Increasing the security of your election by fixing it

Daniel C. Silverstein
dans@csua.berkeley.edu

Damon McCormick
damonmcc@uclink.berkeley.edu

Part One:

Disaster Strikes

The 2000 US Presidential Election led many to question the accuracy of paper ballot systems

Several companies seized on this opportunity to promote electronic voting systems:

- Election Systems & Software
- Diebold Election Systems
- Hart InterCivic
- Sequoia Voting Systems

Lofty Promises Made

- "...three independent but redundant memory paths ensure that no votes will ever be lost or altered." [1]
- "...World-class encryption techniques utilized to store election results." [2]
- "Proprietary firmware on closed system prevents hacker access." [3]

The Message?

- Trust Us!
  - We know what we’re doing!
  - Of course we don't have bugs!
  - Don't have security holes either!
    - And, even if we did, (which we don’t) nobody could *ever* actually exploit them

The End

And so, Democracy was made safe from evil hackers

Or Not

If it looks like snake oil...

And it smells like snake oil...

And it tastes like snake oil...

It’s probably snake oil [4]

Pop Quiz 1

Q: What's the first thing you do after rooting a box?

A: Hide your presence

Q: What's the second thing you do after rooting a box?

A: Patch the hole you came in through
(so nobody else can use it)

Pop Quiz 2

Q: How do you tell that someone rooted your box?

A: Good question!

Forensics analysis is hard!

- You can't trust information from a compromised machine.

Pop Quiz 3

Q: How do you tell that someone tampered with the electronic voting machine you just used to vote?

A: You don’t

No Paper Trail

- The major commercial electronic voting machines do not produce a voter verifiable paper trail
  - Though, thanks in part to the work of David Dill [5], some of the vendors are testing prototypes that do
- Without a paper trail, thre is *no* way to detect tampering

Setec Astronomy

- The major commercial electronic voting systems are proprietary platforms, protected as trade secrets
  - Members of the security community at large cannot scrutinize the machines without signing prohibitive Non-Disclosure Agreements
  - We must trust the vendors to detect machine tampering or malfunction
  - In practice, security through obscurity doesn't help
    - Just look at Microsoft's security record

Too Little Data

- There is little public data on how electronic voting systems behave in a real election setting
  - Not possible to verify the tally in a secret ballot
- Performing a realistic test would be difficult
  - Require thousands of volunteers
  - Expensive
  - Easy to cheat
- Independent third parties can't verify operation of systems without signing an NDA
  - No way to publish results!

The Big Problem

- Electronic voting systems may be worse than paper systems!
- There are numerous avenues of attack on computer ballot systems that simply have no analogue in a paper ballot system

The Big Problem

- Electronic voting raises unique security issues
- Failure to understand these issues could leave US State and Federal elections open to unprecedented fraud!

Part Two:

The Associated Students of the University of California (ASUC) Online Election System (OES)

> "If paramilitary rebels were to take over a voting kiosk and force computer scientists to work day and night, they would still not be able to lodge a single false ballot or affect the outcome."
>
> --Tommaso Sciortino, ASUC Elections Chair [6]

Online Election System

- OES represents a unique opportunity to analyze the security of an electronic voting system
  - Though not fully open, the source to OES was available on request and without an NDA
  - Over 30,000 students were eligible to vote in the election
    - Approximately 9,000 votes were cast
  - We reviewed OES in April 2003; this was its first run.

