

VOTEBOX a tamper-evident, verifiable electronic voting system

DANIEL R. SANDLER KYLE DERR GEORGE MASTROGIANNIS KEVIN MONTROSE COREY SHAW DAN S. WALLACH

WHAT IS VOTEBOX?

VOTEBOX is a **prototype electronic voting machine** developed in the Rice Computer Security Lab.

Its design combines **novel techniques** with other recent e-voting research results in the areas of **distributed systems, cryptography, and usability**.

The result is a voting system that improves on current commercial DRE (direct recording electronic) voting machines and their analog forebears in **trustworthiness, reliability, and security**.

VOTEBOX is intended as a platform for **broad e-voting research** in the areas of security and usability.

It can be used as a starting point for new implementations or integrated with existing systems to increase assurance.

A complete discussion of the **design and implementation** of VOTEBOX can be found in:

Daniel R. Sandler, Kyle Derr, and Dan S. Wallach.
VoteBox: a tamper-evident, verifiable electronic voting system. In *Proceedings of the 17th USENIX Security Symposium (USENIX Security '08)*, July 2008.

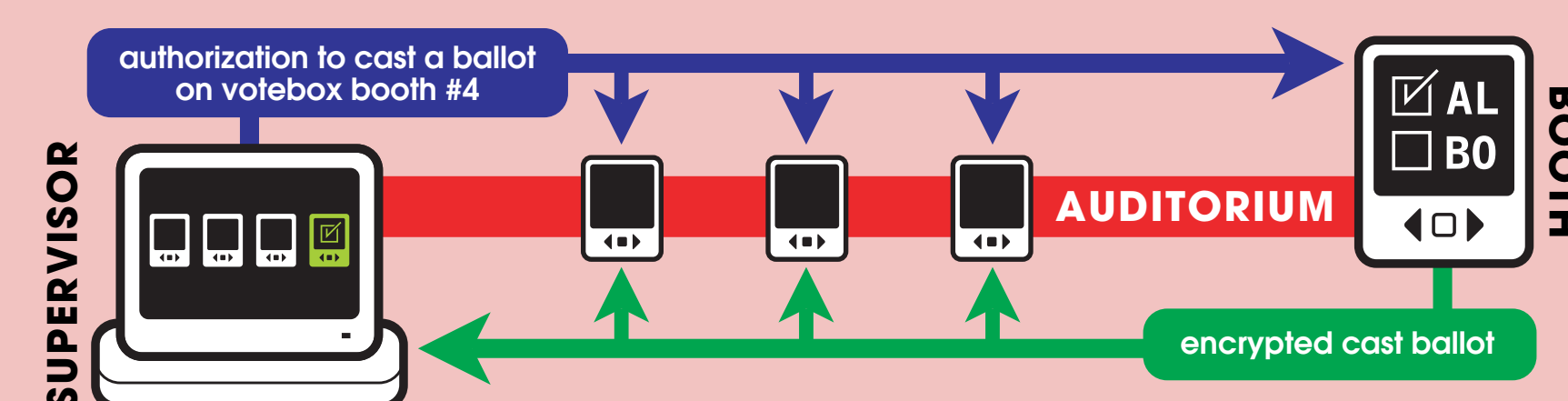
WHAT IS INSIDE VOTEBOX?

AUDITORIUM redundant secure logs

goals: prevent mistakes and recover from failures on election day; facilitate post facto auditing of election results

approach:

- VOTEBOX machines keep **secure logs** of essential election events, allowing credible audits during or after the election
- machines are connected using **AUDITORIUM**, a novel peer-to-peer network that **replicates and intertwines** secure logs to prevent a single machine from tampering with or losing data



D. R. Sandler and D. S. Wallach. **Casting Votes in the Auditorium.** In *Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07)*, 2007.

D. R. Sandler, K. Derr, S. Crosby, and D. S. Wallach. **Finding the evidence in tamper-evident logs.** In *Proceedings of the 3rd International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE '08)*, May 2008.

