# Diffusion of Voter Responsibility: Potential Failings in E2E Receipt Checking

Ester Moher, Jeremy Clark, & Aleks Essex .

Consider any simple mechanism that enables a user to detect a potential security threat

e.g., alarm, webcam light, a ballot receipt number

Consider any simple mechanism that enables a user to detect a potential security threat

e.g., alarm, webcam light, a ballot receipt number

Detecting the *mechanism* is not the same as detecting the *threat* 





## Somebody's Watching Me?

Assessing the Effectiveness of Webcam Indicator Lights

**Rebecca S. Portnoff<sup>1</sup>, Linda N. Lee<sup>1</sup>, Serge Egelman<sup>1,2</sup>, Pratyush Mishra<sup>1</sup>, Derek Leung<sup>1</sup>, and David Wagner<sup>1</sup>** 

<sup>1</sup>University of California, Berkeley, CA {rsportnoff,lnl,egelman}@cs.berkeley.edu, {pratyushmishra,derek.leung}@berkeley.edu <sup>2</sup>International Computer Science Institute, Berkeley, CA, egelman@icsi.berkeley.edu

### ABSTRACT

Most laptops and personal computers have webcams with LED indicators to notify users when they are recording. Because hackers use surreptitiously captured webcam recordings to extort users, we explored the effectiveness of these indicators under varying circumstances and how they could be improved. We observed that, on average, fewer than half of our participants (45%) noticed the existing indicator during computer-based tasks. When seated in front of the computer performing a paper-based task, only 5% noticed the indicator. We performed a followup experiment to evaluate a new indicator and observed that adding onscreen glyphs had a significant impact on both computer-based and non-computer-based tasks (93% and 59% noticed the new indicator, respectively). We discuss how our results can be integrated into current systems, as well as future ubiquitous computing systems.

### **Author Keywords**

Privacy Indicators; Ubiquitous Computing; Usable Security

### **ACM Classification Keywords**

K.6.5. Management of Computing and Information Systems: Security and protection: H.5.2. Information Interfaces and space of these privacy indicators, we examined the effectiveness of similar privacy indicators that are already sufficiently pervasive: webcam recording indicators.

For several years now, laptop sales have surpassed desktop sales [21], and with few exceptions, it is standard for a new laptop to come equipped with a built-in webcam. These webcams face the user and have indicator LEDs to communicate when the webcam is recording. Ideally, the user will notice the indicator, understand that a recording is being made, and take defensive actions in the event that the webcam is recording without the user's consent. Anecdotal evidence suggests that these assumptions are incorrect [13].

Remote Administration Tools (RATs) allow hackers to control an unsuspecting user's computer remotely, allowing them to execute programs, send taunting messages, or eavesdrop via the webcam and microphone [4]. In some cases, hackers have used videos of victims in various states of undress as part of "sextortion" plots: the perpetrator threatens to publicly post the captured videos and/or photos unless the victim pays a ransom [3]. The most famous case of this involved a high school classmate of Miss Teen USA who surreptitiously captured photos of her naked in her bedroom [19]. Unauthorized

### **Somebody's Watching Me?** Assessing the Effectiveness of Webcam Indicator Lights

Rebecca S. Portnoff<sup>1</sup>, Linda N. Lee<sup>1</sup>, Serge Egelman<sup>1,2</sup>, Pratyush Mishra<sup>1</sup>, Derek Leung<sup>1</sup>, and David Wagner<sup>1</sup>

<sup>1</sup>University of California, Berkeley, CA {rsportnoff,lnl,egelman}@cs.berkeley.edu, {pratyushmishra,derek.leung}@berkeley.edu <sup>2</sup>International Computer Science Institute, Berkeley, CA, egelman@icsi.berkeley.edu

### ABSTRACT

Most laptops and personal computers have webcams with LED indicators to notify users when they are recording. Because hackers use surreptitiously captured webcam recordings to extort users, we explored the effectiveness of these

be improved. We observed that, on average, fewer than half of our participants (45%) noticed the existing indicator during computer-based tasks. When seated in front of the computer performing a paper based task, only 5% noticed the indicator space of these privacy indicators, we examined the effectiveness of similar privacy indicators that are already sufficiently pervasive: webcam recording indicators.

For several years now, laptop sales have surpassed desktop sales [21] and with few exceptions it is standard for a new

laptop to come equipped with a built-in webcam. These webcams face the user and have indicator LEDs to communicate when the webcam is recording. Ideally, the user will notice the indicator, understand that a recording is being made, and

Nineteen participants reported that their webcam LED turned on when they were not using it. Almost all of them (18 of 19) believed this was normal behavior or just due to human error...