OES Architecture

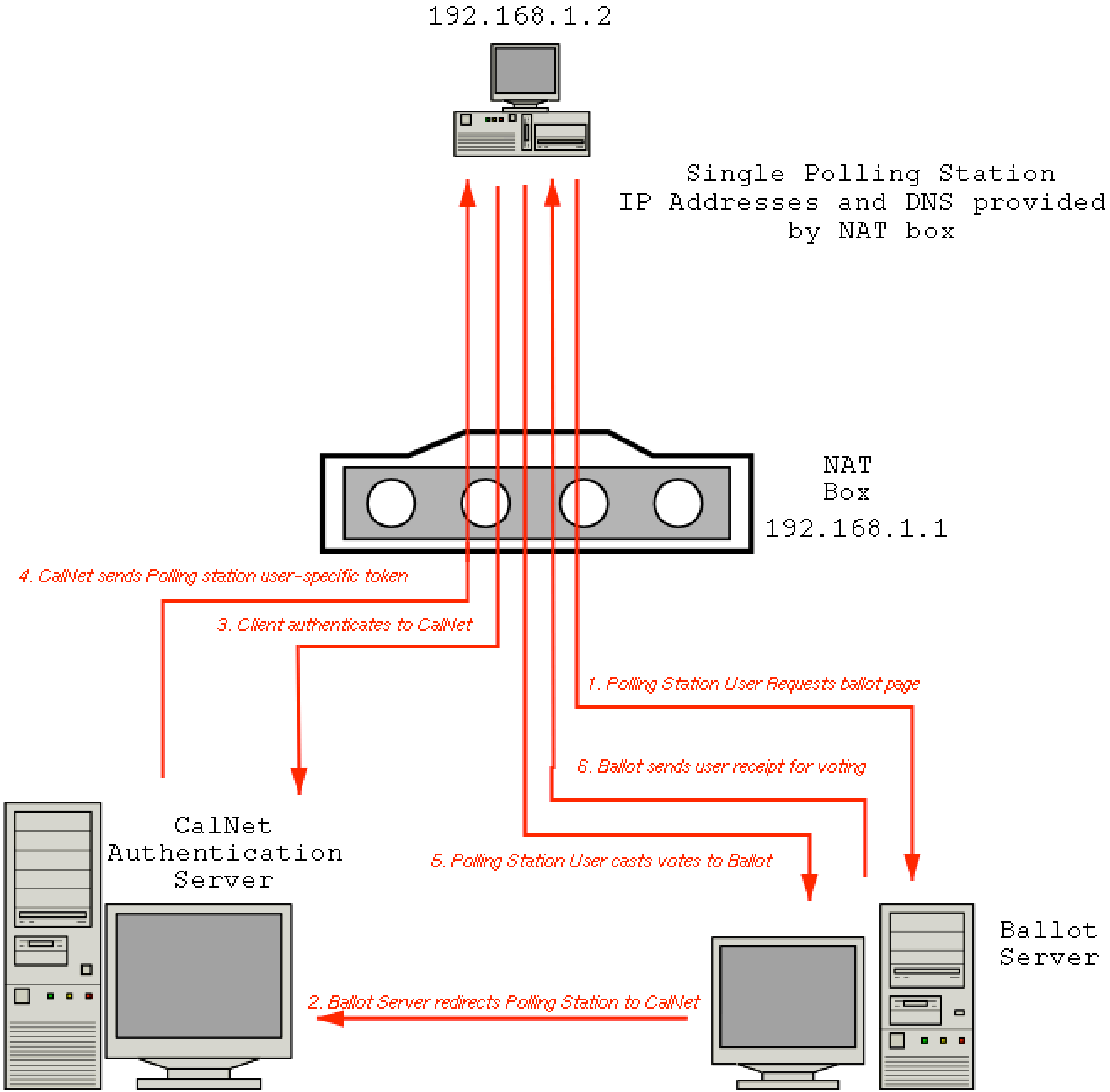
- Ballot Server
- Authentication Layer (CalNet, CalNetAWS)
- Polling Stations

Ballot Server

- The Ballot Server hosts a simple web application students access via a web browser at one of the polling stations
- The voting application works as follows:
  - If necessary, redirect user to CalNet for authentication
  - Perform sanity checks (has user already voted?)
  - Record users vote
- The Ballot Server ran Red Hat 8
- OES was implemented with Macromedia ColdFusionMX on Apache 2.0, using MySQL as a backend database.

