QUT) 23

Intrinsic Security Weaknesses

- Election glitches
 - Machines fail to boot up
 - Fail to record votes or even record them for the wrong candidates
- Computer scientists say the machines are easy to hack
- Voting machine employees could be implicated in bribery or kickback schemes involving election officials

6 Mar 2005 W. Caelli (QUT) 24

Intrinsic Security Weaknesses

- Partisan loyalty of election executives
- Right to vote is useless as long as one has no way of verifying the vote is recorded accurately

6 Mar 2005

W. Caelli (QUT)

25

Information Security & Integrity

- EVMs are stand alone battery operated units
- EVM consists of
 - Control Unit
 - Ballot Unit
- The firmware is masked in a microcontroller in the Control Unit & Ballot Unit.
- This embedded firmware is cannot be read/altered/reprogrammed/tampered.

6 Mar 2005

W. Caelli (QUT)

26

Information Security & Integrity

- Encrypted Voting data storage with Digital signature provided during the factory programming/manufacturing.
- Validation/comparison of memory banks while result computation.
- Encrypted data communication between Control Unit & Ballot Unit.

6 Mar 2005

W. Caelli (QUT)

27

Voting Overview for E-Voting Consideration

6 Mar 2005

W. Caelli (QUT)

28

Introduction - voting

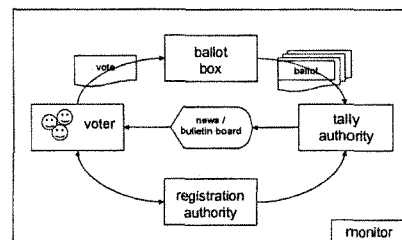
- Fundamental decision-making tool in any consensus-based society
- Applications from reality television shows to national election
- Security is essential to ensure result is: correct, honest, private, containing true opinions
- Voting is changing from paper-based to electronic

6 Mar 2005

W. Caelli (QUT)

29

Introduction - voting procedure




6 Mar 2005

W. Caelli (QUT)

30

Introduction - **electronic voting**

- Motivation: convenient, efficient, accurate (less human error), lower cost (less administration)
- Optical mark-sense, touch mobile/handheld devices,  the Internet, ...
- More features and security compared to traditional paper-based systems ?!?

6 Mar 2005

W. Caelli (QUT)

31

Introduction - **fundamental questions**


1. Can you ever be certain that the voting result is correct?
2. Can you ever be certain that your vote was counted correctly?

6 Mar 2005

W. Caelli (QUT)

32

Voting Security - **threats**


- Motives: political, financial, personal gain
- Possible dishonest entity: developers, vendors, authorities, voters, external entities,
- Equipment failures/glitches
- Cheating: vote buying/selling, intimidation, unauthorised voting, double voting, corrupt authorities, ... 

6 Mar 2005

W. Caelli (QUT)

33

Voting Security - **requirements (1/2)**


- Accuracy: voting result must reflect correct tabulation of ballots
- Privacy: voter-vote relationships must be kept private
- Receipt-freeness: there must not be a receipt proving the content of the vote 
- Eligibility: only authorised voters are allowed to vote

6 Mar 2005

W. Caelli (QUT)

34

Voting Security - **requirements (2/2)**

- Prevention of double voting: each voters is allowed to vote only once
- Fairness: no partial tally is revealed before the end of the voting period
- Robustness: able to tolerate certain faulty conditions and manage some disruption 
- Verifiability / accountability: correct voting process must be verifiable

6 Mar 2005

W. Caelli (QUT)

35

DEVELOPMENTS IN E-VOTING

6 Mar 2005

W. Caelli (QUT)

36

E-Voting Development

- Trust issues: partisan developer
- Software engineering principles and coding standards
- Independent and impartial testing
- Thorough inspection and certification using international evaluation standard
- Secure development environment
- *Standardised cryptography endorsed by experts*

6 Mar 2005

W. Caelli (QUT)

37

System Deployment

- Physical and logical security
- Public acceptance
- Legislation, political issues
- User awareness
- Purchase, roll-out, training and maintenance cost

6 Mar 2005

W. Caelli (QUT)

38

Cryptographic Voting Protocols

- Allows formal security analysis of the system (verifiability)
- Revolves around the privacy of the voter-vote relationship
- Two categories of protocol
 - Use homomorphic encryption and never decrypt individual votes
 - Use mix network and decrypt all votes

6 Mar 2005

W. Caelli (QUT)

39

E-voting prospects

- Increased use inevitable
- Security requirements are complex
- System must be designed, developed, and deployed securely
- Cryptographic protocols, and international standards and certification must be followed
- A specific standard for e-voting implementation is required

6 Mar 2005

W. Caelli (QUT)

40

INFORMATION SECURITY INSTITUTE (ISI)