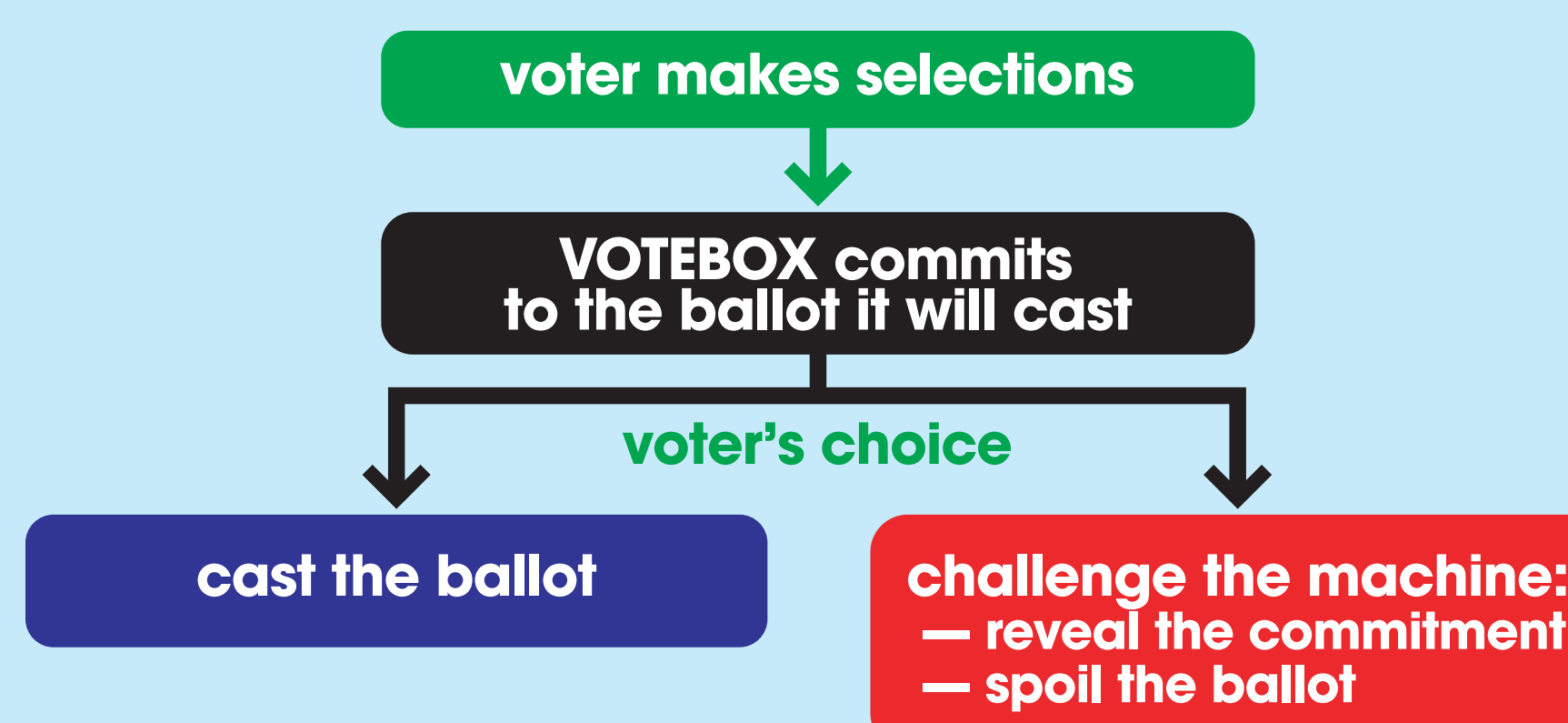
Previously: 2007 Rice Computer Science Corporate Affiliates poster session

CHALLENGES verifiable proof of correct operation

goal: *verifiability*—proof that the machine will faithfully capture the voter's choices and add them to the tally

difficulty: no amount of post facto auditing can catch a machine that switches the voter's choices before casting the ballot!

approach: a novel adaptation of a technique by Benaloh (2007)



the commitment is made by **encrypting and publishing** the voter's choices in AUDITORIUM; if the machine is faulty, it cannot retract the commitment, and will be **caught**

HCI human factors research

joint work with the **Computer-Human Interaction Lab (CHIL)**, led by Dr. Michael Byrne, Associate Professor of Psychology at Rice

collaboration:

- the VOTEBOX user interface was designed jointly with CHIL to reflect and refine the current DRE voting model
- human factors research parameters are built into VOTEBOX

research topics include:

- how **accurate** are users of electronic systems vs. existing systems (e.g. paper, punchcard, lever)? which do users prefer?
- how can we improve the **user interface** (presentation, navigation, confirmation) of e-voting systems?
- do users vigilantly double-check **paper audit trails (VVPAT)**?
- do users notice if the machine is **buggy or malicious** (switches votes, removes votes, etc.)—yes, this means that some builds of VOTEBOX include “evil” code!

