Scantegrity III:
Automatic Trustworthy Receipts, Highlighting Over/Under Votes, and Full Voter Verifiability

Alan T. Sherman, Russell A. Fink, Richard Carback
Cyber Defense Lab
University of Maryland, Baltimore County (UMBC)

David Chaum
Voting Systems Institute

EVT 2011

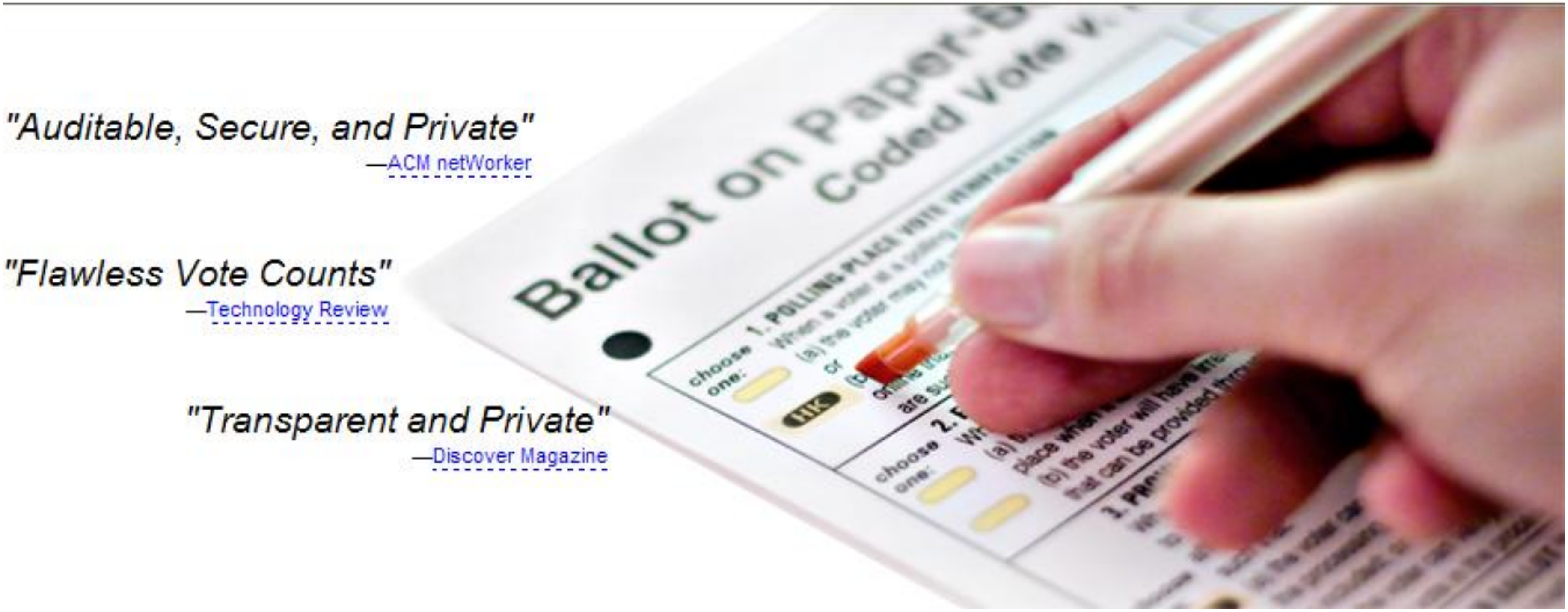
Contributions: Improvements to Scantegrity II

- Three designs for trustworthy receipt printers
- Eliminate need for separate print audit
- New user interface for optical scan: achieve HAVA compliance with backlighting of over/under votes
- Design enhancements with TPM
- Improved security:
  - Encourage more voters to verify on-line
  - Detect marks added to ballot after casting
  - Make copies of all receipts public

Outline

- Scantegrity II end-to-end voter-verifiable elections
- Issues from 2009 Takoma Park municipal election
- Related work
- Three designs
  - Simple image duplicator (separate from scanner)
  - Mark sense translator (connected to scanner)
  - Scantegrity III (embellished mark sense translator protective back-lighted glass)
- Discussion

Scantegrity II



"Auditable, Secure, and Private"
—ACM netWorker

"Flawless Vote Counts"
—Technology Review

"Transparent and Private"
—Discover Magazine

www.scantegrity.org

2009: Takoma Park, Maryland, Elects Mayor with Scantegrity

David Chaum

Inventor, Scantegrity

Issues from Takoma Park 2009

- Many voters did not write down codenumbers
  - Some voters found it difficult to read the codenumbers and write them down
  - Some voters did not known they needed to write down codenumbers to verify on-line
- Scanner was not HAVA compliant
- Print audit added cost and complexity