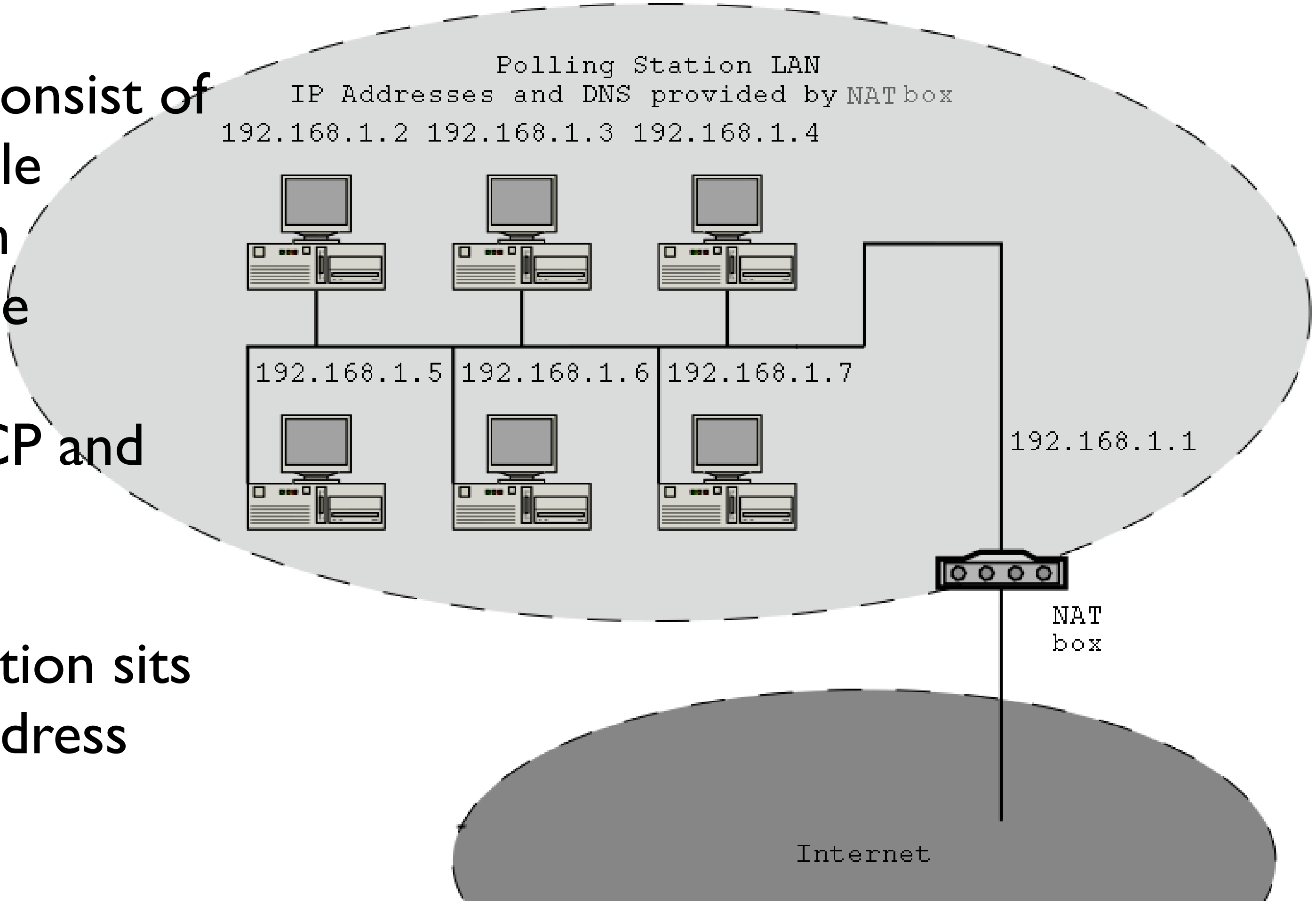
Authentication Layer (CalNet)

- CalNet [7] is UC Berkeley’s central Kerberos authentication system
  - Implemented via Microsoft Active Directory
- Polling station clients authenticate via Kerberos web proxy
- Upon successful authentication, a signed authentication token is passed to the clients web browser


192.168.1.2
Single Polling Station
IP Addresses and DNS provided by NAT box
NAT Box
192.168.1.1
4. CalNet sends Polling station user-specific token
3. Client authenticates to CalNet
1. Polling Station User Requests ballot page
6. Ballot sends user receipt for voting
CalNet Authentication Server
5. Polling Station User casts votes to Ballot
Ballot Server
2. Ballot Server redirects Polling Station to CalNet

Polling Stations

- Polling stations consist of three to ten Apple iBooks behind an inexpensive home router/gateway performing DHCP and NAT
- Entire polling station sits behind one IP address



