

China audience response

Advanced Manufacturer, specialized in voting system, huge selection!

Ads by Google


[Front Page](#) » [Archives](#) » [September 2008](#) »

["UC Computer Scientists Release Video on How to Hack a Sequoia Touch-Screen Voting Machine"](#)

[» Go to The BRAD BLOG front page](#) «

BRAD BLOG Featured Stories

 Blogged by [Brad Friedman](#) on 9/9/2008 9:01PM

[UC Computer Scientists Release Video on How to Hack a Sequoia Touch-Screen Voting Machine](#)

Experts from CA's 'Top-to-Bottom Review' of E-Voting Systems Demonstrate How to Insert Virus, Access Machines Without Disturbing 'Security Seals' in Hack Which Would Not Be Discovered Even in 100% Audit of 'Paper Trails' Single Malicious Individual Shown Flipping Entire 'Touch-Screen w/ Paper-Trail' Election in Seconds...

-- Brad Friedman

The Computer Security Group at the University of California Santa Barbara (UCSB) has [released](#) a short, chilling video demonstrating how a single person can hack an election on a touch-screen voting system --- even one with a so-called "Voter Verifiable Paper Trail" (VVPAT) added to it --- in such a way that it is highly unlikely that the manipulation would ever be detected by either the public or election officials.



The video which shows "just examples of the different ways in which the system can be compromised" is the latest in a similar string of such demonstrations that have been released over the last two years, all showing how easily electronic voting systems can be tampered with, often undetectably.

In the UCSB video posted below, the hack of Sequoia voting system being prepared for use in an entire county, is done in approximately 3 seconds, by a single person with simple insider access and a \$10 USB thumb drive. Every machine used in the county, in such a case, would be effected. Moreover, the viral hack would not be discovered by pre-election "Logic and Accuracy" testing --- in cases where election officials actually bother to perform such tests prior to elections --- nor would it likely be discovered even in the event of a complete, 100% post-election audit of the touch-screen "paper-trail" records.

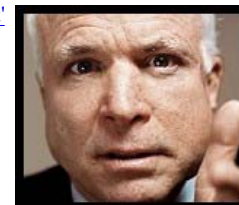
The hack demonstration, prepared by the UCSB scientists as part of California's 2007 ["Top-to-Bottom Review"](#) of all of the state's e-voting systems, also reveals how so-called "security seals" placed on such machines after they've been programmed for an election, can be easily defeated without detection...

How and Why It Was Done...

The landmark California study, which employed dozens of the world's top

[UPDATE: MS Judge Orders Special Senate Election to Top of Ballot](#)
[Dems Alarmed by McCain 'Absentee Ballot' Mail Campaign](#)


"Absentee Ballots Request" forms sent by the McCain camp to many voters in many states, raise Dem concerns of "vote caging" on Thom Hartmann show. Are the fears justified in this particular case? We try to figure it out...


 Related: [GOP Suppression, Tricks Seen in FL, MI, MS](#)

- [FL's 'No Match, No Vote' Will Disenfranchise Thousands: Experts](#)
- [Woodward: 'Secret Weapon' Now Used in Iraq. So What Is It?](#)
- [Prez Candidate on 'Manipulation of E-Voting Machines'](#)
 - [GOP Bigs Honor Anti-Democracy 'Founding Father'](#)
- [Election 'Glitch' in D.C. Fault of Sequoia - UPDATED: Sequoia Denies](#)
- [UC Video: Sequoia 'Paper Trail' System Hacked in Seconds](#)
- [V.A. Finally Relents, Will Follow Law, Allow Voter Registration](#)
 - [Audio: Brad Guest Hosting 'Randi Rhodes Show'](#)
 - [AZ Election Advocate Arrested During Hand-Count](#)
- [Candidates Asked to Take 'No Concessions' Pledge, Voters Asked to Demand It!](#)

Brad's Upcoming Appearances

(All times listed as PACIFIC TIME)

- **WED 9/17, 2:00pm:** Hosting KPFK's "Special Election Year Coverage", [KPFK/Pacifica](#) (90.7FM Los Angeles, 98.7FM Santa Barbara, Call-in#: 818-985-5735)
- **EVERY FRIDAY 5:00pm:** [Peter B. Collins, KRXA 540am](#) (Syndicated in CA, OR, WY, more, Call-in#: 888-5-PeterB)
- **TUE 9/23, 7:30pm:** Live Q&A appearance after screening of [Uncounted](#), w/ filmmaker David Earnhardt  (Fairfax Cinemas, 7907 Beverly Blvd., Los Angeles, CA)

[Media Appearance Archives...](#)

['Daily Voting News' For September 13, 2008](#)

by John Gideon

Voter registrations and voter registration data bases have been a huge problem during the primary elections. There is no reason to believe that they will not be a huge problem in November. One of the only ways to ensure a voter is registered is for that voter to check their registration.

