CrySP

WATERLOO
CHERITON SCHOOL OF
COMPUTER SCIENCE

Democracy Enhancing Technologies:
Toward deployable and incoercible E2E elections

Jeremy Clark

Voting Requirements

- The first election in Canada was a public vote: full integrity but no secrecy
- Now we use secret ballot: secrecy but little integrity
- Extra procedures allow verification of a single polling place with a full day commitment

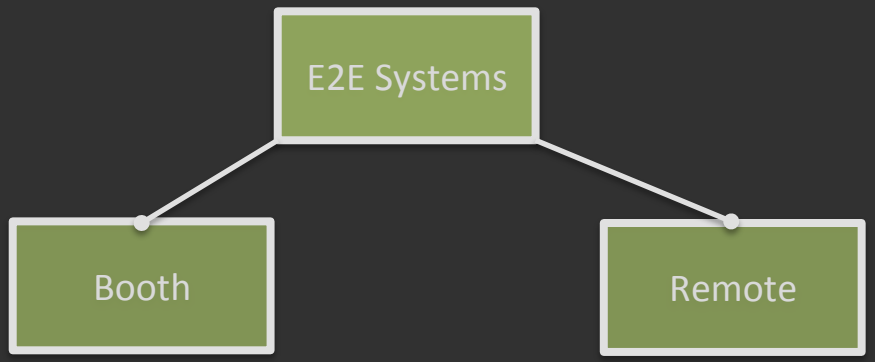
End-to-End (E2E) Verification

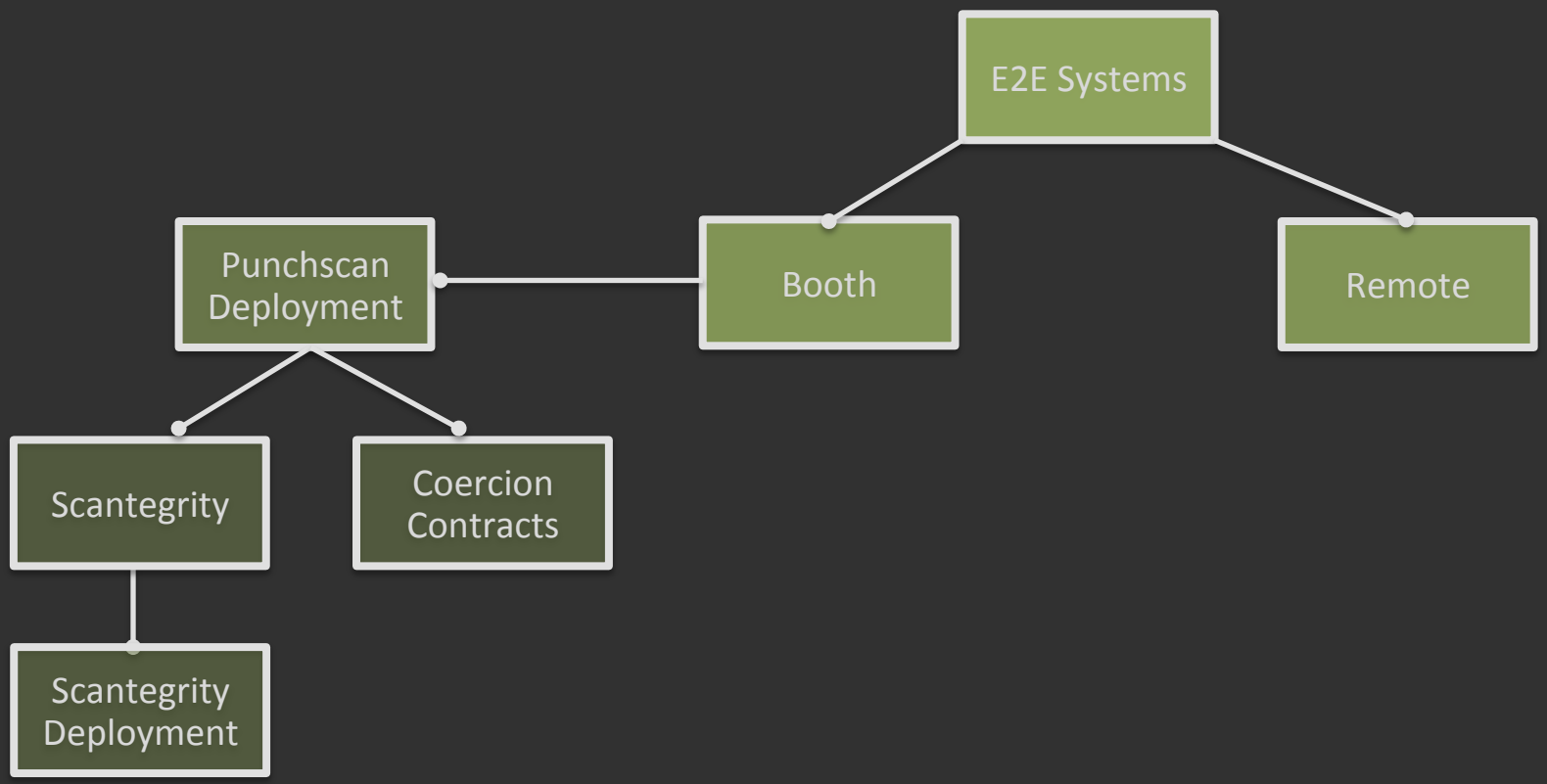
- Same integrity as a public vote
- Same ballot secrecy as a ballot box
- Same level of verification as watching the ballot box all day
- Plus: verification can be done after the election at any time and covers all precincts

