



Computer Security Trends and Applications

Dan S. Wallach Department of Computer Science Rice University Houston, Texas, USA











Big trends in computer security

Cyber threats are everywhere

Any computer could be compromised

Worms/botnets on clients Drive-by downloads on servers

Skills are easy to learn

Broad literature Experiment at home

Dual-use tooling

Security auditing tools can also find and exploit vulnerabilities



The attackers are winning (?)

Defenders must fix all bugs

Attackers need only find one vulnerability

Nobody installs patches

But they're exploited quickly



Insider threats

Nation-state adversaries raise the bar

Stuxnet allegedly targeted Iranian uranium centrifuges

"Cyberwar" is poorly defined

Attackers don't care about crashing "innocent" machines

If a botnet kills 1% of its targets, that's not really a problem

Defenders can't respond in kind

- Difficult to disrupt without collateral damage
- Difficult to attribute to the actual source
- "Proportionate" response?
- Legality of operating outside of your country?
- Coordination with foreign governments?

Stuxnet infections

Country	Infected Computers
China	6,000,000
Iran	62,867
Indonesia	13,336
India	6,552
United States	2,913
Australia	2,436
United Kingdom	1,038
Malaysia	1013
Pakistan	993
Finland	7
Germany	5

Data from Wikipedia, Symantec, etc.

New attack surface: phones

Smartphones are real computers

Every bit as vulnerable to attacks as desktop computers Less manageable by systems administrators

Huge opportunities for targeted attacks

Microphone

GPS tracking

Phone networking

Perfect for spycraft







"I'm still clinging to my BlackBerry," Mr. Obama said Wednesday [7 Jan '09]. "They're going to pry it out of my hands." **They Jork Times**



Example challenge: Updates

Updates from the phone carrier?

UAE phone carrier, *Etisalat*, BlackBerry spyware (July '09)

What about the docking connector?

FlexiSpy and other commercial spy products

Vendor digital signatures on code?

Limits freedom of phone owners

TI calculator private keys were cryptanalyzed (Sept '09)

New attack surface: browsers

Web browsers are multi-"user" systems

Any web page might want to attack another

New browser features evolving rapidly

Engineering challenge: Isolation vs. collaboration

t k y hole	acebook 🛦 🗖 😡 🗍	Search	٩	Gmail Calendar Documer	nts Reader Web more ▼	
edit Mail Value Archive Reportspan Delete Move to v Labels v Stability Contacts Tasks Important and unread - Stability Condus Ntile Contacts Staff CS SHRT Size JSL on elay. Priority Inbox (22) Priority Inbox (22) Priority Inbox (22) Stability Condus Ntile Condus Ntile Congravation Priority Inbox (22)	an Wallach dit My Profile	🗉 News Feed	Top News - Most Recent			Search Mail Search the Web
Reque. Reque. Reque. Results Regue. Cardia Nittle Shirica Cardiy	ts 103 3	Honeysuckle Rose changed her profi		Contacts		ete 💌 📼 Move to 🔻 Labels 🔻
current/offlink Sabrial Cuddy Sabria Cuddy Sabrial Cuddy Sabrial Cuddy	Group	Claudia NEttle listed SCARFACE S		Priority Inbox (22)	II □ ☆ Electro ontier Foun. (II □ ☆ John G	 Support HTTPS Everywhere! - Dear [Csfaculty-I] Monday's COMP 600 ta
CSPub Image:	currently offline. with your friends, te.	6: Image: Sabrina Cudy Ariend of the Family makes thes Mandmade only 2 3 minutes ago - Like - Comment - Share Image: Sabrina Cudy 2 3 minutes ago - Like - Comment - Share Image: Sabrina Cudy 2 3 minutes ago - Like - Comment - Share Image: Sabrina Cudy 2 3 minutes ago - Like - Comment - Share Image: Sabrina Cudy 2 3 minutes ago via iPhoto Uploader - Like - Comment - Share			 FW: Event Summary (Reservation # Notification of Pay Stub Available i 	
Image: Strate of the state			DHS eCrime (41)	# □ ☆ club (# □ ☆ Lena S S (Faculty Club Statement - October 2 Balanced research funds reports - H 	
QuixoteGroup (3058) QuixoteGroup (3058) Image: Comment of the database of the comment of the comment of the database of the comment of the comment of the database of the comment of the da			HoustonCH (2069) mac-zfs-discuss (42)	🗄 🖯 😭 adam.pridgen	my research experience and plan -	
Image: Claudia NEttile Comment - Share Sysrack Cron (5) Image: Claudia NEttile Proposal Review - Here are the results for Usenix Sec 10 Claudia NEttile Usenix Sec 10 Image: Claudia Nettile Proposal Review - Here are the proposal Revi			QuixoteGroup (3058) Roberts	ii⊟ ☆ Yue Liu	counterfeit attack experiment result	
			Sysrack Cron (5) UsenixSec10	Adam Pridgen (3)	Proposal Reviews - Here are the pro	
			Search, add, or invite		 optimal classification selection - Hi paper - Hi, I finally cleared up the paper 	