OES Security Assumptions

- Traffic that polling station clients exchange with CalNet and the Ballot Server is sent via https
  - In principle, this should make it impossible to read or alter traffic
- The security of the election hinges on the security of the CalNet system

Ballot Server Defense

- Physical security emphasized
  - Election officials seemed to have serious concerns that someone would try to break into the server room and steal the server
- Basic network security aspects ignored
  - The database listened for requests from external hosts
  - Access was not restricted exclusively to web traffic originating from one of the known polling stations

Ballot Server Attacks

- It is trivial to tamper with a machine with physical access
    - Election officials implemented strong physical security measures
    - Physical security doesn’t protect against social engineering
- As initially configured, the open database port was the most obvious point of attack

Ballot Server Attacks

- Adding a firewall raised the bar considerably
  - Only traffic from the polling stations on ports 80 and 443 was allowed through
  - An attack would require preparing an exploit in advance, storing it on removable media, and running it from a polling station client

CalNet Defense

- CalNet is not written or managed by the OES developers
- CalNet authentication tokens are timestamped, and have a limited lifetime

CalNet Attacks

- Compromising any of the CalNet machines would be a bad idea
- Capturing authentication tokens does not require compromising CalNet's servers
    - Regardless of the short lifetime, tokens can be replayed

Polling Station Defense

- The election staff originally planned to use computers rented from students for the polling stations
- We suggested that election officials create an unprivileged account on the iBooks that only had permissions to run a web browser
- Default passwords on the router/gateway boxes were changed

Polling Station Attacks

- Had election officials actually used rented student computers, one could give them a trojaned machine
- Even with machines that are reasonably well locked down, it is virtually impossible to protect a machine from tampering if the user has physical access
  - Polling stations were monitered, but voters were supposed to have private voting booths.

Polling Station Attacks

- The key idea here is the need for trusted endpoints
  - Proving the trustworthiness of a machine is incredibly difficult.
  - Conventional hardware is not designed to be tamper resistant
- Tampering with individual clients would be time consuming.
  - 70+ machines spread across 15 polling stations.
- Is it possible to compromise an entire polling station in one fell swoop?

Part Three:

Man-in-the-Middle Attack on OES

Summary

- We want to acquire CalNet tokens so that we can replay them to the Ballot Server to cast fraudulent votes
- It is not possible to sniff the tokens because clients access CalNet and Ballot Server over https
- But we can trick the client into giving us a valid token by making it believe that our man-in-the-middle is the Ballot Server

The Attack

- We will construct a man-in-the-middle box, which we refer to as fakeballot
- Fakeballot is a drop-in replacement for the router/gateways that perform NAT at each polling station
- For this attack, we will need:

Ingredients

- ☑ 1 x86 PC
- ☑ 2 network interfaces
- ☑ 1 GNU/Linux distro (Debian)
- ☑ 1 DNS server (djbdns)
- ☑ 1 DHCP server (ISC DHCP)
- ☑ 1 web server with ssl support (apache + mod_ssl)
- ☑ 1 SSL certificate featuring the FQDN of the Ballot Server signed with a bogus CA (Verisign Inc.) [8]