We address these issues

Related Work

- Sure Vote (Chaum, 2004)
- Vote Here (Neff, 2004)
- Punchscan (Chaum *et al.,* 2006)
- Sigma Ballot (Popoveniuc, 2010)

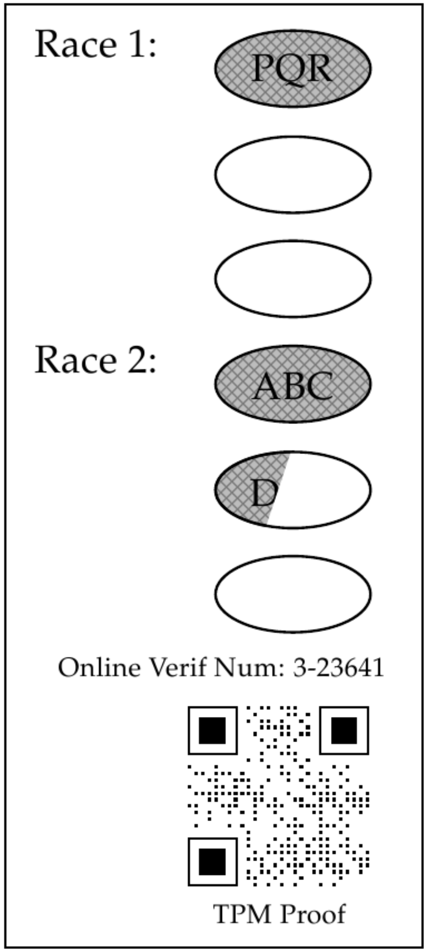
This paper refines and integrates:

- Image duplicator / mark sense translator (Fink & Carback, 2010)
- Scantegrity III (Chaum, 2011)

Image Duplicator

- Separate optional station
- Copies bubble contents
- For each race, orders bubbles by decreasing pixel intensity
- Stateless design
- Reads on-line verification number and markable positions from 2D barcode (and senses alignment marks)

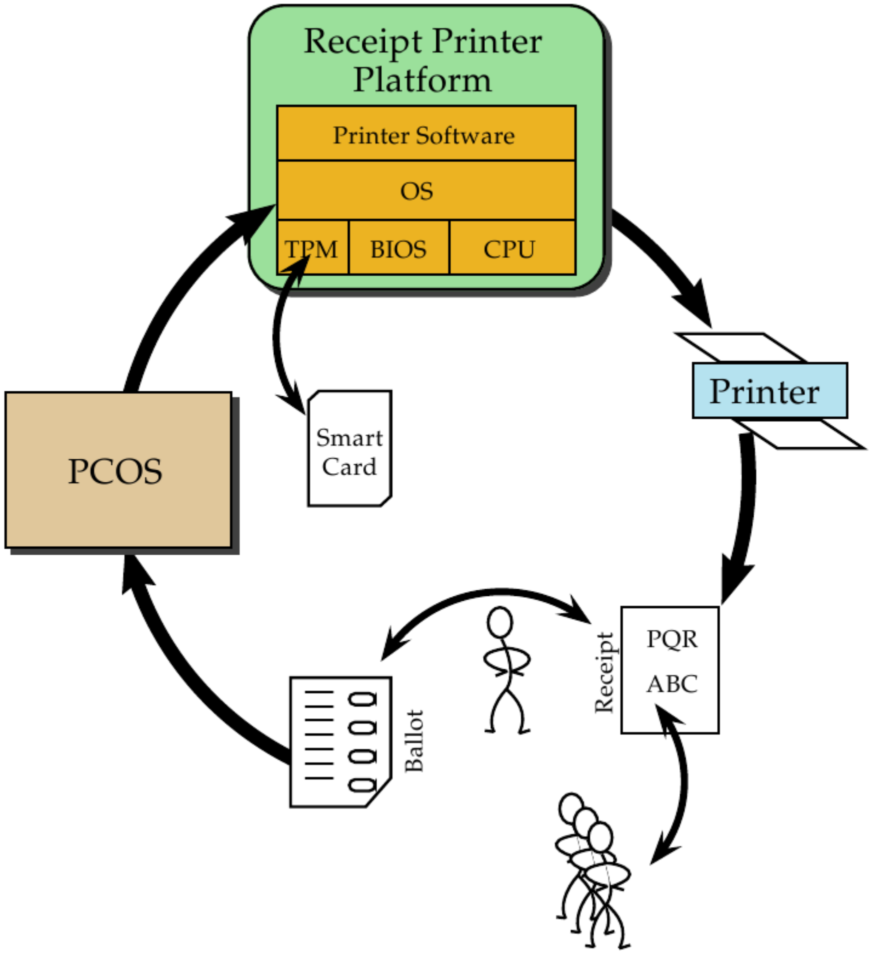
Image Duplicator



Mark-Sense Translator

- Connected to PCOS scanner, which detects marked positions
- Stateful design: prints codes from marked positions and privileged information
- Reads encrypted codes from 2D barcode (key bound to TPM)
- Ballot locked under glass while voter checks receipt