#### Author Keywords

Privacy Indicators; Ubiquitous Computing; Usable Security

#### ACM Classification Keywords

K.6.5. Management of Computing and Information Systems: Security and protection: H.5.2. Information Interfaces and ers have used videos of victims in various states of undress as part of "sextortion" plots: the perpetrator threatens to publicly post the captured videos and/or photos unless the victim pays a ransom [3]. The most famous case of this involved a high

tured photos of her naked in her bedroom [19]. Unauthorized

#### OFFICIAL BALLOT -- WARD 3

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

Do not fill in more than one oval per column. Do not till in more than one oval per conditate. Do not align numbers in the ranking sequence.

To vote for a person whose name is not primed on the baltot, write the name in the space princide and fill in one box in the column indicating your ranking of the write-in condstate.

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

Do not make any identifying marks on your ballot.

When you mark an uval 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 uning booth. Cluded de Takoma Park, Maryland ELECCIONES MUNICIPALES 3 DE NOVIEMBRE DE 2000

#### BOLETA OFICIAL- DISTRITO ELECTORAL 3

Instructiones. Interpret to condition industrial al condition due new superments species, of condition que and su separate species, y and backgloaments. Si is shoken, puede tradition and materialization scolaments of condition gain and superment species.

No reflere más de una casilla por cade columna No volume más de una casilla por cada candidate. No salte números en la accumente de clasificación por orden

Para votar por una paracria cuyo tiontore no auté impressi en la buess, escrita al nontre an el especia provisti y reliere una caselle en la columna para indicar el orden de classificación del candidato que se ha artactos

St useful conside on anton on au bokin, devuelt-exets al just y polar obta.

No hage marcas en su bolete que pueden identificarte.

Cuando usted marque la casille para votar por un candidate, verà un còdigo que podrà usar posteriormente para verificar su voto por Infernet. Ves la logo de instrucciones en la cabina de rotación

MAYOR ALCALDE			
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	Test churca fira specifie	2nd shores 2th update	Sed churks Ses species
Roger B. Schlegel	EED		
Bruce Williams			CED
Tom Smith Write-In Candidate/Para anadir a un candidato		-	

CITY COUNCIL MEMBER WARD MIEMBRO DEL CONSEJO DE LA CIUDAD DISTR	TO ELEC	TORAL 3
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	1stabala framote	2nd choice 2de optim
Dan Robinson		
Write-In Candidate/Para añadir a un candidato		-



3 - 972853 Online Verification Number Número de Verificación por Internet

OFFICIAL BALLOT --- WARD 3

Instructions: Vote for candidates to indicating your franthose candidate, your second choice candidate, and as on. You are free to rank only a first choice if you with

Do not fill in more than one oval per columns. Do not to in more than one oval per considerire. Do not skip numbers in the ranking sequence.

To vote for a person whose name is not primed on the ballot, while the name in the space provided and fill in sine boe in the column indicating your ranking of the write-in candidate.

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

Do not make any identifying marks on your ballot.

When you mark an avail 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 using booth. Cluded de Takoma Park, Maryland ELECCIONES MUNICIPALES 3 DE NOVIEMBRE DE 2000

#### BOLETA OFICIAL- DISTRITO ELECTORAL 3

Instruccionas into per tas conductos induando al conditido per nes au primero spolo, el condition que ano separate spolo, y ou bucequarentes. El la deseu puedo instruccionar potenente al condition que ana su primero spolo.

No relieve más de una casilla por cada enturena No estera rida de arte casilla por cada candidale. No asite números en la secuencia de clasificación por orden.

Para votar por una persona cuyo tiontore no asté impressi en la bueste, escrita al nombre en el especio provisit y reliere una caselle en la columna para indicar el orden de classificación del candidato que re ha añactido:

Si united contents are error err au bolette, devueltvesets al juez y pola obra.

No hage marcas en su bolete que pueden identificante.

Cuando usted margue la casille para votar por un candidate, verà un còdigo que podra usar posteriormente para verificar su voto por Infernet. Ves la logo de instrucciones en la Labate de rotación

Tet chalge fire species	2nd shores 2the sports	3rd chuster 3ra quode
SEED		
-		CHE
	CEED	
	Station .	EEEO

Rank candidates in order of choice Clasifique a los candidatos por orden da preferencia	1st shoke fra spoke	2nd choice 2de optimi
Dan Robinson	-	
Write-In Candidate/Para añadir a un candidato		



3 - 972853 Online Verification Number Número de Verificación por Internet

# Confirmation Code (056)

## , Ballot ID (3-972853)

OFFICIAL BALLOT - WARD 3

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

Do not fill in more than one eval per culume. Do not til in more than one dval per candidate. Do not skip numbers in the ranking sequence.

