Internet Voting for UOCAVA Voters

David Jefferson
Lawrence Livermore National Laboratory

UOCAVA Workshop
August 6, 2010
Washington, D.C.

Outline

1. **Voting security is a matter of national security issue**
2. **Internet voting ...**
   - is fraught with *many* and *profound* vulnerabilities
   - *everywhere you look*
   - that are *not correctable in the foreseeable future* and
   - *put national security at risk*
3. **Fallacies regarding security metrics**
   - great skill to attack
   - security can be measured through testing and pilots
   - one attack at a time fallacy
   - probabilistic thinking fallacy

I) Voting Security is a matter of U.S. National Security

Election Security is a Key Aspect of U.S. National Security

We must treat voting integrity as a national security issue. The legitimacy of the U.S. government (and more) is at stake.

- *A few hundred votes* may suffice to swing a House or Senate race, or the electoral votes of a state.
- Each Senator matters on a national scale.
- Even local races may have billions of dollars at stake in bond and tax measures.
- *We are not talking about e-commerce security here!*

Those who know don't talk!

- The organizers of this Workshop invited relevant agencies to speak about the Internet threat environment.
- The DIA and
- ... the CIA and
- ... the NSA all declined!
- Why?
  - My take: The U.S. national security experts consider cyber threats to be so dangerous, and our exposure to them so great, that they will not say anything detailed about them in public at all.

General Michael Hayden on Chinese cyber espionage program

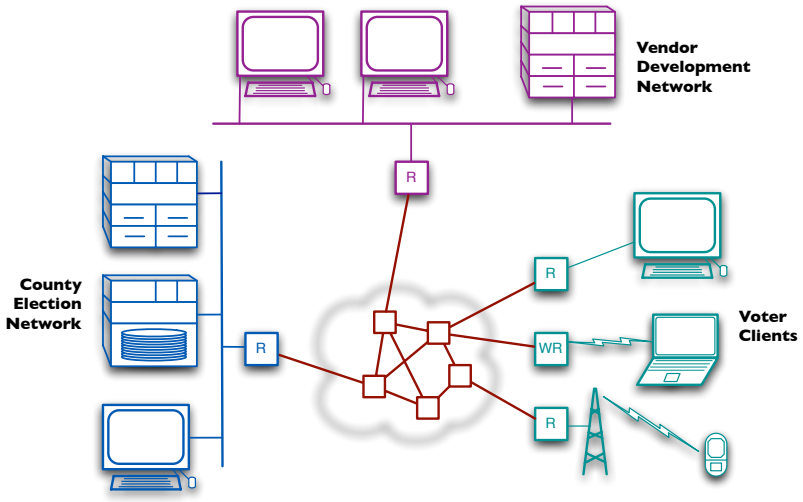
- Former director of CIA *and* of NSA
- Speaking in Keynote address at Black Hat USA 2010 last month (!)

"As an intelligence professional, I stand back in absolute awe and wonder"

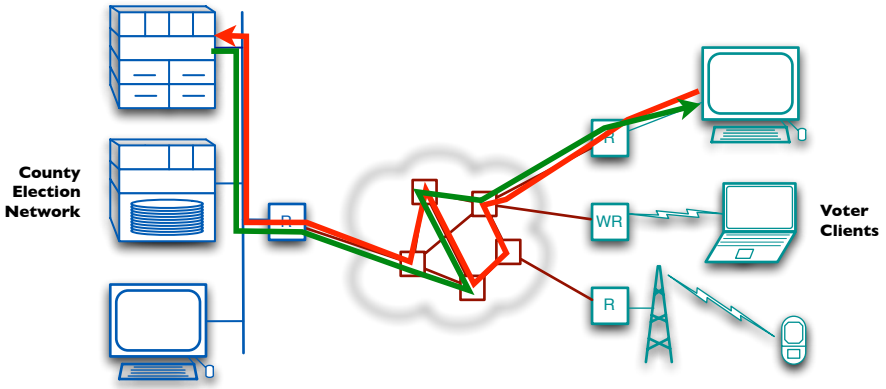
"It is magnificent in its depth, its breadth and its persistence"