6 Mar 2005

W. Caelli (QUT)

41

Research at QUT's Information Security Institute

- Collaborative research institute emphasising interdisciplinary projects:
 - Faculty of Built Environment and Engineering
 - Faculty of Business
 - Faculty of Information Technology
 - Faculty of Law



6 Mar 2005

W. Caelli (QUT)

42

Aims

Conduct multi-disciplinary research to answer information security, information protection and technology policy challenges that confront business, government and the community as a whole

- 41 Researchers
 - 13 Professors
 - 5 Associate Professors
- 89 postgraduate research students

6 Mar 2005

W. Caelli (QUT)

43

Eight Domains

- Cryptology
- E-Business and E-Government
- Technology, Law and Policy
- Governance and Information Protection
- Network Security and Trusted Systems
- Computer Intrusion, Forensics and Evidence
- Biometric Person Authentication
- Social and Behavioural Issues

6 Mar 2005

W. Caelli (QUT)

44

E-Voting Research at ISI

- Aims to providing more security and flexibility
- Decrease trusted entities, increase verifiability
- Focuses on cryptographic protocol designs, essential foundation to a secure system
 - Mix networks
 - Homomorphic encryption
- Papers at international conferences in China, Australia, Spain and India

6 Mar 2005

W. Caelli (QUT)

45

SUMMARY AND CONCLUSIONS

6 Mar 2005

W. Caelli (QUT)

46

THREATS AND PROMISES

- certification of equipment
- validation of equipment design and manufacture
- paper (printer) vs electronic only (no paper)
- addressing the "enrolment" problem

Note:
Evaluated products under "Common Criteria" / IS 15408
through DSD EPL
(See: <http://www.dsd.gov.au>)

6 Mar 2005

W. Caelli (QUT)

47

THREATS AND PROMISES

- installation
- repair
- operation
 - "boot-up"
- vote count consolidation
 - telecommunications
 - denial-of-service

6 Mar 2005

W. Caelli (QUT)

48

THREATS AND PROMISES

- audit
 - fact/record of voting
 - anonymous
- validation of count
 - trust
- acceptance
 - scrutineers
 - general public
 - media

6 Mar 2005

W. Caelli (QUT)

49

THREATS AND PROMISES

- better (worse) than manual processes?
- higher accuracy – potential (at least)
 - ATM's work and we like/trust them !
- acceptability by a PC/Internet literate generation
- conquering distance – Internet voting?
 - not there yet

6 Mar 2005

W. Caelli (QUT)


50

THANK YOU.....**Useful references / websites:**

The Perils of Polling, IEEE Spectrum, October 2004

Verified Voting Foundation

<http://verifiedvoting.org>


 verifiedvoting.org

Questions ?

6 Mar 2005

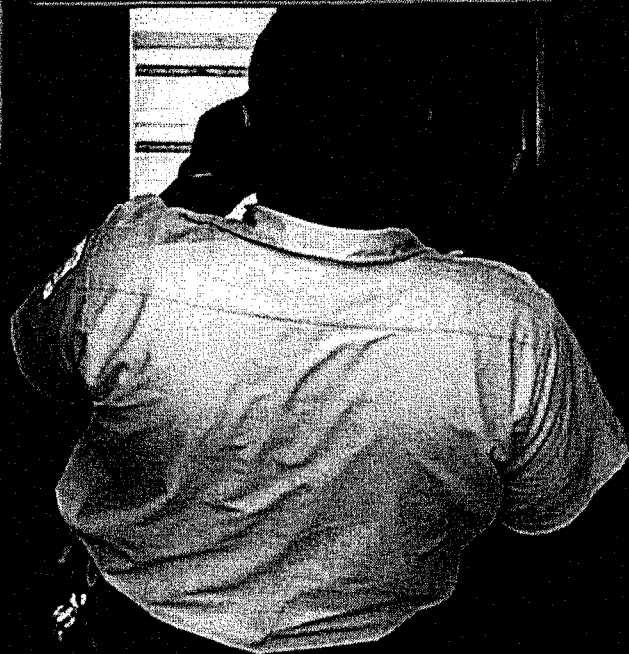
W. Caelli (QUT)

51



EYE OF THE STORM? In the wake of the 2000 U.S. presidential election, Florida's counties turned to electronic voting. Here, Miami voters use new machines made by Election Systems & Software in the November 2002 general election.

THE PERILS OF POLLING



Electronic voting may avert a repeat of the 2000 Florida debacle, but it also creates new problems **BY STEVEN CHERRY**

This November, people all over the United States will cast ballots using methods that span centuries of technological development. In fact, in this technologically advanced country, more than half of the voters will mark their choices by hand on paper ballots, just as their great-great-grandparents may have done.