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

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

Do not make any identifying marks on your ballot.

When you mark an avail 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 using booth. Cluded de Takoma Pack, Maryland ELECCIONES MUNICIPALES 3 DE NOVIEMBRE DE 2000

#### BOLETA OFICIAL- DISTRITO ELECTORAL 3

Instruccionas into per tas conductos induando al conditido per nes au primero spolo, el condition que ano separate spolo, y ou bucequarentes. El la deseu puedo instruccionar potenente al condition que ana su primero ispolo.

No relieve más de una casilla por cada enturena No estera rida de arte casilla por cada candidale. No asite números en la secuencia de clasificación por orden.

Pare votar por una persona coyo nontine no auté impréseu en la buiete, escritur al rombre en el especio provieto y reliere una caselle en la columna para indicar el orden de classificación del candidato que re fra aflactido:

Si withid converte un error en au bolete, devuellveaete al juez y pida obra.

No hage marcas en su boleta que puedan identificanta.

Cuando usted marque la casille para votar por un candidate, verá un código que podrá usar posteriormente para verificar su voto por internet. Ves la hojo de instrucciones en la labite de votación

MAYOR ALCALDE			
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	Test churce fire spectre	2nd shoes 2th upper	Setil churkes Sets species
Roger B. Schlegel	EED		
Bruce Williams	-		CERT
Tom Smith	-	CELED	
Write-In Candidate/Para añadir a un candidato			

Dan Robinson

## Type in your Ballot ID:



3-972853

Online Verification Number Námero de Ferificación por Internet

# Confirmation Code (056)

, Ballot ID (3-972853)

OFFICIAL BALLOT - WARD 3

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

Do not fill in more than one eval per culume. Do not til in more than one dval per candidate. Do not skip numbers in the ranking sequence.

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

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

Do not make any identifying marks on your ballot.

When you mark an avail 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 using booth. Cluded de Takoma Park, Maryland ELECCIONES MUNICIPALES 3 DE NOVIEMBRE DE 2000

#### BOLETA OFICIAL- DISTRITO ELECTORAL 3

Instruccionas into per tas conductos induando al conditido per nes au primero spolo, el condition que ano separate spolo, y ou bucequarentes. El la deseu puedo instruccionar potenente al condition que ana su primero ispolo.

No relieve más de una casilla por cada columna. No estena rida de arte casilla por cada candulado. No auto números en la secuencia de clasificación por orden.

Pare votar por una persona coyo nontine no auté impréseu en la buiete, escritur al rombre en el especio provieto y reliere una caselle en la columna para indicar el orden de classificación del candidato que re fra aflactido:

Si withid converte un error en au bolete, devuellveaete al juez y pida obra.

No hage marcas en su boleta que puedan identificanta.

Cuando usted marque la casille para votar por un candidate, verá un código que podrá usar posteriormente para verificar su voto por internet. Ves la hojo de instrucciones en la labite de votación

MAYOR ALCALDE		1.5	
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	1st chatce trainin		Sed churks Ses quote
Roger B. Schlegel	EED		
Bruce Williams			CHE
Tom Smith	-	(III)	
Write-In Candidate/Para añadir a un candidato			