NAT and DHCP

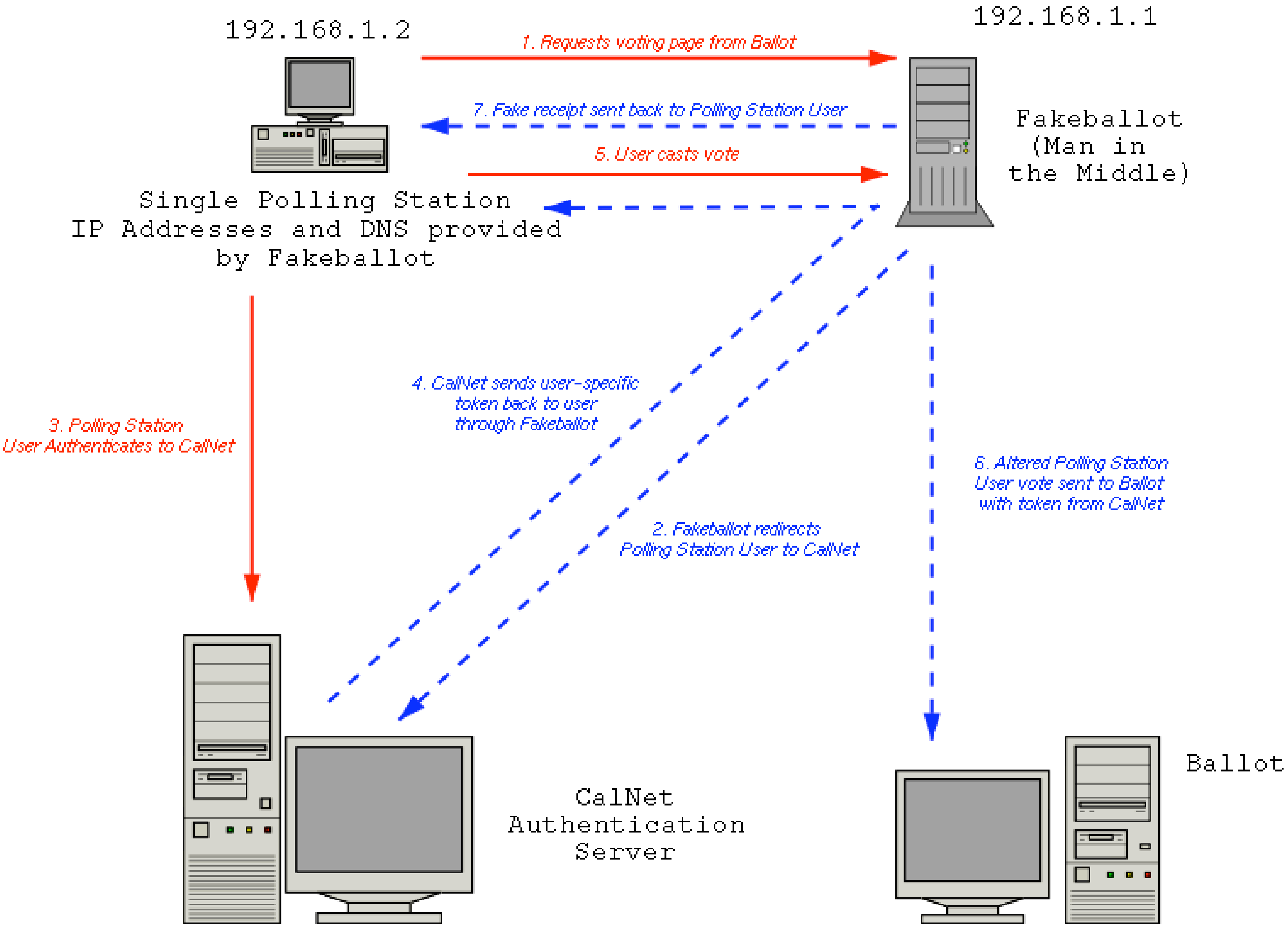
- Configuring linux to perform simple NAT is an iptables one-liner
  - The external IP of fakeballot will be the IP of the polling station we will compromise
  - The internal IP of fakeballot will be 192.168.1.1
- fakeballot runs a DHCP daemon that returns its own IP as the only nameserver

DNS Spoofing

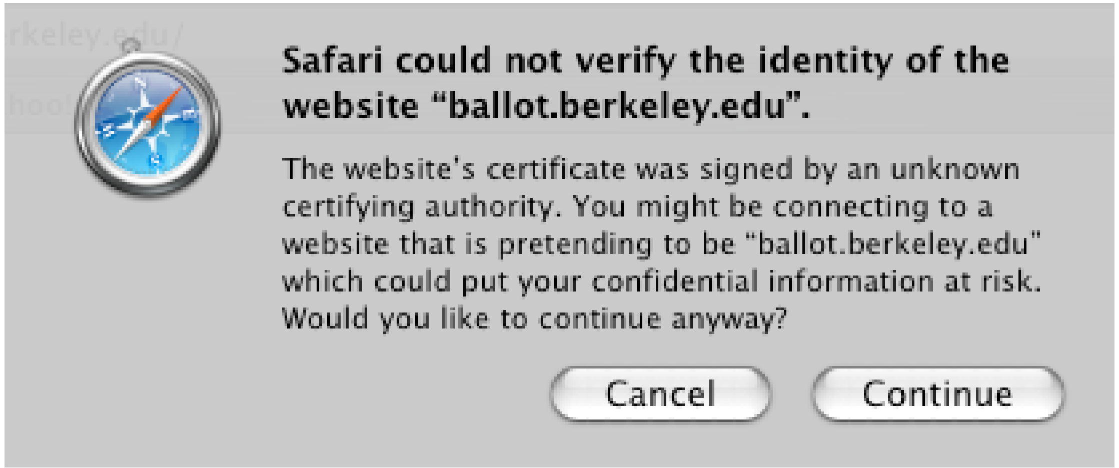
- DNS behaves normally for all hostnames, except that of the Ballot Server
- DNS returns the internal IP of fakeballot whenever a request is made for the Ballot Server's hostname