We recommend every voter check now and then check again just before the voter's state registration closes before November. We urge voters who find themselves purged from the registration roles to write a letter of complaint to their local Board of Supervisors, especially their own representative, with a CC to their SoS, the local newspaper Editor, and their congressional members. If those responsible for representing the citizenry start receiving such letters they might act to eliminate the cause. You can find out the date that your state is closing registration and who to check to ensure your registration is still good [HERE](#): ...

[Click for links to all of today's notable voting news headlines...](#)
[\[DVN' Archives\]](#)
[\[Permalink\]](#) [\[Comments...\]](#)
BRAD BLOG'S 2008 ELECTION INTEGRITY FUND DRIVE!

computer scientists and security experts, was commissioned by Sec. of State Debra Bowen. The first-of-its-kind, independent state analysis, included hack tests --- so-called, "Red Team" attacks --- to analyze the security of the e-voting systems. All of the systems studied were easily defeated by the testers.

The UCSB group was in charge of the analysis of voting machines made by Sequoia Voting Systems.

The methods used in the hack of a Sequoia Edge direct recording electronic (DRE, touch-screen) system --- a system which includes the Sequoia Verivote paper-trail printer, as seen in the video --- were original described in the [Red Team security analysis \[PDF\] of the Sequoia systems](#) as published by the Secretary of State.

The video demonstrating the voting system manipulation was prepared at the same time, but had not been released publicly until now, despite the UCSB Security Group having encouraged the Secretary of State's office to do so for some time. The scientists involved in the tests declined to speak on the record as to their reasons for releasing it on their own at this time.

"We found a number of major flaws that can be exploited to compromise the integrity, confidentiality, and availability of the voting process," explains the [UCSB website where the video was released](#). "In particular, we developed a virus-like software that can spread across the voting system, modifying the firmware of the voting machines."

The page goes on to explain that "The modified firmware is able to steal votes even in the presence of a Voter-Verified Paper Audit Trail (VVPAT)."

In addition to the hack of the paper-trail touch-screen system, the UCSB scientists also demonstrate, in the video, how the Sequoia Edge touch-screen voting system may be accessed and manipulated even *after* so-called "security seals" have been applied to the machine following pre-election programming. The members of the team in the demonstration are seen access the system, while the plastic "security seals" are remain undisturbed in the process.

"Security seals" of this type, as used in California and elsewhere --- seen being easily defeated in the video --- have been cited by election officials and voting machine companies alike as key to the secure use of electronic voting machines such as the one seen being hacked in the video above.

E-Voting "Fatally Flawed"...

"The video shows how one can use a simple USB key to infect the laptop used to prepare the cards that initialize the various voting devices. As a result, the cards are loaded with a malicious software component," UCSB explains.



"When a card is inserted in a voting terminal, the malicious software exploits a vulnerability in the terminal loading procedure and installs a modified firmware, effectively 'brainwashing' the terminal. Later, when the terminal is used by the voters to cast their votes, the firmware uses a number of different techniques to modify the contents of the ballots being cast"

The UCSB Security Group page notes that electronic voting systems are exceedingly vulnerable to malicious manipulation of the type demonstrated in their video.

"While most critical systems are continuously scrutinized and evaluated for safety and correctness, electronic voting systems are not subject to the same level of scrutiny," they write.

"A number of recent studies have shown that most (if not all) of the electronic voting systems being used today are fatally flawed, and that their quality does not match the importance of the task that they are supposed to carry out."

The Latest of Many Such E-Vote Hack Demonstrations...

The Sequoia Edge system seen being hacked in the video above is the same type of system on which [The BRAD BLOG had revealed](#) another serious flaw, just days before the 2006 general election. As we reported at the time, a yellow button on the back of each voting machine (as can be seen in the

**SUPPORT DEMOCRACY!
GET COOL STUFF!
Click here for details!
Only you keep us going!**

COLLECTORS EDITION PREMIUMS for just \$5!