But for the first time in history, more than 25 percent of U.S. ballots will be cast using equipment that directly records votes only on electronic media, such as chips, cartridges, or disks, with no paper or other tangible form of backup. That's nearly triple the number of electronic votes in 2000. Twenty-five years in the making, electronic voting is finally being widely adopted in the United States.

Unfortunately, recent evidence suggests that although we may be ready for electronic voting, the technology is not ready for us.

True, these electronic systems eliminate many of the problems with paper-based ballots—Florida's hanging chads and poorly aligned print layouts being the most notorious. But in their hurry to eliminate paper and avoid another Florida-style fiasco, some equipment makers and election officials are rushing to deploy systems that have known flaws or that have been poorly tested—or not tested at all. Much the same story is playing out not only in the United States but also in Australia, Brazil, India, the United Kingdom, Venezuela, and elsewhere.

Officials are knowingly giving up the ability to perform an independent recount—a fundamental requirement for ensuring the integrity of the votes recorded by a voting machine, and for reconstructing the tally if an election is contested. People using these direct-recording systems will have no assurance that their ballots were cast at all, let alone as intended. And it's likely that some machines will fail, if the record of recent local and other elections is any guide.

Astonishing as it may seem, a world with automated teller machines that dispense cash flawlessly and ticket-selling kiosks that accept and count bills and coins of every denomination still hasn't produced electronic voting machines that are robustly

reliable and with counts independently verifiable. Computer scientists, such as David Chaum, the inventor of digital cash, are working on the problem, but solutions are years away.

Fair and honest elections are a cornerstone of any modern democracy, and yet the democracies that dominate technology development—the United States chief among them—have been surprisingly unsuccessful to date in their attempts to design and deploy electronic voting machines that are free of fundamental defects. This situation is all the more amazing when you consider that over the past couple of years the U.S. government has spent some US \$1 billion and allocated almost \$3 billion more to subsidize the purchase of new electronic voting machines. Despite this enticement, some 20 percent of U.S. election districts have chosen to continue using their existing systems, including some 1950s-era lever machines that were used to vote Dwight D. Eisenhower into the White House.

Now, as the United States prepares for the first presidential election in which electronic voting will play a substantial role, a growing group of technologists is asking whether the problems of electronic voting are endemic. States getting ready to deploy machines are finding that they have been sadly ill informed about them—and that in some cases they will be fielding systems that comply only with obsolete federal guidelines from 1990.

WHY HAS SUCH A SEEMINGLY STRAIGHTFORWARD design challenge proved so baffling? The causes are several—putting together an honest election isn't as simple as it appears. In the United States, one major complication is that elections are run individually by each of the 50 states. Another is the misplaced trust of the state and local bureaucrats responsible for choosing and deploying election equipment; they have been insufficiently skeptical of the claims made by equipment manufacturers—and have in some instances rejected the advice of outside engineers and specialists. Then there's the way the profit-driven vendors themselves rushed some of their machines to market. Finally, there is the system-design challenge itself, which is much more difficult for voting machines than most people realize.

Let's start with the practice, which originated in the U.S. Constitution, of entrusting states and smaller jurisdictions with the responsibility for buying election machines and running elections, including national ones. Many countries, such as India and Brazil, have central election authorities that choose machines for the whole nation.

The United States doesn't have just 50 different decision makers; it has hundreds. Some states choose voting equipment statewide, while others leave such decisions up to counties or municipalities. For years, many voters have been using systems that are partially electronic. Voters fill out a paper ballot that will be optically scanned, much as a standardized test is. Machines count the ballots and a winner is announced. If an election is contested, the ballots can be rescanned or counted by hand.

Electronic voting machines go one small but critical step further by storing the vote digitally instead of on paper. The AccuVote-TSX, a touch-screen system made by Diebold Inc., North Canton, Ohio, is typical. When a voter signs in at the local polling station, a card similar to a modern hotel-room key is activated. The voter inserts it into the machine and makes his selections. When the voter touches a "Cast Vote" area on the screen, the vote is recorded on the machine's hard disk and the access card is deactivated, preventing the voter from voting a second time. Each AccuVote machine has a built-in printer, not to reproduce individual ballots but to record the machine's vote totals when the polls close. The AccuVote also has a modem; election

officials can choose to have it encrypt the vote totals and transmit them over ordinary phone lines.

Though there are at least a dozen manufacturers of electronic voting machines, the three largest—Diebold; Election Systems & Software Inc., Omaha, Neb.; and Sequoia Voting Systems Inc., Oakland, Calif.—share 80 percent of the market.

ES&S, which claims to be the largest maker of electronic voting machines in the world, was formed in 1997 by a merger of two smaller companies, one of which was founded by two brothers, Todd and Bob Urosevitch. Todd is still with ES&S, but Bob was until recently president of Diebold.

