Demo: Remotegrity

Are usable and secure remote voting schemes possible?

Richard Carback
Cyber Defense Lab
University of Maryland, BC

David Chaum
Voting Systems Institute

Jeremy Clark
School of Computer Science
Carleton University

Aleks Essex
School of Computer Science
University of Waterloo

Poorvi Vora
Institute of Computer Science
George Washington University

Filip Zagorski
Institute of Mathematics and Computer Science
Wroclaw University of Technology

ABSTRACT

We present a demo of Remotegrity, a new end-to-end independently verifiable absentee voting system, which was deployed in 2011 for the local election of the City of Takoma Park. Crucially, Remotegrity enables the voter to detects attempts by election insiders to change her vote, so that she may vote in person. She may also vote in person if she experiences an electronic denial of service attack from non-colluding voting computers. Remotegrity is not able to resist an attack where all local computers are colluding to change the voter's vote and she has no access to the election website.

A voter not interested in verification may largely ignore Remotegrity modifications to standard mail-in absentee voting procedures.

Remotegrity was designed to be a verifiable absentee system to replace a traditional mail-in system and it was required that the absentee system be consistent with the polling place system (which uses Scantegrity ballots), and that absentee procedures be very similar to previously-used mail-in absentee procedures.

1. THE VOTER EXPERIENCE

The Mailing Authority mails two types of paper cards to each voter: (a) A Scantegrity ballot with a unique serial number, containing candidate names and corresponding confirmation codes; (b) A Remotegrity Authentication Card (see Figure 4) with several OneTimePasswords and a pair of LockIns – each OneTimePassword and LockIn under a scratch-off layer.

The authentication card.

(see Figure 4) contains two sets of numbers under scratch-offs: *one-use or one-time passwords* (i.e., $9764 - 5930 - 4195 - 1472$) and *audit codes or lock-in codes* (i.e., $3509 - 4903 - 8255 - 8937$) on the bottom. It also contains a visible *serial number* (i.e., $EB3C15$) and a system password (i.e., 9768603372754008) – a number that is posted online if a corresponding ballot is received physically by the Election Authority.

Voting online.

The voter choosing to vote online performs the following steps.

1. Using the mailed paper ballot, she determines the confirmation number corresponding to her vote. In Figure 2, for example, the confirmation number corresponding to candidate *Candidate 1* as first choice is 6055.
2. She goes to the Absentee Voting Website and enters the confirmation number and a one-use password (OTP) scratched-off at random from the authentication card (see Figure 2).

The use of the confirmation number instead of the candidate name ensures that an adversary on the computer or on the line will not know the vote. Further, the adversary cannot reliably change the vote without knowing other valid confirmation numbers on the voter's ballot.

3. The voter may check the Absentee Bulletin Board (ABB), preferably from another computer, to determine if her confirmation number was posted correctly.

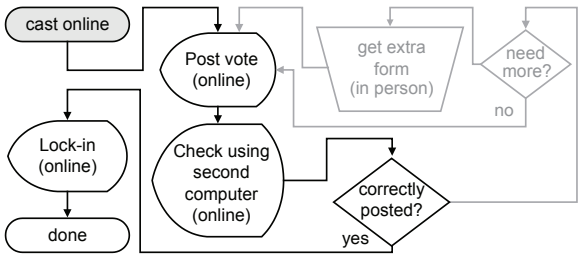


Figure 1: The example vote casting flow chart.

4. After waiting for a prescribed number of hours (four hours, or twelve hours, or the next day), the voter may choose to go back to the ABB, to check that the data she entered are correctly listed. Again, she should preferably, though not necessarily, use another computer.
5. If the data are correctly posted, she locks-in her vote using a randomly scratched-off lock-in code, then displayed on the ABB.

This completes the voting process, however she is encouraged to monitor the ABB, either by just looking at it and checking that her numbers are correctly posted, or by using a program that checks digital signatures and previously-posted data for consistency.