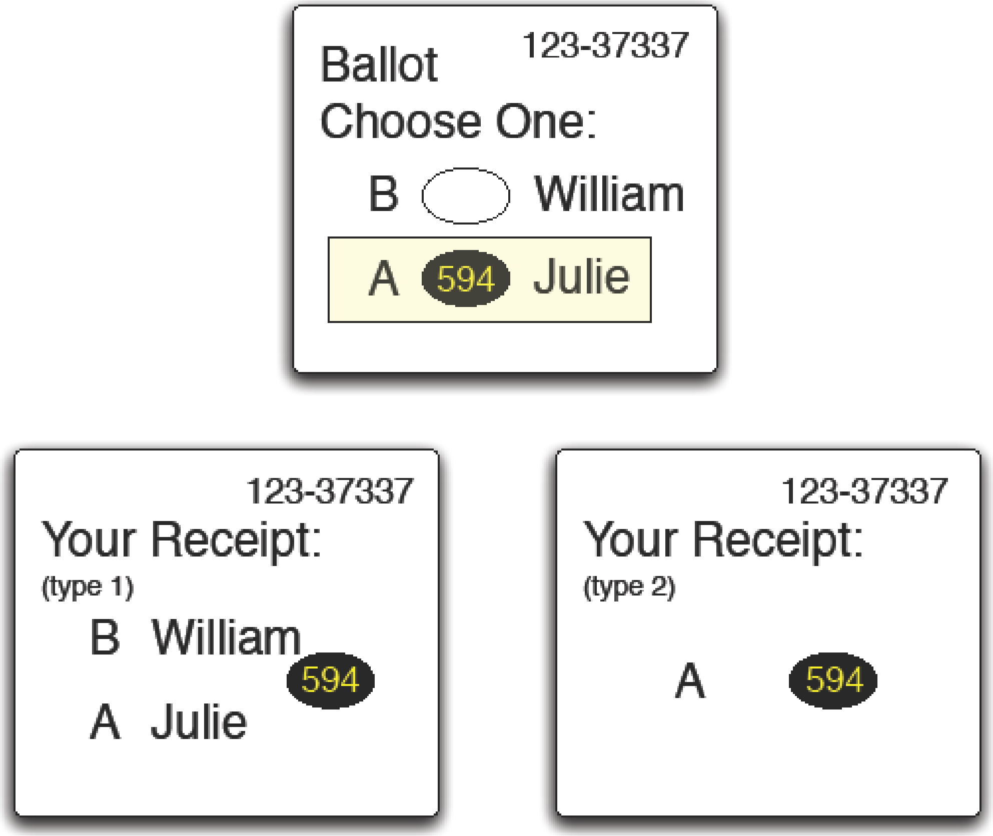
Mark-Sense Translator



Scantegrity III Casting Station

- Embellished mark sense translator
- New ballot format
- Two different receipt types (type chosen in a verifiably random way)
- Eliminates need for print audits
- Highlights over/under votes (and more) with LED backlighting

Scantegrity III Ballot and Receipts



Ballot 123-37337

Choose One:

B ○ William

A 594 Julie

123-37337

Your Receipt:

(type 1)

B William

594

A Julie

123-37337

Your Receipt:

(type 2)