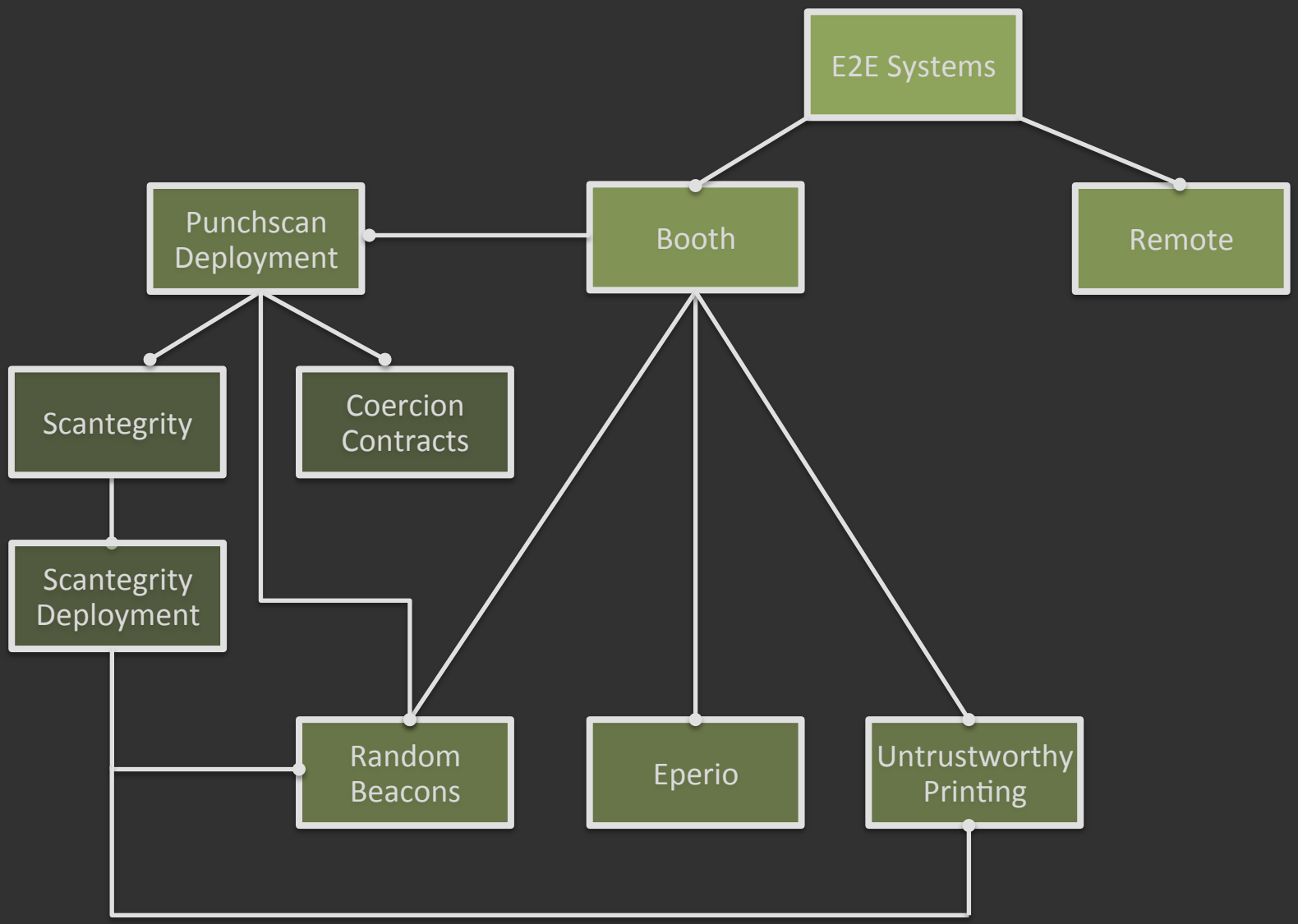
Thesis

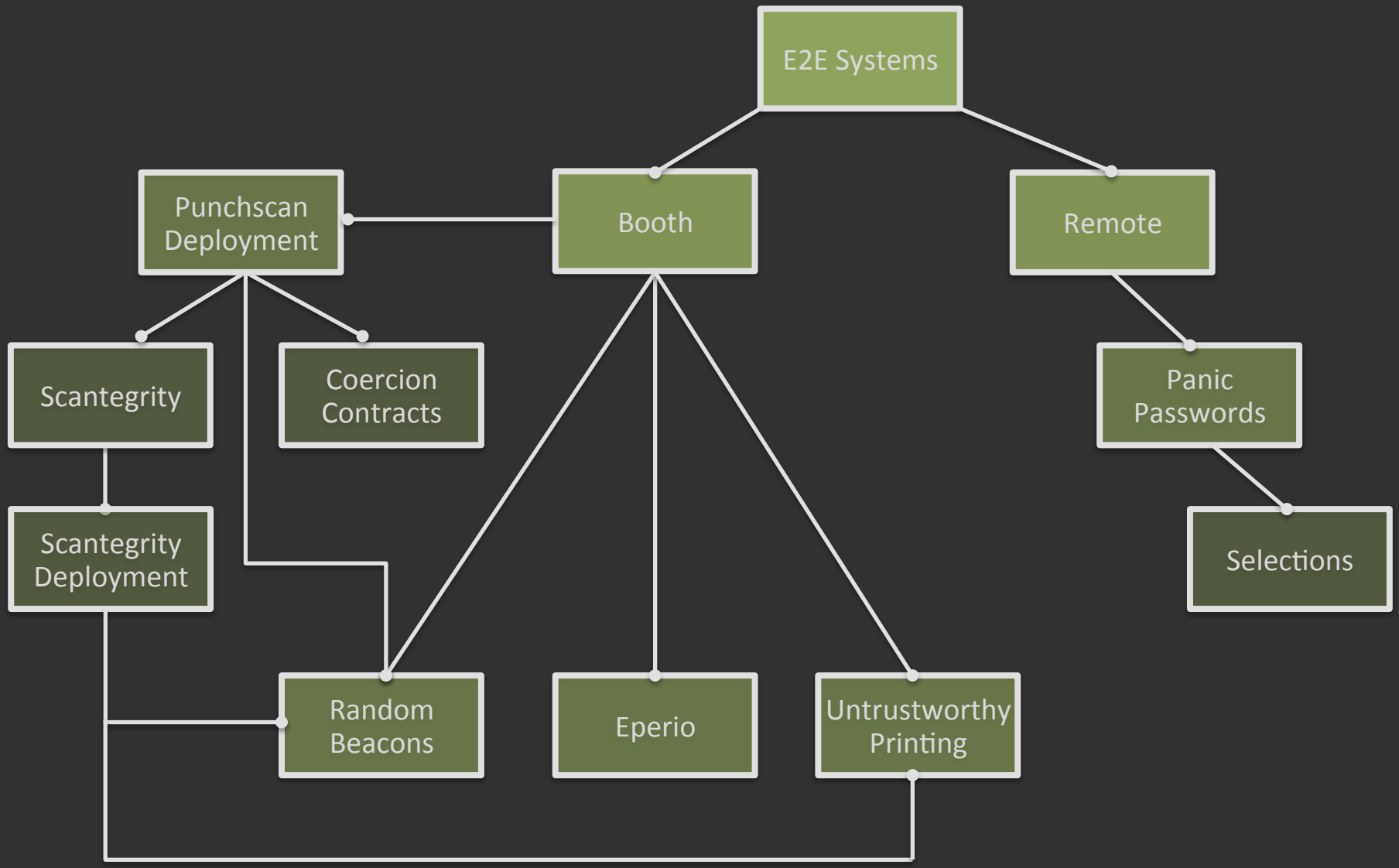
- End-to-end verifiable voting systems, and their components, can be designed for real-world deployability while maintaining a strong notion of ballot secrecy and incoercibility, even in the case of internet voting

Roadmap




E2E Systems
Punchscan Deployment
Booth
Remote
Scantegrity
Coercion Contracts
Scantegrity Deployment


E2E Systems
Punchscan Deployment
Booth
Remote
Scantegrity
Coercion Contracts
Scantegrity Deployment
Random Beacons
Eperio
Untrustworthy Printing


E2E Systems
Punchscan Deployment
Booth
Remote
Scantegrity
Coercion Contracts
Panic Passwords
Scantegrity Deployment
Selections
Random Beacons
Eperio
Untrustworthy Printing

Scantegrity

[EVT 2008]

Problem

- Paper-based E2E systems are generally a replacement for existing systems
- They do not permit manual recounts or traditional audits
- This may create barriers to entry: conceptual, legal, costs, etc.