Good web sites go bad

Syndicated advertisements, web host attacks

Even hit the New York Times' web site

Good web sites go bad

Syndicated advertisements, web host attacks

Even hit the New York Times' web site



	Tech	nical anal	ysis of th	ne NY Tim	nes attack:		
	http://troy.yort.c	com/anato	omy-of-a	a-malware	e-ad-on-nytin	<u>mes-com</u>	
00			-	My computer Or	line Scan		
• • C × A (http://protection-check07.co	om/1/?sess=%3Dm\	Wz9jDwMi02My	ZpcD03Mi4xNzguN	NTU4LjE2MCZ0aW1IPTEy	NTY4MQYMMQkM	😭 🔻) • 🔃 W 🔍 Wikipedi
ost Visited = Latest Headlines & U	SAA AKO Westlaw Lexis N	IYT BBC WP W	/SJ AJE Polit	ico Killeen Aust	tin Facebook Amazor	n Weather ShareThis	
oogle protection-c 🔻 🚼 Search	* 🛉 📲 • 💌 • 🚳 • 🎰 🏠	Bookmarks * 🐴	AutoLink 🔹 📍	🔄 AutoFill 🔻 🌛 [protection-check07		
My computer Online Scan	+						
System Tasks	System scan progress						
View system information	Shared Documents	My Documen	its				
Change a settings	Hard drives						
Other Places	Local Disk (C:)	Local Disk (D:)					
My Network Places My Documents							
Shared Documents	DVD-RAM Drive (E:)						
Details		56%					
My Computer System Folder	Now scanning: autoconv.exe	infected!					
Your Info	Threats and actions:						
IP: 72.178.158.160	Name	Risk level	Date	Files infected	State	*	
Country: United States City: Killeen	8 Email-Worm.Win32.Net	Critical	11.18.2008	36	Waiting removal		
Your private data is under attack!	🔞 Email-Worm.Win32.Myd	Critical	11.18.2008	65	Waiting removal		
						-	
	Description: This program is potentially danger personal information from your co		rojan-Download	er stealing passwords,	credit cards and other		
	Advice: You need to remove this threat as	soon as possible!				-	

۲				
	Full	system	cleanup	

Typical government policy (U.S. Marines, etc.)

Internet SNS are defined as web-based services that allow communities of people to share common interests and/or experiences (existing outside of DoD networks) or for those who want to explore interests and background different from their own. These Internet sites in general are a proven haven for malicious actors and content and are particularly high risk due to information exposure, user generated content and targeting by adversaries. The very nature of SNS creates a larger attack and exploitation window, exposes unnecessary information to adversaries and provides an easy conduit for information leakage that puts OPSEC, COMSEC, personnel and the MCEN at an elevated risk of compromise. Examples of Internet SNS sites include Facebook, MySpace, and Twitter.

http://www.marines.mil/news/messages/Pages/MARADMIN0458-09.aspx (August 2009)

Typical government policy (U.S. Marines, etc.)

a proven haven for malicious actors and content

actors and content and are particularly high risk due to information exposure, user generated content and

exposes unnecessary information to adversaries ... an easy conduit for information leakage

http://www.marines.mil/news/messages/Pages/MARADMIN0458-09.aspx (August 2009)

Typical government policy (U.S. Marines, etc.)