#### Dan Robinson

## Type in your Ballot ID:





Online Verification Number Número de Verificación por Internet

# Confirmation Code (056)

# , Ballot ID (3-972853)

City of Takoma Park, Maryland Cludied de Takoma Park, Meryland MUNICIPAL ELECTION ELECCIONES MUNICIPALES NOVEMBER 3, 2009 **Confirmation Code** 3 DE NOVIEMBRE DE 2009 OFFICIAL BALLOT --- WARD 3 BOLETA OFICIAL- DISTRITO ELECTORAL 3 Instructions: Vote for cardidates by indicating your feature instructions, you per no perchange integrate of perchange on shoke candidate, your second-choice candidate, and so on ness au primers spoiler, el cambinato que less au segurate specific, y You are been to rare only a first choice if you wish and approximation of an obvious possible instantion in antimotication (056)solumente ar candidato que ana 32 primera isposiei. Do not fill in more than one eval per column. Do not till in more than one oval per candidate. Do not aligi numbers in No reliene más de una casilla por caola poluming. No volume más the ranking sequence. de seta casilla por cada candidado. Ati auto economia an la pecuantos ale clasificación por ordem To yote for a person whose name is not primed on the baltot, write the name in the space provided and fill in one box Para ustar por una partorne cuyo nontore no esté impreso en la in the column indicating your ranking of the write-in condiformers, manythe all monitore an all anguants provident y reviews unter caustie state. air la columna para indicar al orden de clasificación del candicielo que He for all address If you make a mistake on your ballot, veturn it to the judge and get another. St untild consiste un antor en au bolets, devuell-easile al justi y picts. 1000 Do not make any identifying marks on your ballot. No hape marcae en su bolete que puedan identificaria. When you mark an sval to rank a candidate, a code will Ballot ID be revealed that you may later use to verify your vote Cuando usted marque la casille para votar por un candidate. online. See the instruction sheet in the upting booth verà un còdigo que podrà usar posteriormante para verificar su voto por Internet. Ves la hoja de indracciones en la cabina de **votación** (3 - 972853)MAYOR ALCALDE Rank candidates in order of choice 1st chatce 2nd shares Clasifique a los candidatos por orden de preferencia. **3rd** chuice Arg spectre Zofe spool-3/8 0000 Roger B. Schlegel 6.260 Bruce Williams Clair Tom Smith (EDE) Write-In Candidate/Para añadir a un candidato

### Type in your Ballot ID: <u>3972853</u>

Thank you. Your confirmation code is 856

Namero de Fertheación por Inter-

## Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy

Richard Carback	David Chaum	Jeremy Clark	John Conway
UMBC CDL		University of Waterloo	UMBC CDL
Aleksander Essex	Paul S. Herrnson	Travis Mayberry	Stefan Popoveniuc
University of Waterloo	UMCP CAPC	UMBC CDL	
Ronald L. Rivest	Emily Shen	Alan T. Sherman	Poorvi L. Vora
MIT CSAIL	MIT CSAIL	UMBC CDL	<i>GW</i>

### Abstract

On November 3, 2009, voters in Takoma Park, Maryland, cast ballots for the mayor and city council members using the Scantegrity II voting system—the first time any *end-to-end* (*E2E*) voting system with ballot privacy has been used in a binding governmental election. This case study describes the various efforts that went into the election—including the improved design and implementation of the voting system, streamlined procedures, agreements with the city, and assessments of the experiences of voters and poll workers.

The election, with 1728 voters from six wards, involved paper ballots with invisible-ink confirmation codes, instant-runoff voting with write-ins, early and absentee (mail-in) voting, dual-language ballots, provisional ballots, privacy sleeves, any-which-way scanning with parallel conventional desktop scanners, end-to-end learned. While the paper provides a simple summary of survey results, the focus of this paper is not usability but the engineering process of bringing a new cryptographic approach to solve a complex practical problem involving technology, procedures, and laws.

With the Scantegrity II voting system, voters mark optical scan paper ballots with pens, filling the oval for the candidates of their choice. These ballots are handled as traditional ballots, permitting all the usual automated and manual counting, accounting, and recounting. Additionally, the voting system provides a layer of integrity protection through its use of invisible-ink confirmation codes. When voters mark ballot ovals using a decoder pen, confirmation codes printed in invisible ink are revealed. Interested voters can note down these codes to check them later on the election website. The codes are generated randomly for each race and each ballot, and

## Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy

Richard Carback	David Chaum	Jeremy Clark	John Conway
UMBC CDL		University of Waterloo	UMBC CDL
Aleksander Essex	Paul S. Herrnson	Travis Mayberry	Stefan Popoveniuc
University of Waterloo	UMCP CAPC	UMBC CDL	
Ronald L. Rivest	Emily Shen	Alan T. Sherman	Poorvi L. Vora
MIT CSAIL	MIT CSAIL	UMBC CDL	GW
Abstract			provides a simple summary of f this paper is not usability but

On November 3, 2009, voters in Takoma Park, Mary-

survey results, the focus of this paper is not usability but the engineering process of bringing a new eryptographic

Scantegrity received a single complaint by a voter who had trouble deciphering a digit in the code and noted it as "0," while the Scantegrity website presented it as "8."