Electronic voting machines have some important advantages over traditional optical-scan systems and their preprinted ballots. For example, machines can be programmed to keep the voter from voting for two candidates for a single office. And text on the screen can be read by voice-synthesis software—useful for illiterate voters as well as the visually impaired. These and other special features are continually refined by the different vendors.



A TOUCH OF GLASS: A voter in Los Angeles tries out a touch-screen electronic voting machine in early voting for a March 2004 primary election [above]. Nearly 16 000 machines made by Diebold Inc. were decertified by the California secretary of state in April, after it was revealed they had been installed without having met the state's certification requirements.

Millions around the world are now using electronic voting machines. A Kashmiri woman, one of more than 600 million eligible voters in India, votes in an April 2004 general election [right]. And a Caracas resident tests Venezuela's new machines in July, in advance of the country's August 2004 presidential referendum [far right].

The diversity of manufacturers and machines is a problem, though, because voting officials are having a hard time keeping up with a shifting cast of companies and with often-flawed, early-generation equipment. Time-consuming testing and certification requirements can't keep up now that elections are suddenly under the force field of Moore's Law. And then there's the problem of springing new machines on the many one- or two-day-a-year volunteer workers needed to run a modern election. The inevitable result is compromised elections.

THE NUMBER OF PROBLEMS IN RECENT YEARS defies listing in a magazine article, but what better place to start than Florida, whose tribulations made the 2000 presidential election infamous? Just two years later, in a 2002 gubernatorial primary, a state of emergency had to be declared because, in two counties, some of the new equipment failed to boot up in time for the start of the election. Or we could start with a November 2003 election in Boone County, Indiana, where 144 000 votes were reported for only 5352 voters.

Or perhaps we should begin with California, which has endured a plenitude of problems commensurate with the state's size and population. Indeed, election officials in California

soured on their new e-voting machines only after a lengthy series of missteps culminated in spring 2004 primary elections that were marred by voting catastrophes throughout the state, across a wide variety of different machines.

In San Diego County, precincts opened as much as 4 hours late; in some areas nearly half failed to open on time. Here and there, voting machines, made by Diebold, rebooted themselves and voters saw generic Microsoft Windows screens instead of ballots. Those problems were traced back to the voter access card encoders. Faults in the power switches drained them of battery power. In northern Alameda County, one in five Diebold encoders had similar problems.

Hearings were held after the primary elections, and on 20 April, California Secretary of State Kevin Shelley released a report charging that Diebold marketed, sold, and installed its AccuVote systems in Kern, San Diego, San Joaquin, and Solano counties prior to full testing, prior to federal qualification, and without complying with the state certification requirements. These and other discov-

lion electronic voting machines in its national election this past spring, eliminating the need for 8000 tons of paper ballots. The BBC and CNN claimed the equipment, produced by two government-owned companies, Bharat Electronics Ltd. and the Electronics Corporation of India Ltd., led to a reduction in the violence common to elections there, yet local papers were "full of reports of thugs taking away voting machines and tampering with booths," according to The Associated Press. [See also "Electronic Voting Eases India Elections," IEEE Spectrum Online, 10 May 2004.] Revoting was required at 1879 stations, and it is unclear whether tampering contributed to the surprising Congress Party victory.

In Ireland, plans to use electronic voting in local and European parliamentary elections in June 2004 were scuttled, partly over concerns about the lack of independent auditability. Also, constant updates by its vendors—Nedap NV, Groenlo, the Netherlands, and Powervote Ltd, Wisteria, England—meant that the software could not be reviewed in a timely fashion. Nedap recently made some of its online e-voting software, used in



eries were subsequently turned over to the California attorney general's office for possible criminal investigation against Diebold.

Ten days later, Shelley issued a controversial decertification notice, withdrawing approval for all direct-recording electronic voting systems in California, deeming them defective or unacceptable. Because of this, the state required nearly 16 000 AccuVote machines in the four counties involved to be recertified to comply with tighter security and auditability measures or replaced with optically scanned balloting in time for next month's election.

PROBLEMS RELATED TO THE INSTALLATION OF UNCERTIFIED COMPONENTS and the coverup of malfunctioning products have occurred with manufacturers other than Diebold. Earlier this year, a June 2003 ES&S memo came to light that indicated flaws in the auditing software for a \$24.5 million installation of its iVotronic voting machines in Miami-Dade County, Florida. ES&S also manufactured voting systems previously used in Venezuela (sold through Indra Sistemas SA, Madrid, Spain) that suffered a 6 percent malfunction rate in actual use.

Indeed, electronic voting has had its share of problems outside of the United States as well. India deployed more than a mil-

Netherlands elections, available as open source, but critics have noted that the released code set cannot be compiled and run, nor is it possible to verify that the code that runs during the election is identical to what was released for review.