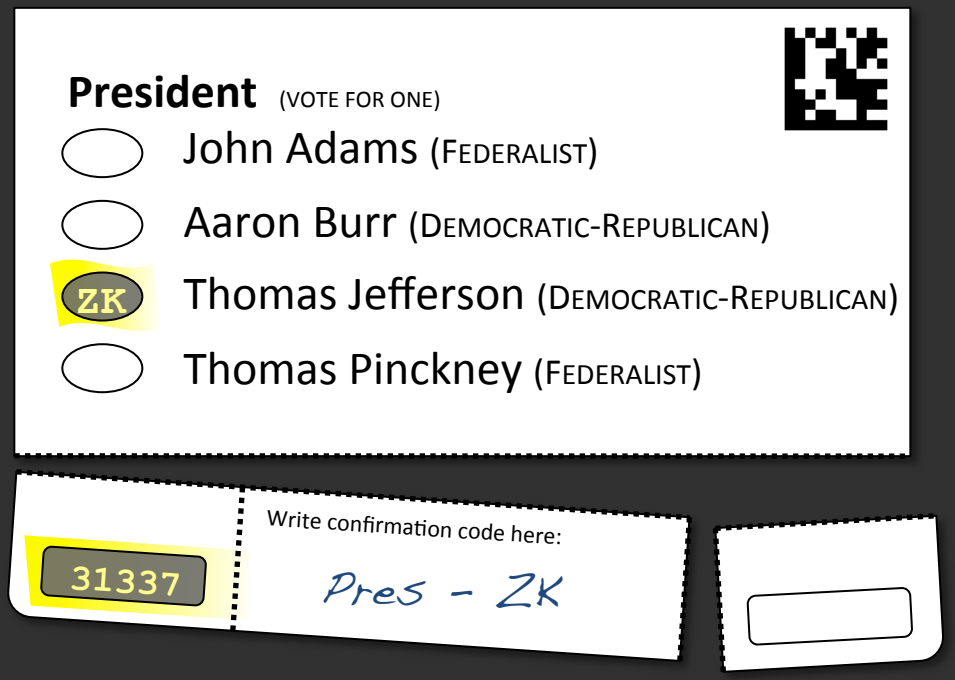
Contributions

- Scantegrity is an add-on for optical scan systems
- It interfaces with existing technology and does not interfere with traditional audits
- Verifiability is opt-in and ballot marking is a similar experience
- Scantegrity also provides very powerful dispute resolution properties

Relation to Thesis

- Scantegrity addresses lessons learned deploying its predecessor Punchscan
- Simple scenarios that arise in real elections, can create non-obvious incoercibility issues
- For example, spoiling ballots

Scantegrity Ballot



Municipal Election with Scantegrity

[Usenix Security 2010]

Problem

- Various E2E systems have been used in elections, however none in a public-sector election
- There is generally a deficit of data on voter experiences with E2E systems

Contributions

- We ran a municipal election with Scantegrity
- This was the first public-sector election for any E2E system (and any open source system)
- We collected observational data, such as time-to-vote
- 271 (out of 1722) voters and 5 pollworkers provided feedback through surveys

Relation to Thesis

- This election is an important milestone for the deployment of paper-based E2E systems
- Redesigned many aspects of the system and procedures after a mock election to improve practicality

City of Takoma Park, Maryland
MUNICIPAL ELECTION
NOVEMBER 3, 2009

OFFICIAL BALLOT — WARD 3

Instructions: Vote for candidates by indicating your first-choice candidate, your second-choice candidate, and so on. You are free to rank only a first choice if you wish.

Do not fill in more than one oval per column. Do not fill in more than one oval per candidate. Do not skip numbers in the ranking sequence.

To vote for a person whose name is not printed on the ballot, write the name in the space provided and fill in one box in the column indicating your ranking of the write-in candidate.

If you make a mistake on your ballot, return it to the judge and get another.

Do not make any identifying marks on your ballot.

When you mark an oval to rank a candidate, a code will be revealed that you may later use to verify your vote online. See the instruction sheet in the voting booth.

Ciudad de Takoma Park, Maryland
ELECCIONES MUNICIPALES
3 DE NOVIEMBRE DE 2009

BOLETA OFICIAL— DISTRITO ELECTORAL 3

Instrucciones: Vote por los candidatos indicando el candidato que sea su primera opción, el candidato que sea su segunda opción, y así sucesivamente. Si lo desea, puede limitarse a seleccionar solamente al candidato que sea su primera opción.

No rellene más de una casilla por cada columna. No rellene más de una casilla por cada candidato. No salte números en la secuencia de clasificación por orden.

Para votar por una persona cuyo nombre no está impreso en la boleta, escriba el nombre en el espacio provisto y rellene una casilla en la columna para indicar el orden de clasificación del candidato que se ha añadido.

Si usted comete un error en su boleta, devuélvasela al juez y pida otra.