II) Internet voting is fraught with intractable vulnerabilities

Generic Internet Voting System



Voting Transaction:
Blank Ballot Request Ballot

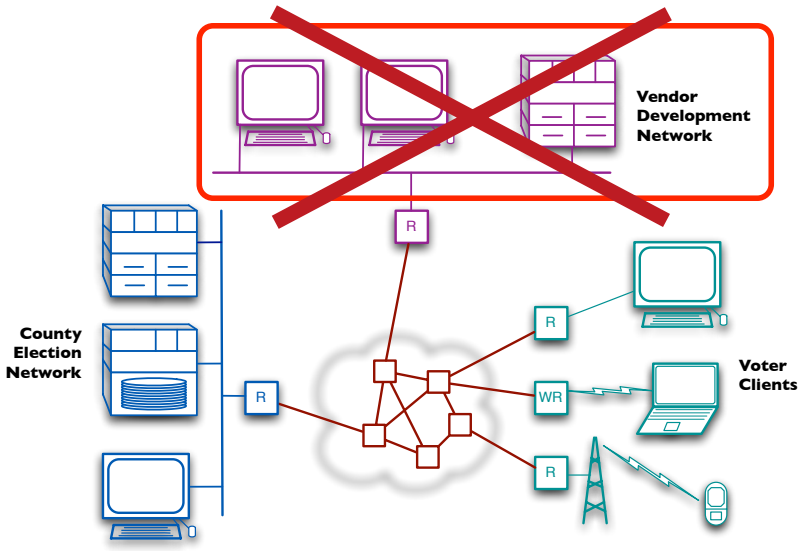


Major Internet voting attack types

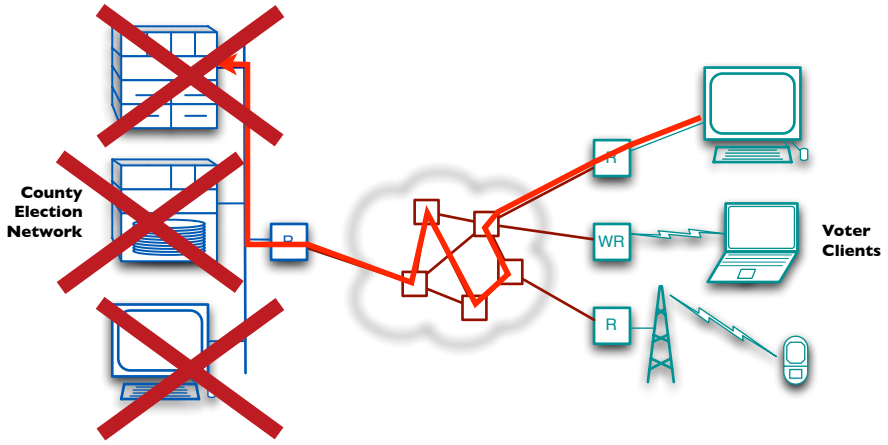
- Vendor development network penetration attacks (many kinds)
- Vendor insider attacks
- Presentation attacks
- Client-side malware attacks of many kinds
- Network attacks (man-in-middle, DNS, router, spoofing, denial of service)
- Server penetration attacks (many kinds)
- Election official insider attacks
- Vote buying or coercion attacks
- *All of these attacks can be engineered by a single person, working alone, from anywhere in the world*

Server and vendor penetration attacks

Vender-side attacks



Server-side penetration attacks



Vendor and county penetration attacks

- Early 2010: Google announced penetration attacks on its networks and those of about 25 other high-tech companies
- Attributed to Chinese gov't operatives
- *Source code* was a prime target
- Google and these other companies have enormous security expertise and resources. Yet they were penetrated with a devastating attack -- undetected for a long time.