SUPPORT THE BRAD BLOG
PLEASE VISIT OUR ADVERTISERS

Brad Friedman's
The BRAD BLOG

[Go to front page...](#)

BRAD BLOG Premium Ads
ADVERTISE Here For Voters
Candidates!
Take The
Standing For Voters
Pledge!

In recent elections, too many candidates have quit before the results were final. Standing For Voters is asking candidates of all parties to pledge to wait for the votes to be counted before conceding, and to challenge suspicious results. Has your candidate taken the pledge?
[Read more...](#)

[Click here to create a BRAD BLOG Premium Ad now!](#)

Ads by Google

1 rule of a flat stomach:
Cut down 9 lbs of stomach fat every 2 weeks by obeying this 1 tiny rule
[FatLoss4Idiots.com](#)

voting machine-China
Competitive price
audience response
electronic voting products for you!
[www.sunVote.com.cn](#)

Rohan Fitzgerald
A strong local voice
Fighting for Gippsland's future
[www.rohanfitzgerald.com](#)

Internet Security Tools
Free Internet Security Scan. Winner of Best Anti-Spyware, Rated 5 Stars
[www.PCTools.com](#)

Barack Obama
Will He Win the 2008 US Election? Read Exclusive Coverage Here.
[www.crikey.com.au/US-Election](#)

- [Recent Entries](#)
- [Archives](#)
- [Important Docs](#)

- [Categories](#)
- [A Few Great Blogs](#)
- [Political Cartoonists](#)

Special Coverage Pages...

[NM GOP/Rep. Heather Wilson 'Vote-Buying' Scandal](#)



[Ann Coulter's Voter Fraud Felony](#)



[L.A. County 'Double Bubble' Debacle](#)



[Thor Hearne's 'American Center for Voting Rights' GOP 'Voter Fraud' Scam](#)



[2008 New Hampshire Primary Mess](#)



[Rush Holt's Election Reform Bill \(HR811\)](#)



[Riverside CA, Sequoia Hack Challenge](#)



['04 White House Website Scrubbing](#)



[Tom Feeney/Clint Curtis Voting Rigging Scandal Summary... Key Articles/Docs...](#)



(Needs updating)
[DOWN FOR THE COUNT: Diebold, DIEB-THROAT & Deep Trouble for America's Voting Machine Company...](#)

· [Make The BRAD BLOG your Homepage!](#)

· [Add The BRAD BLOG to favorites/bookmarks!](#)

· Or syndicate The BRAD BLOG...

XML RSS

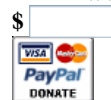
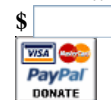
· [Select a BRAD BLOG color scheme...](#)

[Dark on Light \(DEFAULT\)](#) [Classic BRAD BLOG](#)

Please Help Support The BRAD BLOG...

One-time
any amount you like...

Monthly
any amount you like...



UCSB video as well) can be pressed in such a way as to put the system into "manual mode," allowing for an unlimited number of votes to be cast by a single individual.

The hack demonstration video published by the California academics wouldn't be the first such video to detail exactly how an electronic voting system can be hacked by a single malicious individual. Other notable cases include:

- A 2006 Princeton University study revealed how to carry out a similar viral attack on a Diebold touch-screen voting systems, resulting in the spread of a vote-flipping virus, that would spread from machine to machine after access to just one of them (*DISCLOSURE: The machine used in Princeton's testing was supplied to us by a Diebold insider. We then passed it on to the university for the first such independent study of such a voting system.*) [Story here](#), [video demo here...](#)



- While the Princeton scientists also demonstrated how the lock on a Diebold touch-screen system could be opened with either a standard hotel mini-bar key --- or even a paper clip in about 10 seconds time --- another enterprising individual found he was able to fashion a homemade key that would open the Diebold system as well. The key was made after modeling it after a photograph of the key --- the same one is used for every Diebold machine --- as, incredibly enough, posted on the company's website. [Story here](#), [video here...](#)



- A 2006 HBO documentary, [Hacking Democracy](#), showed a paper-based, Diebold optical-scan tabulator being manipulated in a mock election which flipped the results reported by the system. That landmark hack disclosed still-uncorrected security flaws in all Diebold systems (both touch-screen and optical-scan). The exact same Diebold, paper-based tabulators were used in last January's [anomalous New Hampshire primary](#). [Video here...](#)



- A one-minute 2006 hack demonstration of an e-voting system used in the Netherlands, shows how a key chip can be replaced in such a system in just 60-seconds. [PDF analysis here](#), [video here...](#)

"Paper-Trails" Are Meaningless...