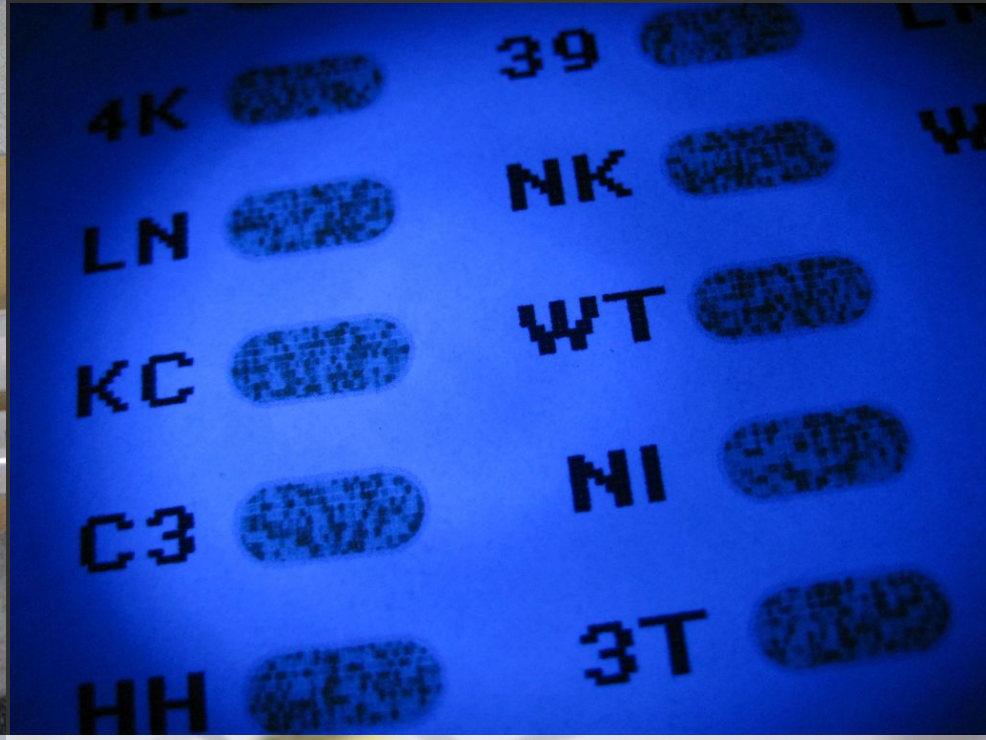
No haga marcas en su boleta que puedan identificarla.

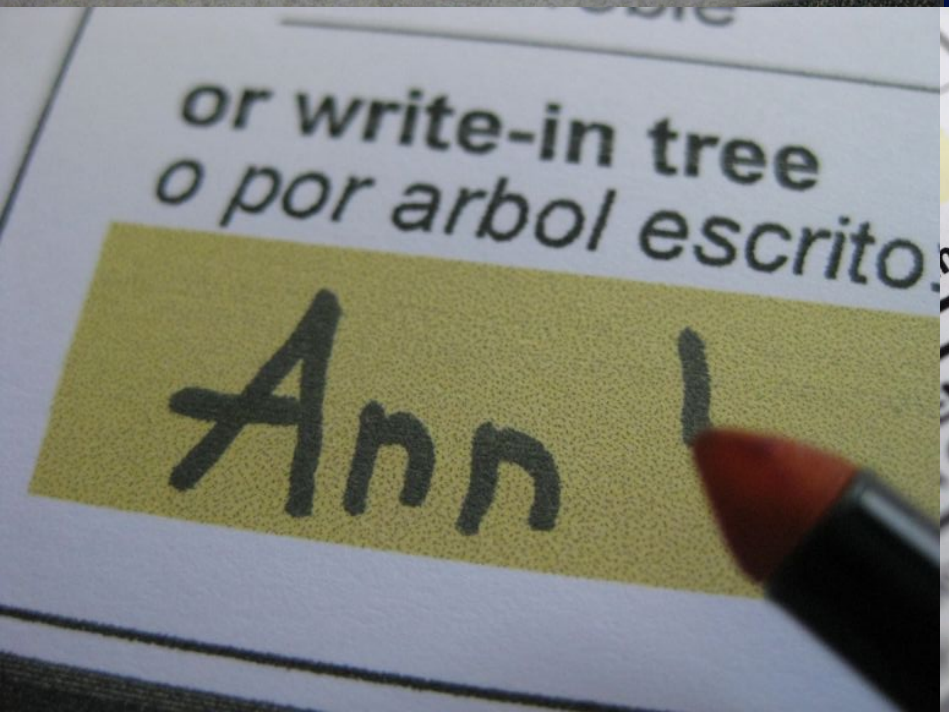
Cuando usted marque la casilla para votar por un candidato, verá un código que podrá usar posteriormente para verificar su voto por Internet. Vea la hoja de instrucciones en la cabina de votación.