Physically securing a system's hardware and software was also a problem in Fairfax County, Virginia, where 1 percent of the county's new WINvote touch-screen machines, made by Advanced Voting Solutions Inc., of Frisco, Texas, had serious malfunctions. Some of the machines were repaired outside the polling place and then returned to the precincts and put back in use, despite the fact that security seals had been broken or removed—in apparent violation of state law.

Worse, at day's end, about half of the vote totals couldn't be electronically transmitted to the county headquarters because the system flooded itself with messages, in effect creating its own denial-of-service attack on the server. One election for the school board was particularly flawed. A still unexplained anomaly in a number of machines apparently subtracted votes from Republican school board candidate Rita S. Thompson, resulting in a possible miscount of 1 percent or 2 percent of her votes—close to the margin by which she lost the election.

There were known problems with the WINvote machines. The Web site for the electoral board of nearby Arlington County even included instructions for poll workers on what to do if: the “voting machine freezes during boot-up,” the “master unit does not ‘pick up’ one of the units in the polling place when opening the polls,” or “when closing the polls, the tally fails to pick up a machine.”

Knowledgeable advice had been offered and spurned. Information-security expert Jeremy Epstein gave Fairfax officials a three-page list of questions after he attended a pre-election training session. A letter from Margaret K. Luca, who was then electoral board secretary, said that she couldn't respond on the grounds that “release of that information could jeopardize the security of that voting equipment.” Critics say that Epstein's experience is typical of the way in which the election community has shut out scientists and engineers and made it impossible to independently test electronic voting systems.

THE SPORADIC EXCLUSION of technologists and academics is especially unfortunate because the design of electronic voting machines is far more difficult than most people—election officials included—realize. At the core is the selection and counting process, which at face value appears simple: here are the candidates, pick one. In fact, the machines must also be able to handle votes for candidates not on the ballot (so-called write-ins) or more than one candidate (when voters choose, say, two out of a list of five people running for council), and “none of the above.” The bigger problem, though, is anonymity.

Voting systems must never link an individual to his or her vote, or else it would be possible for the voter to sell a vote or a politico to coerce one. In short, voting machines need to produce transactions that are auditable. Officials need to be able to recount ballots, trace problems, and eliminate errors. All the while, they must never be able to identify who created which ballot. This problem has engaged some of the brightest minds in computer science and mathematics for a few years now, with no agreement yet about how it can best be solved.

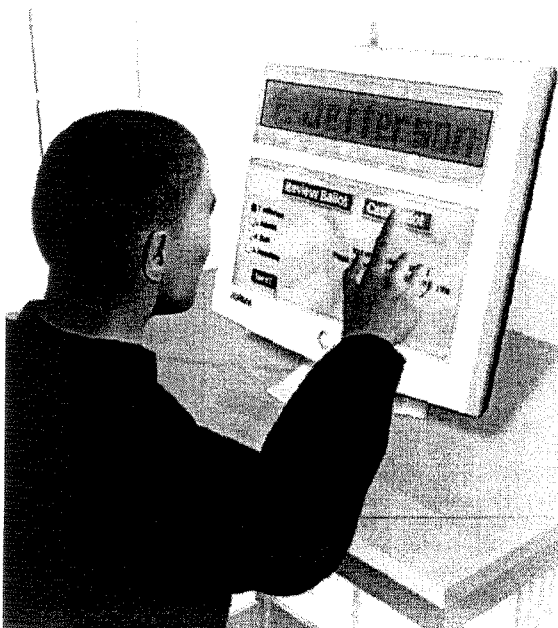
Another big challenge, mentioned above, is independent verifiability. California, for example, audits all its elections by requiring that 1 percent of all paper ballots be manually recounted, whether or not an election is contested. But without the paper, such recounts are not possible. As unpleasant as the Florida 2000 election was, at least there was paper to recount. With paperless electronic voting, on the other hand, a catastrophic malfunction, such as a memory-wiping freeze, can irretrievably lose all the votes collected by the machines.

To date, efforts to add verifiability have focused on adding paper back into the process. In fact, a paper ballot serves two key roles. It gives election officials something to recount in a contested election. In addition, when voters mark—or at least get to look at—a paper ballot when voting, they can be sure the ballot correctly represents their intended votes. Getting electronic voting machines to generate this so-called voter-verified paper audit trail is a key goal of many critics of the current technology. [See, for example, “A Better Ballot Box?” by Rebecca Mercuri, *Spectrum*, October 2002.]