The UCSB demonstration of the Sequoia Edge with Verivote hack is notable, however, given that many proponents of electronic voting --- including many Democrats and their various public interest group supporters, such as People for the American Way (PFAW), Common Cause, Verified Voting, NYU's Brennan Center for Justice and others --- have argued that adding paper-trails (VVPATs) to such systems would mean that any manipulation of the system would be discovered during an examination of the paper-trails after an election. As the video shows, post-election examinations or audits of touch-screen paper-trail systems hacked in this way, would not easily --- if at all --- reveal the manipulation.

Following Bowen's "Top-to-Bottom Review", touch-screen systems made by Sequoia, Diebold and ES&S were restricted to use of one-per-precinct only, in order to marginally meet the disabled-accessible voting requirements of the federal Help America Vote Act (HAVA). She also required a 100% hand-count of the paper-trails produced by such systems, even though the UCSB team found that such audits would not necessarily catch voting system manipulation. Many states around the country continue to allow unfettered use of such hackable voting systems. None, other than California, require 100% post-election audits.

A similar DRE system made by Hart InterCivic was allowed for full use,

[Matt Taibbi](#)
New \$16.32

[The Big Sort](#)
Bill Bishop
New \$16.50

[Change We Can Believe In](#)
Barack Obama
New \$8.37

[The Audacity of Deceit](#)
Brad O'Leary
New \$17.13

[What It Takes](#)
Richard Ben Cramer...

[Privacy Information](#)

Or by Snail Mail

Make check out to...

Brad Friedman
7095 Hollywood Blvd., #594
Los Angeles, CA 90028

The BRAD BLOG receives no foundational or corporate support. Your contributions make it possible to continue our work.
About Brad Friedman...

- [Bio & Testimonials](#)
- [Media Appearance Archive](#)
- [Articles & Editorials Elsewhere](#)
- [Contact](#)

Additional Stuff...

[Brad Blog Named...](#)



The BRAD BLOG - Year in Review 2006

[Part 1](#) - [Part 2](#) - [Part 3](#)

Other Brad Related Places...

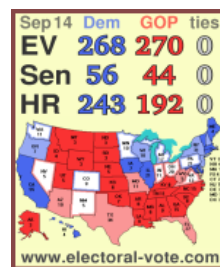


Contact Congress

Enter your ZIP code and contact your representatives

Contact the media!





almost inexplicably, after the California testing, in two different counties.

Despite the quickly mounting scientific evidence persuading against the use of such systems in American elections, Congressman Rush Holt (D-NJ) and Senator Diane Feinstein (D-CA) have proposed a number of bills which would allow for the continued use of touch-screen voting systems with paper-trails. The Republican caucuses in each chamber have so far stymied all such legislation, even as they argue in favor of the use of all such electronic systems, with or without the often misleading paper-trails.

MORE COVERAGE: See [John Byrne at RAW STORY](#) and [Rady Ananda at OpEdNews](#).

Prices now *slashed* in [The BRAD BLOG's 2008 Election Integrity Fund Drive!](#) Please support our continuing coverage of your election system, as found *nowhere* else. [Click here](#) for a number of cool new collector's edition Premium products **now available starting at just \$5!**



[[Print Version](#)] [[Email it!](#)] [[Permalink](#)]

[Categories for this item: [Diebold/Premier](#), [Election Irregularities](#), [Debra Bowen](#), [California](#), [Election Reform](#), [Sequoia Voting Systems](#), [Election Fraud](#), [Election 2008](#)]



« [PREVIOUS STORY "Open Thread"](#)
 » [Go to The BRAD BLOG front page](#) «
 "[John McCain Puts Lipstick on a Lie](#)" [NEXT STORY](#) »

READER COMMENTS ON

"[UC Computer Scientists Release Video on How to Hack a Sequoia Touch-Screen Voting Machine](#)"

(20 Responses so far...)