a proven haven for malicious actors and content

actors and content and are particularly high risk due to information exposure, user generated content and

exposes unnecessary information to adversaries ... an easy conduit for information leakage

http://www.marines.mil/news/messages/Pages/MARADMIN0458-09.aspx (August 2009)

Access is hereby prohibited to Internet SNS from the MCEN NIPRNET

Ban pushes personnel to use personal resources

Smartphones, Internet via private ISPs

The need for cryptography

Mid-90's debate: Strong crypto vs. key escrow

Debates centered around terrorists using unbreakable crypto Government key escrow: Vulnerable to attack? Conclusion: Strong crypto was essential for commerce

Strong crypto won, used most everywhere

Internet / Web standards: Carefully analyzed Other industries (e.g., SCADA, e-voting): Often very weak

Many web sites don't use crypto

Vulnerabilities were "hypothetical"

Firesheep codebutler.com/firesheep

Single-click attacks

Wi-Fi sniffer Browser integration Instant login / exploit



Solution? HTTPS everywhere (e.g., encrypted.google.com)

HTTPS everywhere?

Performance issues

Increased server cost Complicates caching

Trust issues for certification authorities

Browsers have hundreds of "roots" of trust Who do **you** trust?

Defeats traffic monitoring

Great Firewall of China wouldn't know what you were doing

00				Keychain Access	
Click to unlock the	e System Roots	keychain.			
Keychains					
🖞 login	Certificate	Staat der Nederlan	den Root CA		
PrivatedDatak	Red an	Root certificate authorit			
PrivatedDatak		Expires: Wednesday, De		3:15:38 AM CT	
System		This certificate is valid	d		
System Roots	Name		Kind	Data Madified	F undament
	-			Date Modified	Expires
		curity 1024 V3	certificate		Feb 22, 2026 2:01
		curity 2048 V3	certificate		Feb 22, 2026 2:39
		Certificate Services	certificate		Dec 31, 2028 5:59
	-	Global CA	certificate		Dec 31, 2029 1:52
	-	Trust CA	certificate		Dec 31, 2029 1:40
		y Comation EV RootCA1			Jun 5, 2037 9:12:
		Communication RootCA1			Sep 29, 2023 11:2
		Class1 CA	certificate		Apr 6, 2021 5:49:
	NAME	Class2 CA er Nederlanden Root CA	certificate		Apr 6, 2021 2:29: Dec 16, 2015 3:1
		er Neden Root CA - G2			Mar 25, 2020 6:0
		d Clasfication Authority			Jun 29, 2034 12:3
		om Certification Authority			Sep 17, 2036 2:46
Category		om Root CA 1	certificate		Aug 18, 2025 5:0
All Items	-	gn CA 1999 18:00:58)			Nov 26, 2031 5:2
. Passwords		gn Gold CA - G2	certificate		Oct 25, 2036 3:30
Secure Notes		gn Platinum CA - G2	certificate		Oct 25, 2036 3:36
My Certificates		gn Silver CA – G2	certificate		Oct 25, 2036 3:32
Keys		stCenter Class 1 CA	certificate		Jan 1, 2011 5:59:
Certificates		stCenter Class 2 CA	certificate		Jan 1, 2011 5:59:
		stCenter Class 2 CA II	certificate		Dec 31, 2025 4:5
	TC Tru	stCenter Class 3 CA	certificate		Jan 1, 2011 5:59:
	TC Tru	stCenter Class 3 CA II	certificate		Dec 31, 2025 4:55
	TC Tru	stCenter Class 4 CA	certificate		Jan 1, 2011 5:59:5
	TC Tru	stCenter Class 4 CA II	certificate		Dec 31, 2025 4:55
	TC Trus	tCenter Time Stamping CA	certificate		Jan 1, 2011 5:59:
	🖂 TC Tru	stCenter Universal CA I	certificate		Dec 31, 2025 4:5
	🖂 TC Tru	stCenter Universal CA II	certificate		Dec 31, 2030 4:5
	📴 TC Tru	stCenter Universal CA III	certificate		Dec 31, 2029 5:5
	📴 TDC In	ternet Root CA	certificate		Apr 5, 2021 12:03
	TDC O	CES CA	certificate		Feb 11, 2037 3:09
	📰 Thawte	Personal Basic CA	certificate		Dec 31, 2020 5:5
	🔝 Thawte	Personal Freemail CA	certificate		Dec 31, 2020 5:55
	📰 Thawte	Personal Premium CA	certificate		Dec 31, 2020 5:5
	🖂 Thawte	Premium Server CA	certificate		Dec 31, 2020 5:59
	📰 thawte	Primary Root CA	certificate		Jul 16, 2036 6:59:
	📰 Thawte	Server CA	certificate		Dec 31, 2020 5:59
		d Certificate Services	certificate		Dec 31, 2028 5:59
		RUSTHizmet Sağlayıcısı			Mar 22, 2015 5:22
		RUSTHizmet Sağlayıcısı			Sep 16, 2015 5:07
		RUSTHizmet Sağlayıcısı			Dec 22, 2017 12:
	_	Root Certification Authority			Dec 31, 2030 9:59
	-	DATACorp SGC	certificate		Jun 24, 2019 2:06
	_	SERFirication and Email			Jul 9, 2019 12:36:
ו		SEPEIrst-Hardware	certificate	169 item	Iul 9 2019 1-19-2