Configuring Apache

- Apache listens on fakeballot's internal IP
- We wrote a small perl script to proxy traffic to and from Ballot Server
  - We simply make standard https requests from Ballot Server, and pass the returned data directly to the client
  - We have the user's authentication token
    - It is sent via http post in most Ballot Server requests
  - When the voting forms are submitted, we dynamically change the user's votes.


192.168.1.2
192.168.1.1
1. Requests voting page from Ballot
7. Fake receipt sent back to Polling Station User
5. User casts vote
Fakeballot (Man in the Middle)
Single Polling Station IP Addresses and DNS provided by Fakeballot
4. CalNet sends user-specific token back to user through Fakeballot
3. Polling Station User Authenticates to CalNet
6. Altered Polling Station User vote sent to Ballot with token from CalNet
2. Fakeballot redirects Polling Station User to CalNet
CalNet Authentication Server
Ballot

What about SSL?



Safari could not verify the identity of the website "ballot.berkeley.edu".

The website's certificate was signed by an unknown certifying authority. You might be connecting to a website that is pretending to be "ballot.berkeley.edu" which could put your confidential information at risk. Would you like to continue anyway?

- fakeballot's SSL certificate is signed by a bogus certificate authority
- This leads to ugly warning messages

Why SSL Doesn’t Matter

- Count on user behavior
  - Browser warnings not that scary, typical users just ‘Click Ok’
  - Only one user needs to accept the certificate
- Attacker can add certificate
  - ASUC poll workers easy to social engineer
- Browser bugs
  - At the time, Safari would accept any cert signed by a valid authority, regardless of the name specified [9]
  - Similar bugs appeared in Netscape and IE

Part Four:

Lessons Learned

Critical Vulnerabilities in OES

- OES suffered from multiple critical security vulnerabilities
  - Easy to find and exploit
  - Common ‘beginner’ blunders
  - More subtle holes yet to be found?

OES vs. Commercial Systems?

- OES differs from the commercial systems in a number of important ways
  - Commercial electronic voting systems don't connect to the internet
    - At least, we sincerely hope not
  - OES source is available for review
  - Expected lifetime for OES is much shorter
    - Commercial systems could be in use for decades

Cause for Concern?

- In light of OES' flaws, existence of similar bugs in commercial systems is plausible
- Commercial systems are closed
  - Amplifies damage resulting from a security breach
  - Increases time before holes are discovered
- Vendors appear new to computer security
  - Mistakes likely
- Higher Stakes
  - Commercial systems will be used to elect the President

What you can do

- Endorse VerifiedVoting.org's Resolution on Electronic Voting [10]
- Write to Congress
  - Emphasize need for voter verified paper ballot
  - Encourage the use of open source voting systems
- Talk to local officials
  - Purchasing decisions for voting hardware are often made at the county level

References

1. http://www.essvote.com/pdf/iv101502.pdf
2. http://www.diebold.com/solutions/election/accuvote_ts.htm
3. http://www.sequoiavote.com/productGuide.php
4. See Bruce Schneier’s excellent crypto snake oil rant
   http://www.counterpane.com/crypto-gram-9902.html#snakeoil
5. http://www.verifiedvoting.org/
6. Daily Californian, 2/11/2003
   http://www.dailycal.org/article.asp?id=10858
7. http://calnet.berkeley.edu
8. The real Verisign is Verisign, Inc.
9. Safari Common Name verification bug
   http://www.secunia.com/advisories/8756/
10. http://www.verifiedvoting.org/resolution.asp