... He also stated that if he were not a trusting individual, he would believe that he had **proof** that his vote was altered.

sional ballots, privacy sleeves, any-which-way scanning with parallel conventional desktop scanners, end-to-end

generated randomly for each race and each ballot, and

OFFICIAL BALLOT -- WARD 3

Instructions: Vote for candidates to indicating your franthose candidate, your second choice candidate, and as on. You are free to rank only a first choice if you with

Do not fill in more than one eval per culume. Do not til in more than one dval per candidate. Do not skip numbers in the ranking sequence.

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

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

Do not make any identifying marks on your ballot.

When you mark an avail 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 using booth. Cluded de Takoma Park, Maryland ELECCIONES MUNICIPALES 3 DE NOVIEMBRE DE 2000

#### BOLETA OFICIAL- DISTRITO ELECTORAL 3

Instruccionas into per tas conductos induando al conditido per nes au primero spolo, el condition que ano separate spolo, y ou bucequarentes. El la deseu puedo instruccionar potenente al condition que ana su primero spolo.

No relieve más de una casilia por cada ostumena No volves rida de una casilia por cada candidale. No aute números en la accuencia de clasificación por orden.

Para votar por una persona cuyo tiontore no auté impressi en la buiete, escrita el nombre en el especio provisti y reliere una caselle en la columna pera indicar el orden de classificación del candidato que re fra añactido:

Si wolled converte un error en au bolete, devuelheasels al juez y pida obra.

No hage marcas en su boleta que puedan identificante.

Cuando usted marque la casille para votar por un candidate, verà un còdigo que podrà usar posteriormente para verificar su voto por Internet. Ves la logo de instrucciones en la labite de rotación

MAYOR ALCALDE			
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	Test churce fire specifies	2nd shores 2nd sports	Brd churke Bra spools
Roger B. Schlegel	SEE		
Bruce Williams			CED
Tom Smith	-	CEED	
Write-In Candidate/Para anadir a un candidato			

CITY COUNCIL MEMBER WARD MIEMBRO DEL CONSEJO DE LA CIUDAD DISTR	TO ELEC	TORAL
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	1stabalas fra quote	2nd choice 2de optim
Dan Robinson	1000	
Write-In Candidate/Para añadir a un candidato	-	-



3 - 972853 Online Verification Number Número de Verificación por Internet

# The receipt check is the weakest link in most E2E systems

## We wanted to stress test it

OFFICIAL BALLOT - WARD 3

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

Do not fill in more than one eval per columns. Do not to in more than one dval per conditate. Do not align numbers in the ranking sequence.

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

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

Do not make any identifying marks on your ballot.

When you mark an uval 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 using booth. Cluded de Takoma Park, Merytand ELECCIONES MUNICIPALES 3 DE NOVIEMBRE DE 2000

#### BOLETA OFICIAL- DISTRITO ELECTORAL 3

Instructiones you has sensitively industrial industrial of condition gas ness as primers species, of conditions gas and separate species, y and backgovernerse. Si is shown, punch investors and methodologic polariteries of condition gas and by primers (public).

No reliane más de una casilla por cada ontunena No velora más de una casila por cada candidale. No salte números en la accuencia de clasificación por orden.

Pare votar por una persona coyo tiontine no asté impressi en la buiete, escrita el nombre en el especio provisti y reliere una caselle en la solumna pera indicar el orden de classificación del candidato que re fra aflactido:

Si setted consets on arror en su bolets, devueltesaits al junz y pida oha.

No hape marcas en su boleta que puedan identificante.

Cuando usted margue la casille para votar por un candidate, verá un código que podrá usar posteriormante para verificar su voto por Internet. Ves la logo de instrucciones en la ública de rotación

MAYOR ALCALDE			
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	Test churce fire specifies	2nd shores 2nd sports	Brd churke Bra spools
Roger B. Schlegel	SEE		
Bruce Williams			CED
Tom Smith Write-In Candidate/Para anadir a un candidato		-	

CITY COUNCIL MEMBER WARD MIEMBRO DEL CONSEJO DE LA CIUDAD DISTR	TO ELEC	TORAL
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	1stabalas fra quote	2nd choice 2de optim
Dan Robinson	1000	
Write-In Candidate/Para añadir a un candidato	-	-



3 - 972853 Online Verification Number Número de Verificación por Internet

# The receipt check is the weakest link in most E2E systems

## We wanted to stress test it

## Question 1:

4% of receipts checked

??% would file a dispute?

OFFICIAL BALLOT -- WARD 3

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

Do not fill in more than one oval per column. Do not till in more than one oval per conditate. Do not akip numbers in the ranking sequence.

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

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

Do not make any identifying marks on your ballot.