Can we beat the hackers?

Increasing computer power

Faster CPUs, more RAM, disk, network, etc.



Impact on computer security

Remember everything!

Network monitoring / email / web history / backups

Post-facto forensics, corporate auditing

Process and filter everything!

Anti-spam / anti-malware (also anti-pornography)

Potential to get ahead of the attackers

Caveat: Big data collection leads to serious privacy concerns

Better software engineering

Software auditing tools (e.g., Coverity and Fortify)

Scanning legacy code to detect large classes of bugs

New programming languages

Important classes of errors are flagged during development

"Security" as priority in the development cycle

Example: Microsoft will now favor security over backward compatibility in its engineering process

U.S. DHS Research Roadmap

http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

- 1. Scalable trustworthy systems
- 2. Enterprise-level trustworthiness metrics
- 3. System evaluation life cycle
- 4. Combatting insider threats
- 5. Combatting malware and botnets
- 6. Global-scale identity management
- 7. Survivability of time-critical systems
- 8. Situational understanding and attack attribution
- 9. Provenance
- **10. Privacy-aware security**
- 11. Usable security

Applied Security: Electronic Voting

DRE voting machines (Direct Recording Electronic)



DRE voting machines (Direct Recording Electronic)



touch screen / buttons graphical display





touch screen / buttons graphical display

flash memory

Sarasota, Florida

CD-13 Race, November 2006

Christine Jennings v. Vern Buchanan


In a nutshell...

Did voting machines steal a Democratic victory?

In Katherine Harris' old Florida district, more than 18,000 votes went missing -- and a Republican won a House seat by 369 votes.

By Katharine Mieszkowski

Print 🖴 | Email 🖂 | Digg it 🔛 | Del.icio.us 📲 | My Yahoo 💽 | RSS <u>N</u> | Font: S / S+ / S++

The recount is over in the 13th Congressional District in Florida. The lawyers have won -- and the Democrat has lost. As in the presidential election of 2000, that loss appears to have been caused by a glitch in the voting process. But this time, the controversy centers on the very electronic voting machines many counties around the country purchased after the 2000 election in hopes of avoiding the sort of debacle that produced Bush v. Gore.

On Monday, Florida election officials named Republican Vern Buchanan the victor in the race for the House seat that Katherine Harris -- the Katherine Harris who was Florida's secretary of state during the 2000 recount -- vacated to run for the Senate. The Florida Elections Canvassing Commission, which is made up of Gov. Jeb Bush and two other elected Republican officials, said that the results of the recount showed Buchanan had beaten Democrat Christine Jennings by 369 votes in a race where nearly 240,000 votes were cast. The commission awarded the victory to Buchanan despite the fact that the mystery of more than 18,000 missing votes has not been resolved.



Photo: AP/J. Scott Applewhite

Christine Jennings, the Democratic candidate in Florida's unresolved 13th Congressional District, second from left, after posing with freshman members of the House for a group photo on the steps of the Capitol in Washington on Nov. 14, 2006.

Did voting machines steal a Democratic victory?

In Katherine Harris' old Florida district, more than 18,000 votes went missing -- and a Republican won a House seat by 369 votes.