A GLIMMER OF HOPE

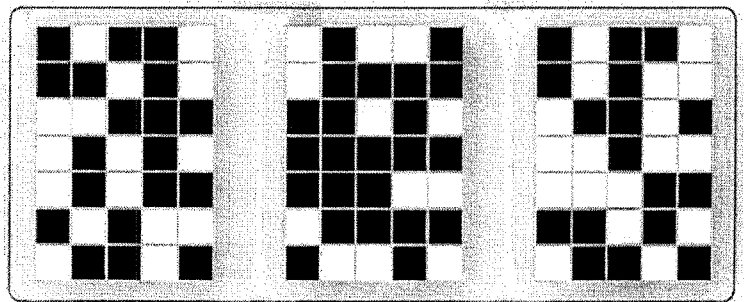
Cryptographer David Chaum's approach to electronic voting could lead to transparently verifiable, unhackable elections.

1 In the booth, the voter chooses from the ballot using an electronic device, such as a touch screen [below].

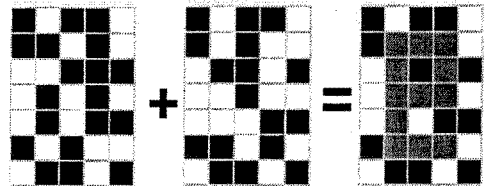


2 As the voter chooses a candidate, the name of that candidate is projected on a special small screen at the top of the display.

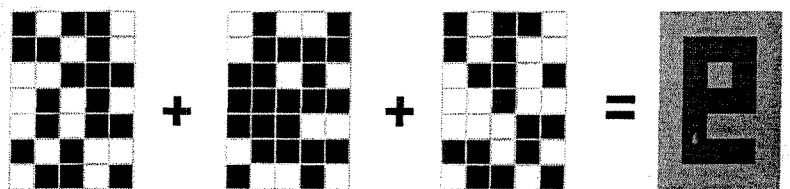
3 The candidate's name on the small screen is formed by projecting in superposition the “tiled” pattern from three doubly encrypted strips printed in the machine by a thermal printer after each choice is made. Two of the strips are black and white only. Each is an encrypted version of the voter's selection. The third strip, needed only to enhance readability, contains blue as well as black and white tiles. Shown here are tiles coded for the letter “e.”



4a It's possible to form the “e” by superimposing only the two black and white strips. The letter “e” then shows up in gray, but the background is a distracting pattern of black and white tiles.



4b When all three strips are superimposed, the result is much more readable: the black and white background becomes gray and the letter “e” appears in blue.



The electronic tally stored in the machine can be taken to be the official vote; in this case the separately printed ballots are scanned only when an election is contested. Alternatively, the paper ballots can be scanned immediately, and that result is the official one. In either event, if something goes wrong with the election, the paper ballots can then be counted, and recounted—by hand if necessary.

Next month, Nevada will use electronic voting machines made by Sequoia that produce paper ballots. It will be the first U.S. state to do so, though only in some counties. Unfortunately, the Sequoia machines use a continuous paper roll, so voter confidentiality could conceivably be compromised by matching ballots to the order in which people voted. Simply cutting the roll after each vote and letting the slips of paper fall into a box at random would be an improvement.

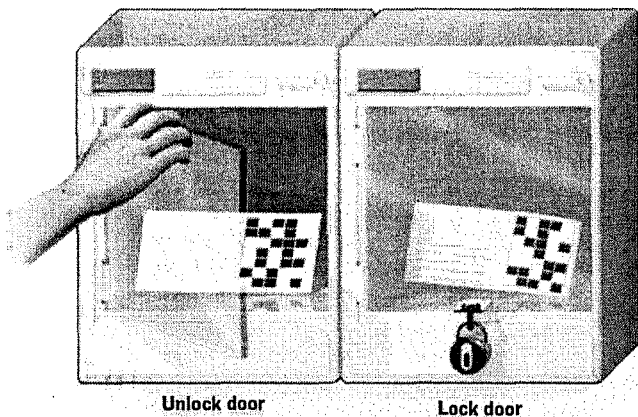
The importance of backing up the electronics with a paper trail was underscored in the 20 April report by California Secretary of State Shelley, in which he mandated the addition of an accessible, voter-verified, paper audit trail for all newly purchased direct-recording electronic systems and a retrofit for existing ones by July 2006.

THESE FUNDAMENTAL ISSUES—how to verify electronic votes, how to test e-voting hardware and software, and how to maintain the security and integrity of e-voting systems—logically fall under the province of legislative authorities and standards bodies. Yet the United States has tied its own hands in this regard.

One logical legislative opportunity was in the language of the Help America Vote Act (HAVA) of 2002, which fueled the rush to electronic voting throughout the United States, with more than \$3 billion to be used by state and local governments to replace their old punch-card and lever systems. An additional \$30 million of HAVA money was supposed to have been allocated to the National Institute of Standards and Technology, Gaithersburg, Md., to support the development of more stringent election system examination criteria than those developed by the Federal Election Commission in 1990 and 2002.