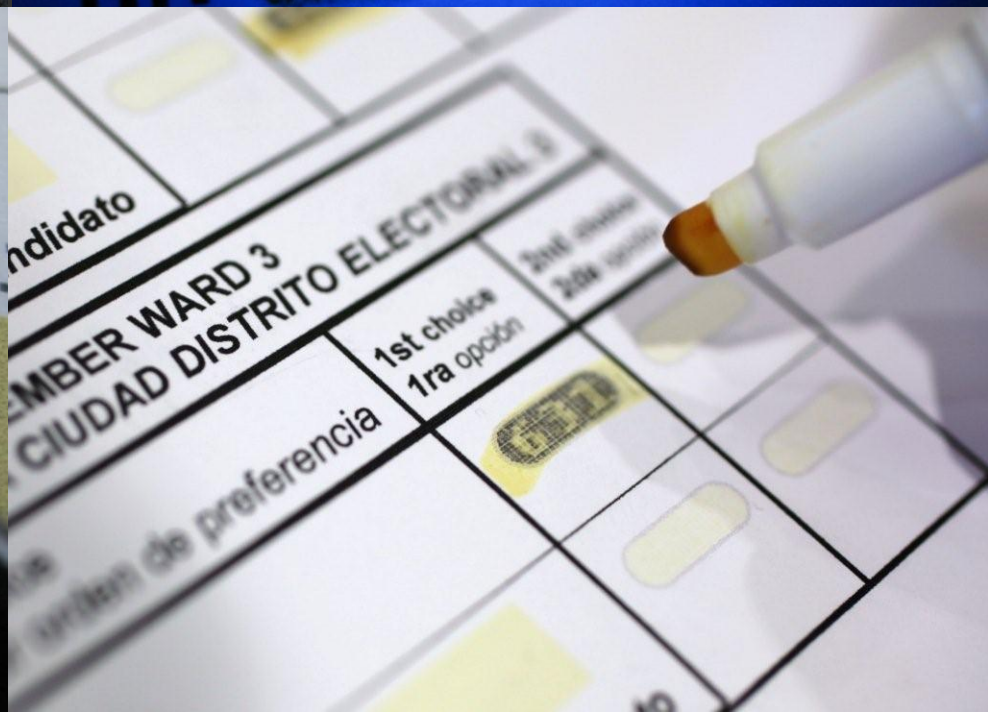
MAYOR *ALCALDE*			
Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice *1ra opción*	2nd choice *2da opción*	3rd choice *3ra opción*
Roger B. Schlegel	1st		
Bruce Williams			3rd
Tom Smith		2nd	
Write-In Candidate/*Para añadir a un candidato*			

CITY COUNCIL MEMBER WARD 3 *MIEMBRO DEL CONSEJO DE LA CIUDAD DISTRITO ELECTORAL 3*		
Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice *1ra opción*	2nd choice *2da opción*
Dan Robinson		
Write-In Candidate/*Para añadir a un candidato*		

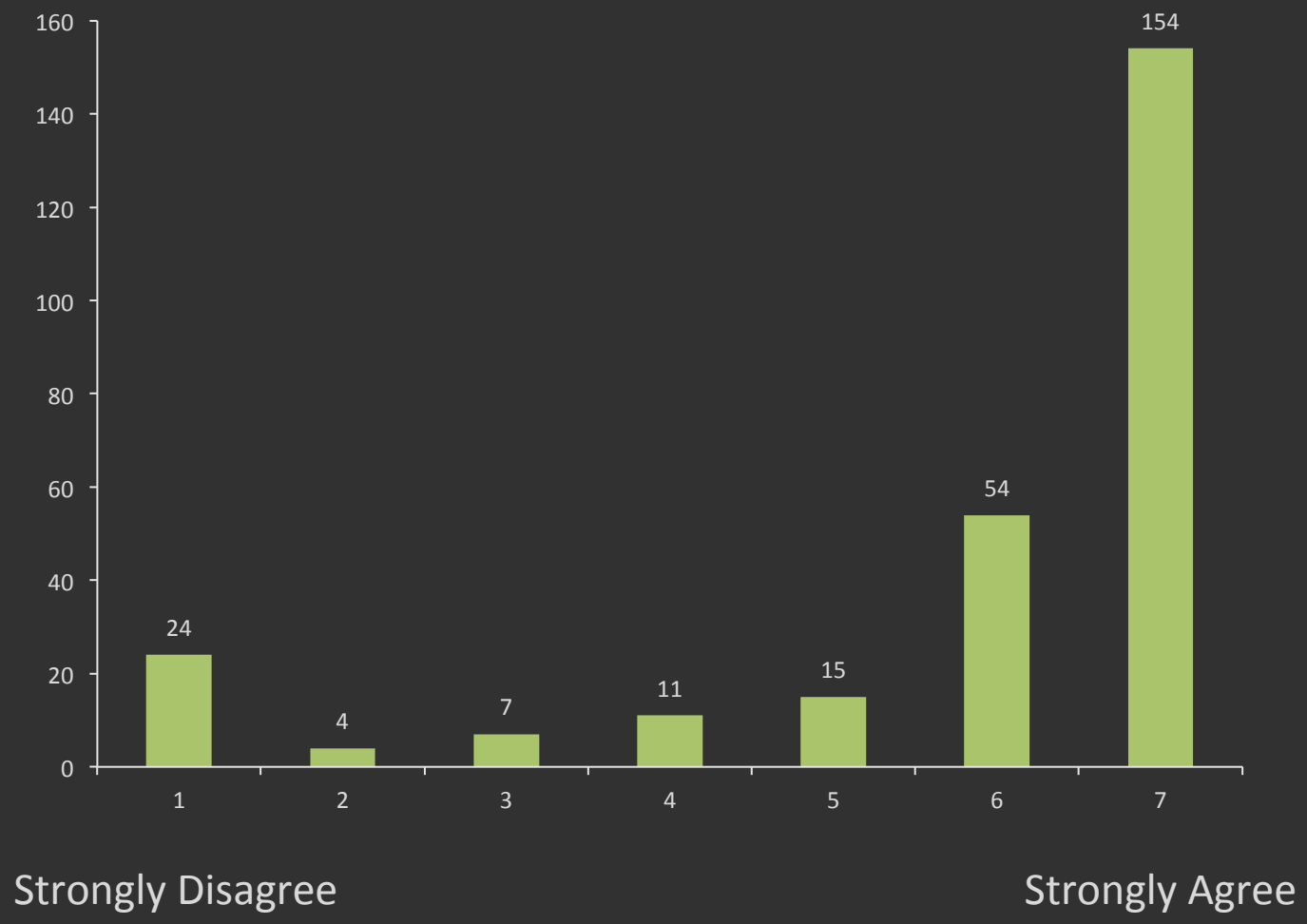
3-972853
Online Verification Number
Número de Verificación por Internet