By Katharine Mieszkowski

Print 🖴 🛛 Email 🐹 📄 Digg it 🔛 👘 Del.icio.us 📲 🖂 My Yahoo 👥 📄 RSS 🔝 👘 Font: S / S+ / S++

The recount is over in the 13th Congressional District in Florida. The lawyers have won -- and the Democrat has lost.

Buchanan had beaten ... Jennings by 369 votes in a race where nearly 240,000 votes were cast.

produced Bush v. Gore.

On Monday, Florida election officials named Republican Vern Buchanan the victor in the race for the House seat that

... mystery of more than 18,000 missing votes ...

which is made up of Gov. Jeb Bush and two other elected Republican officials, said that the results of the recount showed Buchanan had beaten Democrat Christine Jennings by 369 votes in a race where nearly 240,000 votes were cast. The commission awarded the victory to Buchanan despite the fact that the mystery of more than 18,000 missing votes has not been resolved.



Photo: AP/J. Scott Applewhite

Christine Jennings, the Democratic candidate in Florida's unresolved 13th Congressional District, second from left, after posing with freshman members of the House for a group photo on the steps of the Capitol in Washington on Nov. 14, 2006.

Undervote rates by race

U.S. Senate	1.14%	Absentee	2.5%
Congress	12.90%	ES&S	
Governor	I.28%	iVotronic	14.9%
Atty General	4.36%		
C.F.O.	4.43%		

Theory #1: Rational abstention

Theory #1: Rational abstention

Nobody seriously believes this.

Theory #2: Human factors

Theory #2: Human factors

Were voters confused by the ballot design?

OFF	ICIA	L GENI	ERAL	ELI	ECTION	BALLO	T
	SAR	ASOTA	COUN	ITY,	, FLOR	IDA	
0.1	10.00	NOVE	1BER	7,	2006	T-d	

CONGRESS IONAL

UNITED STATES SENATOR (Vote for One)

Katherine Harris	REP
Bill Nelson	DEM
Floyd Ray Frazier	NPA
Belinda Noah	NPA
Brian Moore	NPA
Roy Tanner	NPA
Jrite-In	
//7	



	U.S. REPRESENTATIVE IN CONGRESS 13TH CONGRESSIONAL DISTRICT (Vote for One)	
Vern Buchanan		REP
Christine Jennings		DEM
	STATE	
	GOVERNOR AND LIEUTENANT GOVERNOR (Vote for One)	
Charlie Crist Jeff Kottkamp		REP
Jim Davis Daryl L. Jones		DEM
Max Linn Tom Macklin		REF
Richard Paul Dembinsky Dr. Joe Smith		NPA
John Wayne Smith James J. Kearney		NPA
Karl C.C. Behm Carol Castagnero		NPA
Write-In		
evious Page	Page 2 of 21 Public Count: 0	Next Page

Theory #3: Machine malfunction

Theory #3: Machine malfunction

Did engineering failures of the machines induce the underotes? Did voters see their undervotes on the summary screen? Poor touchscreen calibration

Poor touch sensitivity

Hardware and software failures

Manufacturing defects

Dan Rather Reports had a long piece on this issue

Angle of view to the screen

Theory #4:

No evidence to support this.

Exceptionally difficult to prove.

Never ascribe malice to what can adequately be explained by incompetence. – Napoleon

Machine vs. human error

Machine vs. human error

Critical concept relative to Florida law

If the summary screen showed "Jennings" and the machine recorded "none", then Jennings should win

Machine vs. human error

Critical concept relative to Florida law

If the summary screen showed "Jennings" and the machine recorded "none", then Jennings should win

Regardless, the machines failed to capture voter intent Experts on both sides agree Jennings would have won

"Recount"

Same results as before (largely meaningless)

"Recount"

Same results as before (largely meaningless)

"Parallel" election tests

Poorly conducted, inconclusive results

"Recount"

Same results as before (largely meaningless)

"Parallel" election tests Poorly conducted, inconclusive results

Software examination

Found nothing (but significant / unrelated security holes) Never looked at the hardware

State lawsuits

Judge denied plaintiff's discovery motion

State lawsuits

Judge denied plaintiff's discovery motion

Congressional Committee on House Administration GAO investigation affirmed result (Jennings conceded)

State lawsuits

Judge denied plaintiff's discovery motion

Congressional Committee on House Administration GAO investigation affirmed result (Jennings conceded)

Florida banned electronic voting systems Jennings ran again and lost to then-incumbent Buchanan

What's next?