A 594

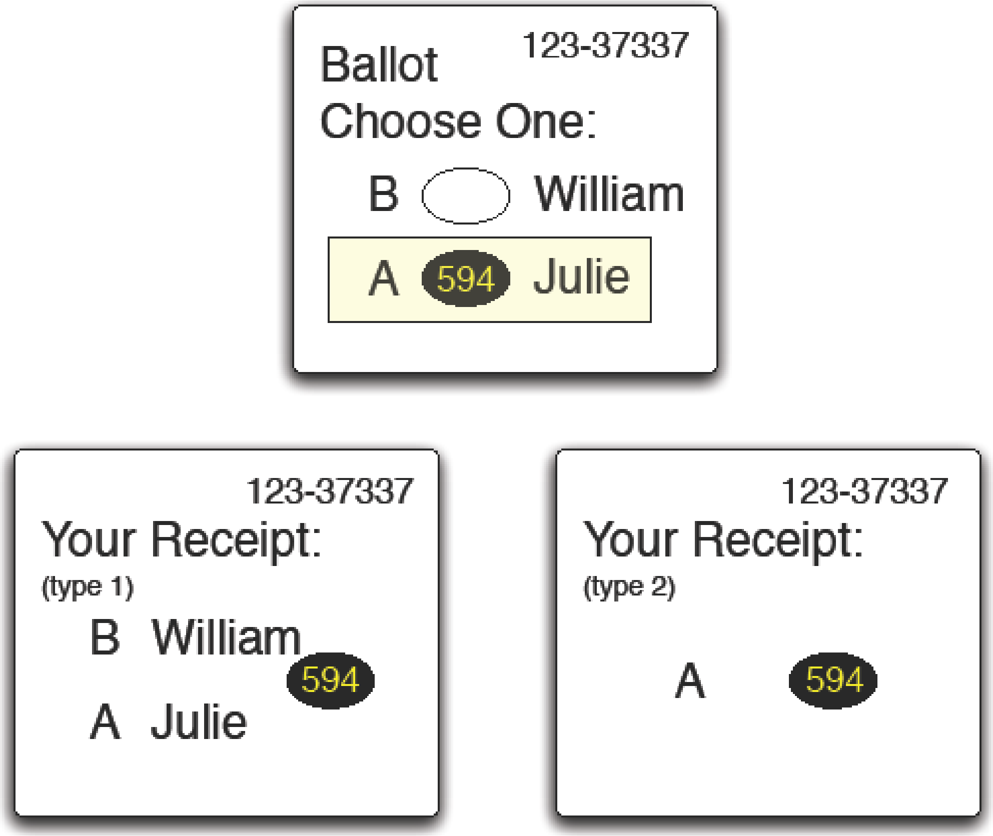
Verifiable Randomness

- Random
- Unpredictable
- Voter can verify that proper procedure was followed (but voter doesn’t influence)
- Bits become part of public audit record
- *Ex:* Camera observes roll of red/green die in clear dome

Eliminating Print Audits

- In Scantegrity II, print audit is destructive: audited ballot cannot be cast
- In Scantegrity III, indirection permits auditing of cast ballots
  - Receipt type I catches misprinting of S1 codes (after release of race→S1 commitment)
  - Receipt type II catches misprinting of S2 codes (after release of S1→S2 commitment)

Scantegrity III Ballot and Receipts



Ballot 123-37337

Choose One:

B ○ William

A 594 Julie

123-37337

Your Receipt:

(type 1)

B William

A Julie

594

123-37337

Your Receipt:

(type 2)

A 594

Bolstering Designs with TPM

- End-to-End *integrity* is not End-to-End *security*
- Protect privacy, enforce election policy,
  detect problems sooner
- TPMs help ensure correct software is booted,
  provide place to store keys & codes,
  offer monotonic counters
- Election integrity does *not* depend on TPM

Discussion

- Image duplicator
  - Simple, stateless, low marginal risk
  - Separate station; no guarantee same ballot is cast
- Mark sense translator
  - More complex mechanism, TPM learns codes
- Scantegrity III casting station
  - Eliminates print audit; backlights ballot
  - More complex ballot and checking at station

Security Advantages

- More voters will likely verify votes on-line if receipts are easier to produce
- Copies of *all* receipts could be made publicly available
- Improves usability and accessibility
- Can detect if extra marks are added after scanning (for stateful designs)
- Failsafe mode of operation is Scantegrity II

Potential Threats: Malicious Receipt Printers

- Leak codes
  - Privacy loss; facilitates bogus claims of malfeasance
- Produce invalid signatures; authenticate false receipt; malfunction
  - Disruption; discreditation

Similar to threats from malicious scanners.

Cannot violate integrity without detection: voter can compare receipt with ballot; voter can still make hand-written receipt.

Eliminating Invisible Ink

- With mark sense translator, could “late-bind” codes by printing codes for first time on receipt (requires trust in TPM)
- Reduces complexity caused by invisible ink
- Failsafe mode of operation becomes Scantegrity I, if technology fails
- Improves accessibility (*e.g.,* blind voters can hear codes)

Open Problems

- Implement and test
- How well will human voters respond to designs?
- Improve accessibility

Conclusion

- Improvements to Scantegrity:
  - Print trustworthy receipts automatically
  - Eliminate print audit
  - New back-lighted interface for opscan
- Three receipt printer designs
  - Simple stateless image duplicator introduces fewest potential additional security vulnerabilities
  - Which is best depends on situation

Acknowledgments

- Sherman was supported by DoD IASP grants H98230-09-1-0404 and H98230-10-1-0359.

Questions?