Disclosures and Disclaimers

- **I work at Lawrence Livermore National Laboratory (LLNL), historically a nuclear weapons laboratory, and now a broad national security research laboratory.**
- **It is one of the highest security installations in the U.S.**
- **Disclaimers**:
  - ***I do not speak in any way for LLNL***
  - ***Nothing I say refers in any way to LLNL's or any other classified networks***

LLNL Experience

- **Our (unclassified) networks are under continuous attack 24 x 7. We are a huge international espionage target.**
- **We see every kind of threat there is:**
  - Email, web, social engineering, direct penetration, and malware attacks
  - Domestic and foreign attacks
  - Script kiddie mischief and state-sponsored espionage attacks
  - Untargeted and targeted attacks
  - Fast- and slow-spreading attacks
  - Single shot and "advanced persistent threat" (APT) attacks
  - Moderate- and world-class expert attacks
- ***We have one of the strongest cyber security programs anywhere, and still, as in any other large enterprise, some dangerous stuff gets through!***

Any county with even partial jurisdiction over an important election is a potential international security cyber target.

So is its vendor.

This means:

Los Angeles County
Cook County
King County
Miami-Dade County
Allegheny County
Cuyahoga County
Fulton County
3000 others .....

And vendors:

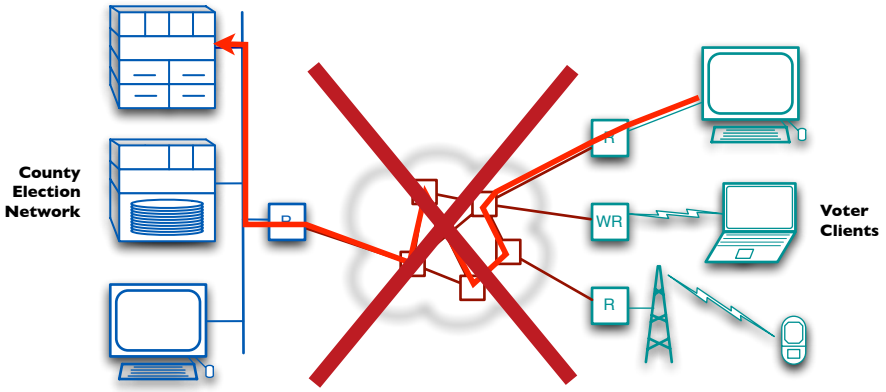
Scytl
Everyone Counts
anyone else?

If attacked by serious adversaries these organizations have essentially no chance of successfully defending.

No general solution to the problem of penetration attacks is even on the horizon.

Network attacks

Voting Transaction: Network Threats



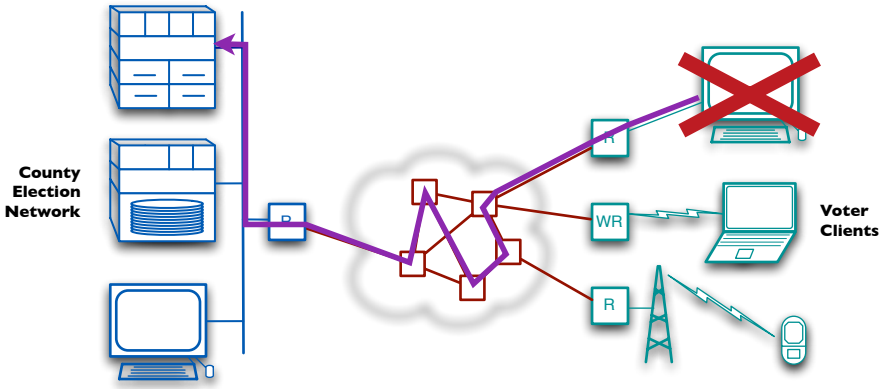
Network attacks

- **Many kinds of network attacks**
  - router attacks
  - DNS attacks
  - spoofing attacks
  - DDOS attacks (indiscriminate or selective)
- **Whole country of Estonia was brought down in May 2007 by massive DDOS attack**
  - Estonia -- promoter of Internet voting
  - Attack came from Russian nationalists, probably not Russian gov't
- **Canadian provincial party election was attacked *on election day* by DDOS in 2004 by parties unknown.**

No general solutions to DDOS or most other network attack problems are even on the horizon.

Client side attacks

Voting Transaction: Client-side Threats



PC Malware

- Almost all PCs connected to the Internet have some kind of malware in them today
- Usually cannot bring up a PC running XP without it getting infected *during the process of downloading the patches!*
- Huge *botnets* have been created out of infected PCs
  - spam
  - identity theft
  - now ... consumer banking

No general solutions to client malware attacks are even on the horizon.

Perfect is the enemy of the good?