Unfortunately, the NIST funding was not distributed, and technical commission appointments were stalled. Even if a more timely standard had been produced, the cart was put before the horse: receipt of HAVA monies for equipment purchases was not linked to compliance with any new HAVA requirements. As a consequence, no machine currently in use has HAVA certification, since no such certification actually exists, nor, once it does exist, is it likely to be enforceable by 2006, the deadline set by HAVA for all the new systems to be in place.

Although HAVA requires that newly purchased voting units “produce a permanent paper record with a manual audit capacity for such system,” election officials and vendors have let this clause be satisfied by just a paper strip on which vote totals are printed at the end of the election. That strip would be useless if a real recount were required. U.S. Representative Robert Wexler, of election-impaired Palm Beach, Fla., refers to this printed summation as a “reprint” rather than a “recount.”

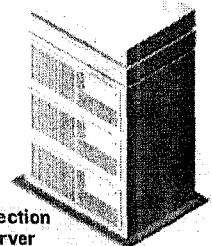


5 When done, the voter is allowed to choose freely which of the two doubly encrypted strips to take as a receipt. After the voter chooses one, the door on the other is locked. (The voter never gets the middle strip, since it shows the vote in clear text.) At the close of the polls, the digital representation of the encrypted receipt that the voter took is posted on an election Web site.

7

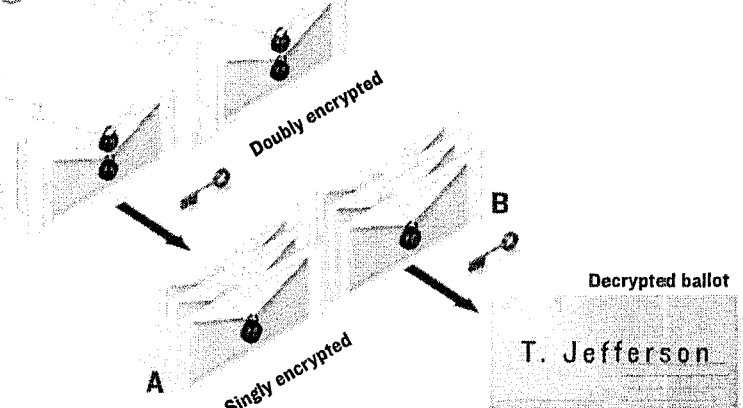
The decrypted votes, exactly what voters saw in the booths on the special screens, are also posted on the Web. To protect ballot secrecy, these are without serial numbers and in a random order.

Actually, three versions of the ballots are posted on the Web: doubly encrypted ballots, singly encrypted ballots, and decrypted ballots.



Election server

8



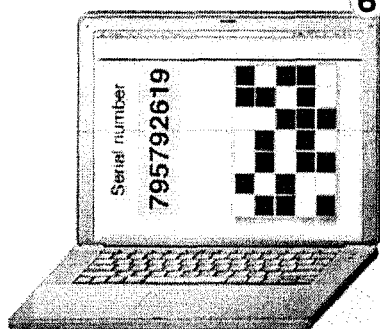
To count the votes, the doubly encrypted ballots on the Web are divided by a random draw into two groups. Decrypting keys are published for one group. The ballots in this group ought to match their counterparts among the collection of singly encrypted ballots stored on the Web (A).

Keys are also posted for the other group of singly encrypted ballots (B). These allow anyone to decrypt, and

reveal, the original alphabetic characters [above], which should match their counterparts among the previously posted collection of unencrypted ballots. A perfect match proves, with mathematical certainty, that no ballot has been tampered with, while the two-stage decryption process, which never used the same ballot in both stages, preserves voter anonymity.

6

The voter can look up the receipt's serial number on the Web and verify that the doubly encrypted receipt is posted there correctly. The voter, or anyone he allows, can verify his vote on the ballot by digitally scanning the ballot or even by spot checking, by hand and eye, the tile pattern on the receipt, matching it to that on the Web. [The pattern shown here is representative and not to scale.]



In the absence of a voter-verified paper audit trail, the security of a voting system rests squarely on there being some kind of certification process. Yet certifying equipment even to the 2002 standard is proving to be problematic, since it is voluntarily adopted by the states, and not all have signed on yet. Only three companies are authorized to perform the commission's examinations, which are paid for by the vendors—an arrangement that many critics say compromises the testing.

Even after a system is certified, election officials must strive to ensure that the system that voters use on Election Day is the same as the system that was tested. Yet federal guidelines don't require any kind of electronic or digital signature to track software from certification to installation (although HAVA commissioners have lately said this would be a good idea).

This security hole and many others were identified by experts several years ago, in comments on the earlier 2002 Federal Election Commission certification guidelines. To address these problems, the IEEE Standards Association had formed a working group on voting standards. The importance of this work was recognized in the HAVA bill, where the IEEE was named as a representative body to the federal Technical Guidelines Development Committee of the U.S. Election Assistance Commission.