S. P. Everett, K. K. Greene, M. D. Byrne, D. S. Wallach, K. Derr, D. R. Sandler, and T. Torous.
Electronic voting machines versus traditional methods: Improved preference, similar performance. To appear in *Human Factors in Computing Systems: Proceedings of CHI 2008*.

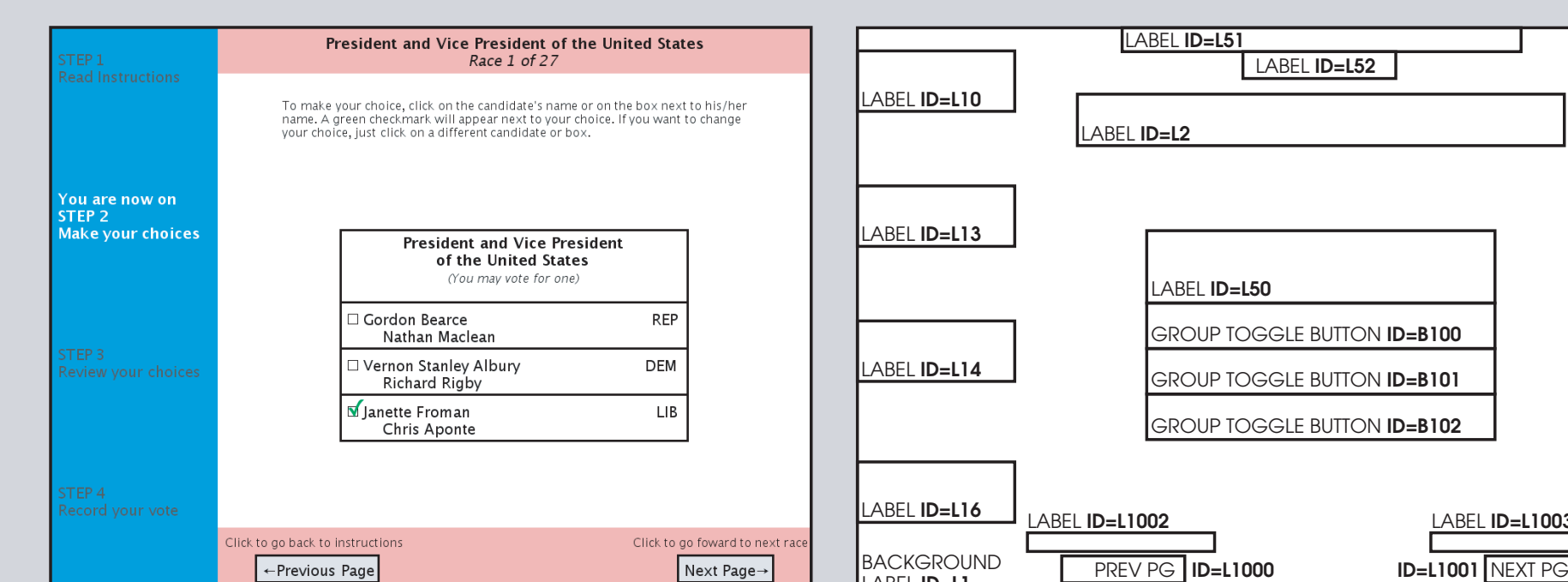
PRUI pre-rendered user interface

goal: reduce the size of the *trusted computing base* (the portion of the voting machine that must absolutely be correct)

approach: move complex graphics rendering out of the voting booth software, leaving only simple operations:

- place a bitmap on the screen
- accept touchscreen or keyboard input

ballot definition files, compiled in advance using our ballot creation software, contain all necessary graphics to present the ballot (including text in all required languages)



VOTER USER INTERFACE

BALLOT DEFINITION FILE

this technique was pioneered in the e-voting domain by the K-P Yee (2006, 2007); VOTEBOX demonstrates how it integrates with other approaches

VOTEBOX IS A PRODUCT OF



AND IS POSSIBLE THANKS TO SUPPORT FROM



source code, documentation, and publications at votebox.cs.rice.edu