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

• A few hundred votes may suffice to swing a House or Senate race, or the electoral votes of a state.

• The legitimacy of U.S. government is at stake.

• Even local races may have billions of dollars at stake in bond and tax measures.

• Wherever there is a concentration of votes sufficient to swing a major election there is a national security concern.

• General Michael Hayden (Former director of CIA and of NSA, speaking in Keynote address at Black Hat USA July, 2010) on Chinese cyber espionage program:

  “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
Email voting – the worst idea ever!

- Transmitted in the clear (not encrypted)
- Copying, dropping, or modifying votes in transit is easy *and can be automated* by any IT person controlling a router or email forwarding agent somewhere in the path from voter to county.
  - Vacuumed up by national intelligence agencies
- Voter’s name must be attached -- all privacy is lost
- Obvious that message contains a ballot, making attacks easy
- Voter’s address in the From: header is completely forgeable
- Subject to arbitrary delays and (occasionally) dropping or duplication.
- Email addresses change frequently and are often shared
- PDF and other image formats may be used to inject malware into server side
- *Email voting has no security whatsoever*
- *It is worse than voting on the backs of postcards because of automated attacks*
- *FAX voting is just as bad*
- *Most dangerous form of yet contemplated.*
Generic Internet Voting System

designed as Web application
Vender penetration 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.
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.
Client-side malware attacks
Client 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!*

• The age of smartphone malware is just beginning

• Huge *botnets* have been created out of infected PCs
  • spam
  • identity theft
  • now ... consumer banking
Network attacks
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 probably came from Russian nationalists, not Russian gov’t

• Canadian provincial party election was attacked on election day by DDOS in 2004 by parties unknown.
Voting system “certification” idea fails

- Internet voting systems are not closed and fixed over time. They are open, and change constantly.

- Technology is constantly changing underneath IV systems
  - Hardware, OSs, browsers, plug-ins, document software, crypto standards and software, authentication mechanisms

- Threat environment is constantly changing
  - Circulating malware, botnets, penetration techniques, DDOS kits, rootkits, attack technology at all levels of software and protocol

- No IV system has ever been used twice without modification in the U.S., and cannot be for the foreseeable future

- The very idea of “certification” makes no sense in such a circumstance. You can’t “certify” something that is always changing!
Q: If I can conduct big financial transactions online safely, why can’t I vote online?

A1: Online financial transactions are not safe!

Banks lose hundreds of millions of dollars every year in online banking and credit card fraud. They absorb it as business expense and do not disclose it.

Now some botnets (Zeus) specialize in online bank fraud. Expect big changes in online transaction authentication.

A2: Security requirements for voting are structurally dissimilar to those for financial transactions

secrecy, privacy
transparency
transferability
irreversibility
DC Internet Voting Test Election

- Web-app Internet voting system architecture
- Completely virgin system never before used, never certified against any standard
- Intended for use in live general election after one field test!
- “Experiment” was completely uncontrolled
- Prof. Halderman’s server side penetration attack completely successful in 36 hours
- Halderman confident his team could have penetrated in other ways as well.
- No opportunity to try other kinds of attacks because they were still illegal
- Chinese and Iranian hackers were poking around!
- Besides the penetration attack, the system had a horrendous PDF-related bug as well that would have resulted in mostly blank ballots cast!
No generally effective defenses to any of these attack modes are even on the horizon.

PCs are not secure, and won't be in the foreseeable future.

The Internet is not secure, and won't be for the foreseeable future.

The situation is getting worse, not better, year by year.

If a competent team decides to attack an Internet voting system, that system will almost certainly be compromised. The defenders have essentially no chance!
III) What should be done to aid overseas and military voters?
How should overseas voters be better served?

• Adjust ballot prep and mailing schedules to give more lead time for mailing out paper ballots

• Adjust canvass schedule if necessary to permit mail-in ballots to arrive after election day, as long as they have a legible postmark proving they were mailed before the end of election day

• Distribute *blank ballots* online. Have voters print them, fill them out, and mail them back.
Online Distribution of Blank Ballots

- Still many security and technical problems, although probably manageable:
  - Ballot authentication
  - Image file format (not PDF please!)
  - Paper & printing standards
  - Scannability

- Saves one mail delay trans-ocean mail delay

- Verified Voting, FVAP, and NIST working together on plans for workshop soon to nail down the technical and security issues involved

- We should master this before we consider only return of voted ballots! Crawl before you walk!
End