The IEEE working group has had its share of controversy, largely over the question of voter-verified paper audit trails. During the fall of 2003, Herb Deutsch, a longtime ES&S employee, was appointed to chair the IEEE Voting Equipment Standards primary working group (P1583), and an attempt was made to push a draft of the standard through the acceptance process.

This first P1583 draft omitted any mention of requirements pertaining to voter-verified paper audit trails. The draft also included what some say is a major security loophole: a blanket exemption for all commercial off-the-shelf components, including operating systems such as Windows or Unix and standard hardware modules such as modems and wireless transceivers. The 2002 Federal Election Commission's guidelines have the same exemption. "The 2002 FEC standard was our starting point," Deutsch notes. "So our first draft was built on that, and we thought major improvements were made."

Protests by IEEE members, academicians, and other concerned individuals led to the submission of more than 1000 specific comments, which have taken nearly a year to resolve. The IEEE new draft does cover the issue of voter-verified paper audit trails, though it does not require them.

Should every electronic voting machine include a paper audit trail? "That's a question of policy," says Deutsch. "This is a requirements standard, it's not a design standard. Policy will be set by governmental agencies. California has made a paper audit trail mandatory, some other jurisdictions haven't, so the standard has to cover both."

Proponents of paper audit trails still fear, however, that if a direct-recording electronic voting machine has no paper output, there will be nothing to audit an election with. Deutsch believes that the standard will have provisions for adequately dealing with security and auditability for direct-recording sys-

tems that don't have a paper audit trail. Even among those who don't agree, there seems to be a growing acceptance of the idea of letting the standard treat paper audit trails as an option, for now. Since the original draft didn't mention paper audit trails at all, proponents can certainly feel some progress has been made. Deutsch, for his part, says that a standard, once it exists, can always be improved, but if the P1583 committee doesn't approve this version in the next few months, the Election Assistance Commission may look elsewhere for a standard.

MEANWHILE, COMPUTER SCIENTISTS continue to argue about whether sufficient auditability can be provided without paper. Certainly, many electronic funds transactions are conducted without paper, using encryption techniques to track the communications. To date, though, no one has come up with the rigorous mathematical proofs necessary to fully justify assertions of their implementation's correctness.

The cryptographer David Chaum, an inventor of electronic cash, among other things, has demonstrated a unique approach to voting and auditing elections, using multiple layers of encryption. Basically, Chaum's system lets election officials post electronic ballots to the Internet. Voters can then check that their votes were included in the election tally. [See diagram, "A Glimmer of Hope."]

Although paper is still needed, Chaum's proposal is important because it is the first system whose electronic tallies are as reliable as a count of the paper ballots, while still preserving voter anonymity. But it is not likely to be adopted soon,

because of its theoretical complexity. It also creates a potential new problem: one of its stages involves using trusted intermediaries to scramble the votes in a way that preserves anonymity. If these third parties were to collude with one another, anonymity could be compromised.

Even after the mathematical problems are solved, fully securing the vote will still require the active involvement of a well-educated and even skeptical citizenry. Voting is a complicated social phenomenon whose difficulties cannot be resolved simply by throwing technology at it. Voting machines have to be physically secure before, during, and after Election Day. Election workers need to be well trained and able to deal with the problems inherent in any technology. (As the saying goes, To really screw things up, you need a computer.)

It's unusual and more than a bit surprising that in the short term, technologists want to slow down the move to electronic systems while many election officials are ready to speed ahead. If the officials started down the electronic voting path by underestimating the problems of deploying the technology, computer scientists may have underestimated the long-standing difficulties of conducting traditional all-paper elections. Election officials now seem to be coming to understand the merits and demerits of electronic voting systems. Overall, the current debate over electronic voting has certainly raised the bar for election equipment. And every year, we get a chance to do better.

The writer gratefully acknowledges Rebecca Mercuri's invaluable help in the preparation of this article.

TO PROBE FURTHER

There are a number of sites devoted to improving electronic voting security and reliability. Among them are those of the nonprofit Verified Voting Foundation Inc. (<http://verifiedvoting.org>); Black Box Voting, a site created by Bev Harris, author of a self-published book of the same name (<http://www.blackboxvoting.com>); and Rebecca Mercuri's Notable Software Inc. (<http://www.notablessoftware.com>).

The Organization for Security and Co-operation in Europe, in Vienna, a 55-nation consortium that plans to send observers to monitor the 2004 U.S. presidential election, can be found at <http://www.osce.org>. In addition, the Verified Voting Foundation is also organizing and training technology experts to monitor the election. As of August, more than 700 volunteers had signed up. For details, see <http://vevo.verifiedvoting.org/techwatch/>.