4K
39
LN
NK
KC
WT
C3
NI
HH
3T


or write-in tree
o por arbol escrito
Ann


ndidato
EMBER WARD 3
CIUDAD DISTRITO ELECTORAL 3
1st choice
1ra opción
orden de preferencia

Overall, the voting system was easy to use



Coercion Contracts

[Vote-ID 2009]

Problem

- A number of papers presented a subtle attack against Punchscan receipts
- Adversary can influence the probability that a (utility-maximizing) voter will vote for the adversary's preferred candidate through a contract
- The specifics of these contracts varied and no general properties were presented

Contributions

- We analyze the three examples in the literature
- We generalize contracts to arbitrary number of candidates and levels of utility
- We examine the effectiveness of contracts when voters deceive the adversary

Relation to Thesis

- Maintaining incoercibility is difficult in E2E systems
- Issues like these tend to arise when you replace standard cryptographic primitives with techniques that can be used on paper or by voters without computers (i.e., deployable systems)
- Coercion contracts, and this study, influenced the design and procedures of Scantegrity

Random Beacons

[EVT/WOTE 2010]

Problem

- Systems like Punchscan and Scantegrity (and Eperio) require external, verifiable randomness for the tally proof
- We used, heuristically, financial data to create the required challenges
- The soundness of this approach was not studied: do closing prices have sufficient entropy?

Contributions

- We used tools from computational finance to conservatively estimate the entropy in a closing price
- For MSFT over a single day: 7.76 bits of entropy
- For DJIA (40 stocks) over a single day: 218 bits of entropy

Contributions

- We also consider how to convert a list of prices into a usable random seed
- Our approach: use proper extraction plus we add some additional security properties that could be useful in general scenarios

Relation to Thesis

- These contributions are about deployablity
- Financial data is used because it is intuitive, widely available, and provides sufficient entropy in a timely manner

Eperio: Election verification in a spreadsheet

[EVT/WOTE 2010]

Problem

- Auditing E2E systems, like Scantegrity (or systems based on more involved cryptography), is a difficult task
- Existing auditing tools require configuration, specific versions of software, external libraries, etc.

Contributions

- Eperio is a verification protocol that can be interfaced with paper-based E2E ballots
- Eperio is designed to be lightweight, easy to audit, and fast
- Auditing can be done manually within a spreadsheet, with a spreadsheet macro, or with custom code
- Python implementation: ~50 lines of code and runs out-of-the-box on OS X, Linux & bootable Linux CDs

Relation to Thesis

- A commonly cited criticism of E2E systems is that they are not understandable
- We feel that simplifying systems can help deployment in real world elections
- With Eperio, more voters can learn by doing

Toward Untrustworthy Printing

[HotSec 2009]

Problem

- Many paper-based E2E systems offer strong ballot secrecy throughout the election except when the ballots are printed
- Can we distribute printing of arbitrary secrets between two non-colluding printers?

Contributions

- A protocol for printing a random string from a set of strings
- A protocol for printing a random permutation of a set of strings
- Seven-segment logic to reduce the representation of a character

Relation to Thesis

- Printing is a direct consequence of using paper-based voting systems, and paper-based systems themselves are being explored for deployability reasons
- An adversary that can corrupt the printer can coerce voters

Two-Party Printing (HBC)

- Printers A and B agree on an authenticated sheet of paper to be used
- Printer A generates a random visual cryptography share and prints it in invisible ink
- Printer A generates a set of shares that will combine with A's random share to generate the set of strings
- Printer A permutes the set
- Printer B chooses a random index and A and B use oblivious transfer to send the share to B
- Printer B prints its share on top in invisible ink

Panic Passwords

[HotSec 2008]

Problem

- Panic passwords are a way for a user to signal distress covertly
- No attention from the academic community
- The trivial solution: issue two passwords, one real and one fake, does not usually work: adversary will demand both passwords

Contributions

- We provide a threat model for categorizing scenarios where panic passwords may be used
- We identify novel attacks against the panic password systems
- We present several new systems to protect against strong adversaries
- In particular, we provide a system that is suitable for internet voting

Relation to Thesis

- Incoercibility is difficult in internet voting because an adversary can be physically present while the voter casts a vote
- Panic passwords seem like a good fit for providing incoercibility
- They also have deployability advantages relative to cryptographic techniques for faking actions

Selections: Coercion-Resistant Internet Voting

[Financial Cryptography 2011]