COMMENT #1 [[Permalink](#)]

... [LEFTISBEST](#) said on 9/9/2008 @ 11:58 pm PT...

This is likely the most significant and damaging video of Sequoia ever published. It pulls the eyelids off all the lies Sequoia has manufactured about the problems being with voter-errors, poll worker errors, ROV staff errors, but NEVER with the incredibly primitive "security" software and hardware barriers erected by Sequoia. Sequoia ALWAYS had the answer - it was to point the finger anywhere but at itself.

It is time for Counties to rise up in unison and sue Sequoia for violation of warranty of merchantability and false advertising. It has never delivered a dependable product, has ALWAYS been extremely vulnerable to insider and Sequoia support fraud, yet seeing it demonstrated so blatantly here makes it all so easy to understand how an election can be flipped in a matter of seconds.

Elections officials, Boards of Supervisors, and election integrity advocates should all be on the same side after viewing these two videos (one is 9 minutes and the second one is 7 minutes). It is really critical to stay and watch the second one as well, it shows how the hardware seals are useless against anyone bent on defeating the seals and shows how critical it is to have the machines 100% totally secured at all times. Any "sleepovers" where machines are stored in public locations (like public bathrooms in Riverside!), poll workers' homes and garages, etc. for up to 10 days or more before the election make them easy targets for any political operatives, of either party.

The second video also shows how the Sequoia Optec 400 C high-speed programmable scanners are also easily (but with a bit more difficulty) hacked in a period of minutes.

No longer can elections officials claim that it can't happen here, not with Sequoia equipment. This information was released a year ago in the Red

Telephone:

Precinct:

Type of problem:

Details of problem:

Were you able to successfully vote?
 No Yes
 By clicking 'Share my story' I have read and agree with disclosure policy.

Admin

• [Login](#)

Team report from the Secretary of State's office report, but only now are we seeing it demonstrated so vividly. Seeing IS believing.

And NO, it's not because they (the scientists) had access to all the Sequoia proprietary code and unlimited working time. So do the Sequoia technicians who offer "patches" to be installed whenever they say they are needed, without getting them approved by the Secretary of State. These "patches" could contain exactly the kind of trojan horses demonstrated in the video. And since the ROVs are not allowed to see the software, they are unwitting partners to any scam Sequoia choses to run. The gig is now up - electronic voting machines and electronic counting machines cannot be trusted - do not trust that which you cannot see.

The ONLY way to ensure transparent, accurate and secure elections is to require all paper ballots and hand count them in the precincts on election night before they ever leave the precinct. Post the results with a copy going to the central tabulator (if one is still employed) and then match the hand count against the machine. Hand counts, done twice before ever leaving the precinct (performed by a fresh team of election board members) have a much higher likelihood of being correct than a hackable, manipulatable, programmable black box where no one can see the bits and bites whizzing around in cyberspace. Electrons and Elections don't mix.

COMMENT #2 [[Permalink](#)]

... EWASTUD said on 9/10/2008 @ 12:30 am PT...

It is frightening and hard to believe that our elections are still mostly at the mercy of such deliberately flawed technology and corrupt government officials.

COMMENT #3 [[Permalink](#)]

... JS said on 9/10/2008 @ 5:06 am PT...

An article on truthout says that the neocons are already getting ready to steal the vote in Ohio, there must be something that can be done to stop this madness.

COMMENT #4 [[Permalink](#)]

... SHAKESPURR said on 9/10/2008 @ 9:29 am PT...

This video is too slow, long and methodical to keep the viewer's attention. I am as rabid about this stuff as anyone, but I was getting bored with it. There needs to be an edited, punched-up version that is only two or three minutes long (with a link to the longer version, possibly).

COMMENT #5 [[Permalink](#)]

... LEFTISBEST said on 9/10/2008 @ 11:19 am PT...

I agree with Shakespurr. It is WAY too long. We don't need to see the "voter" punching every possible vote in every scenario. We get the idea.

It can cut to the chase on each of the scenarios, and get the second video contents onto the shortened one b/c it shows the ease with which the seals are defeated and how the Optech 400-C can be compromised.

Otherwise the media won't do squat with it. Who do we need to get to to see about shortening this up and reissuing it?

COMMENT #6 [[Permalink](#)]

... LEFTIST said on 9/10/2008 @ 12:28 pm PT...