When you mark an uval 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 using booth. Cluded de Takoma Park, Merytand ELECCIONES MUNICIPALES 3 DE NOVIEMBRE DE 2000

#### BOLETA OFICIAL- DISTRITO ELECTORAL 3

Instructiones your not consistent instruments of constitution does need to prevers upcoles, of constitution gate law sequence spectra, y and backglowerses. Si is shown, punch involves a selection of polymers of constitution gate and by prevent species.

No reliane más de una casilla por cada ontunena No velora más de una casila por cada candidale. No salte números en la accuencia de clasificación por orden.

Pare votar por una persona coyo tiontine no asté impressi en la buiete, escrita el nombre en el especio provisti y reliere una caselle en la solumna pera indicar el orden de classificación del candidato que re fra aflactido:

Si setted consets on arror en su bolets, devueltrepets al just y pida otra.

No hape marcas en su boleta que puedan identificante.

Cuando usted marque la casilla para votar por un candidate, verá un código que podrá usar posteriormante para verificar su voto por Internet. Ves la logo de instrucciones en la úsbisa de rotación

MAYOR ALCALDE			
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	Test churce fire specifies	2nd shores 2nd sports	
Roger B. Schlegel	EED		
Bruce Williams			CED
Tom Smith Write-In Candidate/Para anadir a un candidato		-	

CITY COUNCIL MEMBER WARD MIEMBRO DEL CONSEJO DE LA CIUDAD DISTR	TO ELEC	TORAL
Rank candidates in order of choice Clasifique a las candidatos por orden de preferencia	1stabala framote	2nd choice 2de optitu
Dan Robinson	1000	
Write-In Candidate/Para añadir a un candidato	-	-



3 - 972853 Online Verification Number Número de Verificación por Internet The receipt check is the weakest link in most E2E systems

## We wanted to stress test it

## Question 2:

4% checked when the result was reasonable

??% when it is fraudulent?



## Clowdflower (Canada's MTurk), 841 participants

# Asked people to vote for a charity to receive a donation (\$50 CAD)

### Charity vote!

As a thank you for participating, please vote for one of the five charities listed below.

We will donate \$50 to the charity that is selected by the largest percentage of participants, and let you know the outcome of the vote.

Please select one of the following:

- C United Way
- C Feeding America (food banks)
- C Livestrong
- O National Rifle Association
- C Church of Scientology
- O No Thanks/no vote

603 recipients completed their ballot and received an email with a link to the results

84 clicked

Half (42) were shown the correct result (Feeding America) and **22** checked their receipt

We inverted the results, reporting that the Church of Scientology won despite it receiving the least votes 603 recipients completed their ballot and received an email with a link to the results

84 clicked

Half (42) were shown the correct result (Feeding America) and **22** checked their receipt

603 recipients completed their ballot and received an email with a link to the results

84 clicked

Half (42) were shown the correct result (Feeding America) and **22** checked their receipt

Half (42) were shown the incorrect result (Scientology) and **32** checked their receipt

The result was significant

# Dispute Filing (Study 2)

# 

## REPORT SUSPICIOUS ACTIVITY CALL 800 492 TIPS

## Clowdflower, 755 participants

We tried to get an upper-bound on the number of reports:

- 1) Unexpected result
- 2) We primed the voter to anticipate the potential for error
- 3) We used an internet-savvy crowd

# We provide each voter who checked (7.4%) with an *incorrect* confirmation code and the ability to report it

	ź
Your confirmation code is:	
CRB	
If the confirmation code above is the same as your records, your vote has been counted correctly.	
If the confirmation code above is the NOT same as your records, your vote has been counted INCORRECTLY.	
To report a problem, click the link below:	
Report an error	
Finish	

We provide each voter who checked (7.4%) with an *incorrect* confirmation code and the ability to report it

• Report a problem
Please use the space below to report an issue with your vote:
The code was incorrect
*Please input your confirmation code to assist in resolving this dispute:
Finish

## How many voters reported the error?

## How many voters reported the error?



## (4 voters out of 755)

Not sure why the number is so low

Theories:

1) Bystander effect - someone else will report it

2) Knowledge gap - don't trust their own judgement

# 1,212,629

# 1,212,317

7.5% file disputes: detect fraud with 99.99%



7.5% file disputes: detect fraud with 99.99% 0.5% file disputes: detect fraud with 43.25%



If a malicious EA changes *n* receipts: *n* > margin of victory / 2
minimize *n* to avoid detection

# Replication

# Counter-measures

# Thank You Questions?

C Richard Bentley