Problem

- Internet voting allows for coercion and vote selling
- Literature mitigates these attacks by allowing voters to fake some authentication values
- Authentication is based on cryptographic values ("something you have") and faking a value requires computations
- No internet voting system in the literature allows both linear tallying and revocation

Contributions

- Selections is an internet voting system that is verifiably correct and protects against over-the-shoulder adversaries
- It uses panic passwords to make both authentication and deception easier for the voter
- Tallying and revocation of voters are efficient in the number of voters

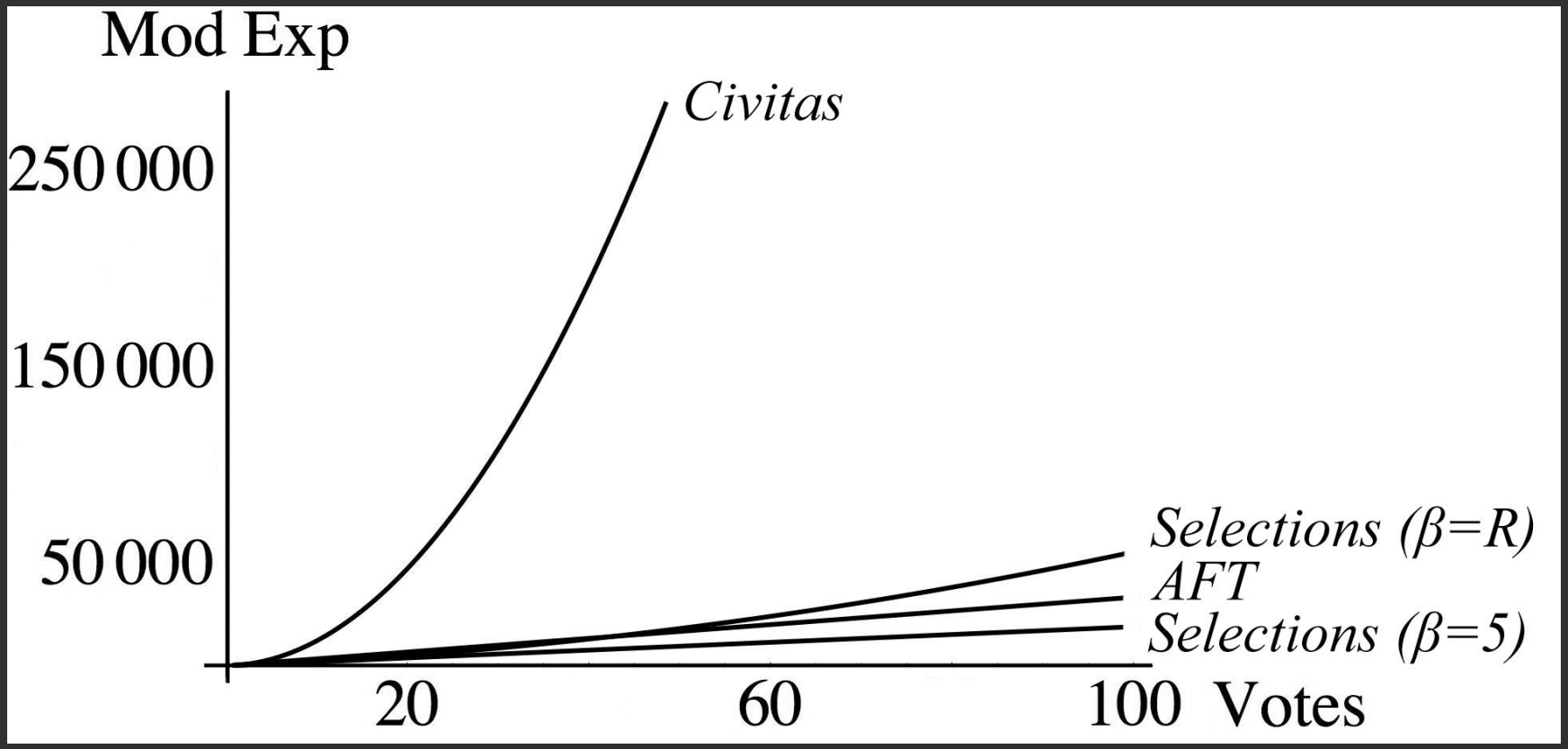
Relation to Thesis

- Selections is designed to move coercion resistant, verifiably correct internet voting systems toward deployability
- This is reflected in making it password-based and in the registration process, as well as providing real-world requirements like revocation
- Efficiency is also a deployment concern: related work is too slow for typical sized precincts

- Verifiably correct:
  - Only votes from eligible voters are kept
  - Only votes with real passwords are kept
  - Only one vote per voter is kept
  - Votes are not modified

- Coercion resistant:
  - If sometimes voters actually vote how an over-the-shoulder adversary wants them to
  - Sometimes they deceive the adversary and vote the way they want to
  - The adversary cannot tell the two apart

Efficiency


Mod Exp
250 000
150 000
50 000
Civitas
Selections (β=R)
AFT
Selections (β=5)
20
60
100
Votes

Thank You