Hacking Paper
Some Random Attacks on Paper-Based E2E Systems

John Kelsey, NIST

Andrew Regenscheid, NIST

Tal Moran, Weizmann

David Chaum

End to end voting system

- Voter interacts with system
  - Gets receipt
- System counts votes and publishes results
- Voter can verify their vote included in total from receipt
  - But must not be able to use to sell vote!
- Anyone can verify vote count correct
- Examples: Punchscan, Pret-a-Voter, Threeballot

Scratch-Off Cards

- Physical device to give us this property:
  - First you must commit to a challenge
  - Then you get some hidden information
  - You can’t undo the challenge and cover it back up.

Smith's Position

	1	2	3	4
a	#	#	#	#
b	#	#	#	#
c	#	#	#	#
d	#	#	#	#

Smith's Position

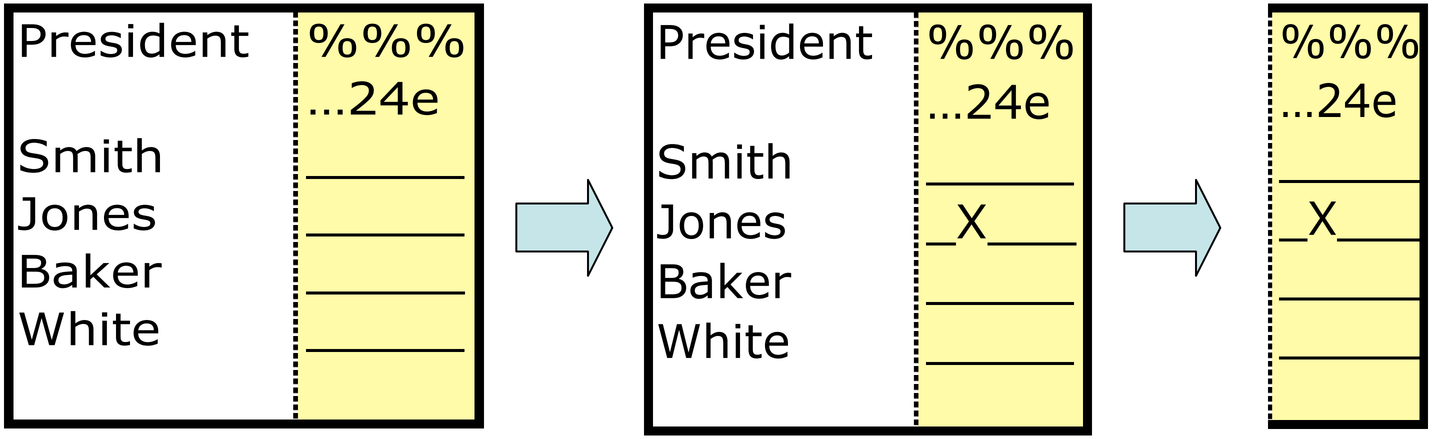
	1	2	**3**	4
a	#	#	#	#
b	#	#	F	#
c	#	#	#	#
d	#	#	#	#

Pret a Voter

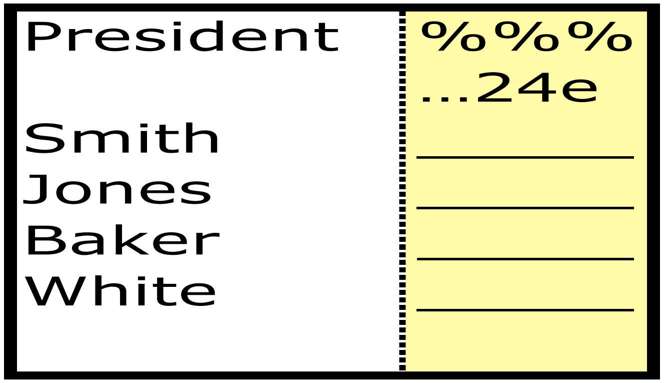
- Internals very similar to Punchscan
- Ballot in two halves:
  - Left has candidate names in random order
  - Right has boxes/blanks to fill in.
- Voter may either audit blank ballot
  - Get receipt with opened ballot
- Or vote right side
  - Get copy of right side as receipt.

Pret-A-Voter Picture

- Voter gets ballot
  - May audit ballot or vote it
- To vote, mark choice and detach ballot; copy of scanned ballot is your receipt
- To audit, scan blank ballot and get back receipt showing correct left side.



Applying the attack to Pret-a-Voter



President	%%% ...24e
Smith	________
Jones	________
Baker	________
White	________

```
Last digit of serial number
 0   5  a   f    k   p   v
... |... |... |... |... |... |...
 4   9  e   j    o   t   z
#   #   #   #   #   #   #

Smith blank:
 1   2   3   4
#   #   #   #

AUDIT WHEN SUM%10 ==9
```

1 Commit to S/N and ballot.

2 May be:

--required to audit/open

--required to vote according to commitment.

```
Last digit of serial number
 0   5  a   f    k   p   v
... |... |... |... |... |... |...
 4   9  e   j    o   t   z
#   #   4   #   #   #   #

Smith blank:
 1   2   3   4
 5  #   #   #

AUDIT WHEN SUM%10 ==9
```

Wider application to many end-to-end schemes

- Punchscan
- Some variants of ThreeBallot