6. If the ABB does not display her data correctly, the voter may retry from another computer.

If the voter revisits the ABB after locking-in and observes

incorrect data against her authentication card serial number, she may have proof of cheating (with non-negligible probability) because the numbers may not be the ones she scratched-off. Additionally, if she checks digital signatures immediately after the initial verification or after locking-in, she has proof if the ABB later attempts to change any data.

Voters can choose to mail-in the paper ballot or vote in person at any time during the protocol, or even after they have cast an electronic vote. Paper ballots over-rule electronically-communicated confirmation numbers, and a vote cast in person on election day over-rules all other votes.

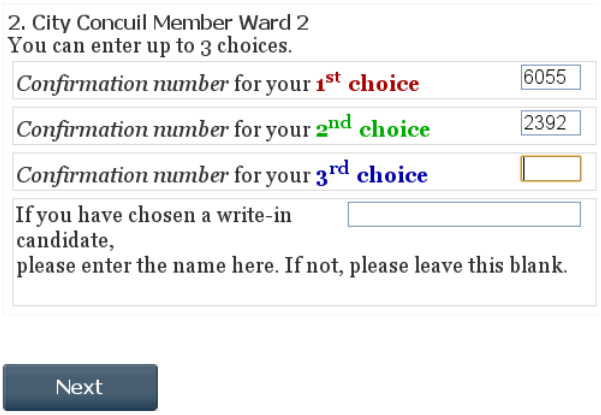
2. DEPLOYMENT

The prototyped system was used in the Takoma Park election of 2011. Board of Election members and the City Clerk reviewed many versions of the protocol and constantly urged simplification. Preliminary usability tests on a population of users who responded to an announcement by the city demonstrated that an original protocol which required lock-in was too complicated. It also demonstrated that instructions were not clear. We simplified the protocol and instructions for the final election.

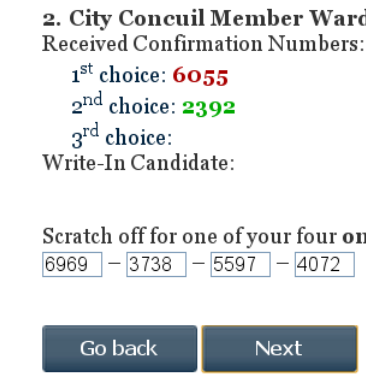
Appendix

CITY COUNCIL MEMBER WARD 2 *MIEMBRO DEL CONSEJO DE LA CIUDAD DISTRITO ELECTORAL 2*			
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*
Ward 2 Candidate 1	6055	3028	3106
Ward 2 Candidate 2	9480	2392	1257
Write-In Candidate/*Para añadir a un candidato*	3755	1222	6380

Figure 2: Part of a Scantegrity mail ballot with confirmation numbers. This figure omits the ballot web-serial number which is different than the authentication card's serial number.



(a) Voter enters confirmation codes corresponding to her choice



(b) Voter checks her choice and enters one time password

Figure 3: The Online Vote-Casting Procedure

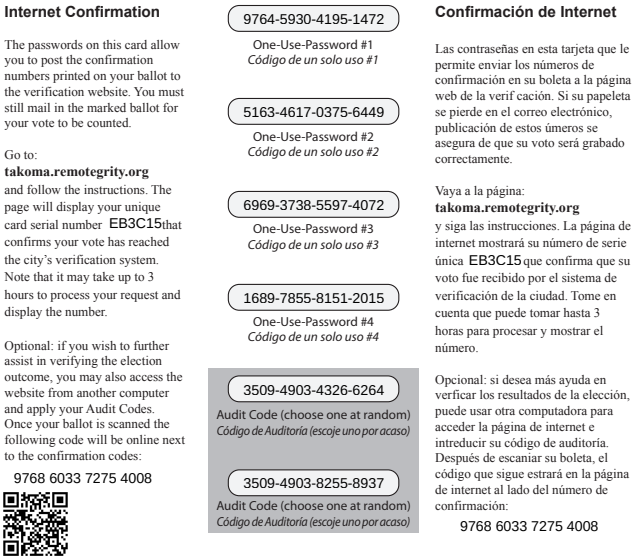


Figure 4: Remotegrity *Authentication Card*. All *one-use-passwords* and *audit codes* are under scratch-off.