- We are *not* faced with a choice between two reasonable but imperfect systems.
- We are faced with a choice between a class of reasonable but imperfect systems (VBM) and a class of *catastrophically dangerous systems (Internet voting)*.

III) Fallacies Regarding Security Metrics

Fallacy 1: Security can be measured via testing and pilots

- **Computer Security Maxim**: Testing can sometimes tell you if there *is* a security vulnerability, but it can never tell you there is *not* one.
  - How would you test a person to prove he is not a thief?
- Black hat attackers will *never* attack your pilot project
- White hat attackers *cannot attack with all they have*, because many attacks are illegal!
- Don't rely on security -- rely on auditing!

Fallacy 2: One attack at a time

- Attacks are cheap
- Attackers must be expected to attack multiple jurisdictions at once (e.g. multiple Florida counties) simultaneously
- They can be expected to use multiple different attacks simultaneously
- Multiple attackers can independently attack the same election
- Any security metrics we discuss *must* take cognizance of these facts.

Fallacy 3: Probabilistic thinking regarding security

- If you think in terms of the probability that the adversary will attack, or use a particular kind of attack, you are probably thinking wrong!
- Adversary will choose the worst case attack against the weakest target *all the time*, not just some fraction of the time.
- The proper mathematics for security estimation is game theory (minimax analysis), not probability
- Probability theory is appropriate for reliability analysis, not security.

Hypothetical Security Metric: MVAPY

Mean Votes Affected per Year (by all attacks combined)

(Same as David Wagner discussed earlier today.)

$$\sum_{\text{all attack modes } a} p(a) * v(a)$$

where

p(a) is probability per year that successful attack *a* will occur

v(a) is the number of votes affected by attack *a*

What is wrong with MVAPY?

$$\text{MVAPY} = \sum_{\text{all attack modes } a} p(a) * v(a)$$

- No exhaustive list of nonoverlapping attack modes
- MVAPY metric assumes only one attack at a time!
- No way of assigning meaningful probabilities to the use of any particular attack
  - Do not confuse the distribution of your uncertainty with distribution of your adversary's probability distribution
- Useful metrics must be *operational* and *validatable*, but this is not
- Humans are notoriously terrible at estimating probabilities of devastating events that have never occurred.

Metric Factors for Voting System Security

- Number of cooperating people required to conduct attack (Dill, Lazarus, Schneider)
- Cost ($) of an attack
- Time required to set up an attack
- Number of people / organizations in the world with the means to conduct an attack against a particular voting system
- Worst case number of votes that can be affected by a particular attack
- Number of jurisdictions using a voting system to which an attack applies
- Detectability of the attack
- Measurability of the number of votes affected by the attack
- Correctability of the attack
- Persistence of the attack
- Effects of attack
  - Votes changes
  - Votes (selectively) lost
  - Phony votes inserted
  - Vote privacy exposed
  - Disenfranchisement
  - Votes bought or cast under duress
  - FUD
- Number of insiders with write access to code under development
- Number of insiders with critical access to electronic votes and logs
- Max number of ballots transmitted through any single router, proxy, mail forwarding agent, etc.

Paper and Software

- **Software independence**
  - "software" was not the key issue
  - It was really "complex system" independence. (Read the paper.)
  - paper is a simple system
- **Paper**
  - write-once memory that can be read and written by (most) humans without additional hardware or software!

Congressional mandate?

- IANAL, so I cannot comment on the legal issues. But lawyers I know do not believe this really is a mandate.
- In any case ...
  - If Congress asked NIST to "square the circle", how would NIST produce the standard?
  - If Congress asked for standards for perpetual motion machines, how would NIST write those standards?
  - If Congress asked for a fair market for plums and lemons, how would anyone create it?

Washington Declaration?

- **My advice:**
  - Use Internet for *registration* and *blank ballot transmission* and (maybe) *proxy registration*
  - Do not transmit voted ballots over the Internet at all
  - If you must do so anyway for some limited purpose, require end-to-end paper trail and real risk limiting audits
  - FVAP, EAC, NIST: Ask Congress to lift this mandate or expectation
  - Tell Senators and Congressmen that they are putting the national security and their own re-election at risk!

End