What's next?

Four years later, we still don't know what happened Rice study: bad layout causes errors, but voters fix them Iowa study: slow touchscreens increase error rate Theory: Sarasota suffered from both problems

What's next?

Four years later, we still don't know what happened Rice study: bad layout causes errors, but voters fix them Iowa study: slow touchscreens increase error rate Theory: Sarasota suffered from both problems

We need better recount / challenge procedures Transparency is more important than vendor trade secrets

Make it easier to audit results after the election

every vote included is valid; every valid vote is included

Make it easier to audit results after the election every vote included is valid; every valid vote is included

Make it harder to make mistakes on election day

tolerate accidental loss/deletion



Make it easier to audit results after the election every vote included is valid; every valid vote is included

Make it harder to make mistakes on election day

tolerate accidental loss/deletion





Connect the machines together.

VoteBox's approach

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

D. Sandler, K. Derr, and D. S. Wallach, **VoteBox: A Tamper-Evident, Verifiable Electronic Voting System**. 17th USENIX Security Symposium (USENIX Security '08).

VoteBox's approach

Store everything everywhere

Massive **redundancy**

Stop trusting DREs to keep their own audit data

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

D. Sandler, K. Derr, and D. S. Wallach, **VoteBox: A Tamper-Evident, Verifiable Electronic Voting System**. 17th USENIX Security Symposium (USENIX Security '08).

VoteBox's approach

Store everything everywhere

Massive **redundancy**

Stop trusting DREs to keep their own audit data

Link all votes, events together

Create a secure timeline of election events

Tamper-evident proof of each vote's legitimacy

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

D. Sandler, K. Derr, and D. S. Wallach, **VoteBox: A Tamper-Evident, Verifiable Electronic Voting System**. 17th USENIX Security Symposium (USENIX Security '08).
How can I be sure my vote is faithfully captured by the voting machine?

polling place













a technique due to Benaloh [2007]

a technique due to Benaloh [2007]

at the end, instead of casting your ballot:

force the machine to **show it to you**

a technique due to Benaloh [2007]

at the end, instead of casting your ballot:

force the machine to **show it to you**

this happens on election day

no artificial testing conditions (versus "logic & accuracy tests")

the voting machine cannot distinguish this from a real vote until the challenge

voter makes selections









What is the commitment?

How do we force the machine to produce proof of what it's about to cast on the voter's behalf?

What is the commitment?

How do we force the machine to produce proof of what it's about to cast on the voter's behalf?

Benaloh's proposal

Print the encrypted ballot behind an opaque shield.

- You can't see the contents, but you can see the page.
- The computer cannot "un-print" the ballot.

What is the commitment?

How do we force the machine to produce proof of what it's about to cast on the voter's behalf?

Benaloh's proposal

Print the encrypted ballot behind an opaque shield.

You can't see the contents, but you can see the page.

The computer cannot "un-print" the ballot.

How do you test the commitment?

What is the commitment?

How do we force the machine to produce proof of what it's about to cast on the voter's behalf?

Benaloh's proposal

Print the encrypted ballot behind an opaque shield.

You can't see the contents, but you can see the page.

The computer cannot "un-print" the ballot.

How do you test the commitment?

View and decrypt it.

But decryption requires the private key for tabulating the whole election!

challenging the machine

challenging the machine

When challenged, the machine must reveal random nonce (part of the cryptosystem)

We can then decrypt this ballot (only) and see if it's what we expected to see

In Benaloh, the encrypted ballot is on paper

An **irrevocable** output medium

decrypting requires additional equipment

VoteBox's network serves the same purpose



































Overseas/military remote voting

Overseas/military remote voting

Usability (e.g., Benaloh scheme)

Overseas/military remote voting Usability (e.g., Benaloh scheme) Pushing research out of the lab

Overseas/military remote voting Usability (e.g., Benaloh scheme) Pushing research out of the lab

http://votebox.cs.rice.edu

Overseas/military remote voting Usability (e.g., Benaloh scheme) Pushing research out of the lab

> <u>http://votebox.cs.rice.edu</u> (Open source software distribution)