Election Integrity:
A Vulnerability Assessor's View

Roger G. Johnston, Ph.D., CPP

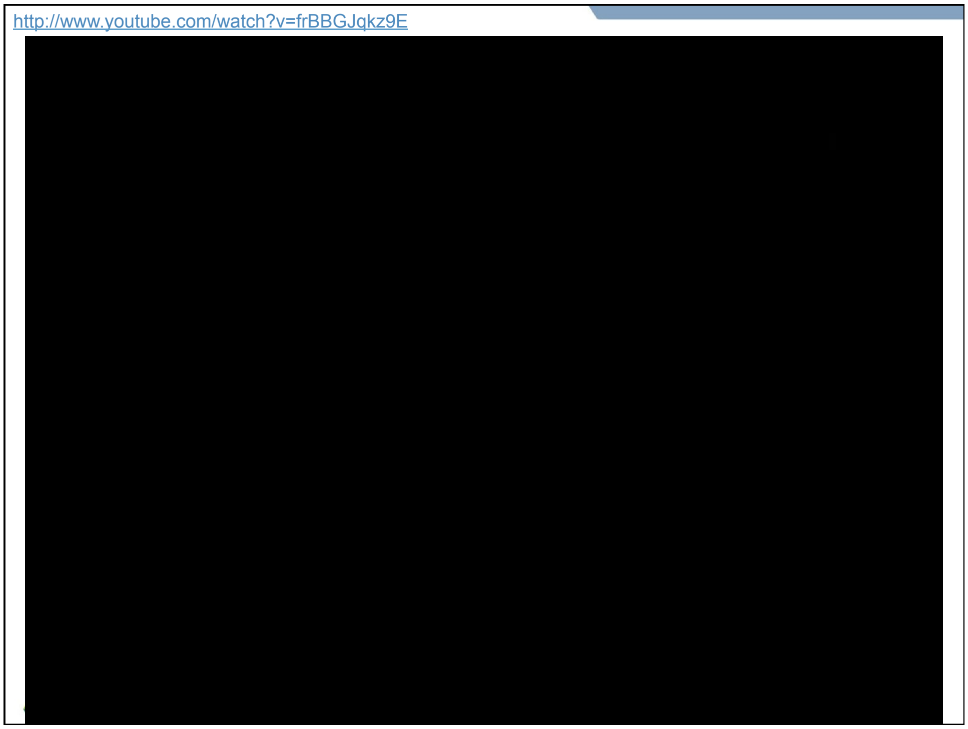
Vulnerability Assessment Team
Argonne National Laboratory

630-252-6168 rogerj@anl.gov
http://www.ne.anl.gov/capabilities/vat

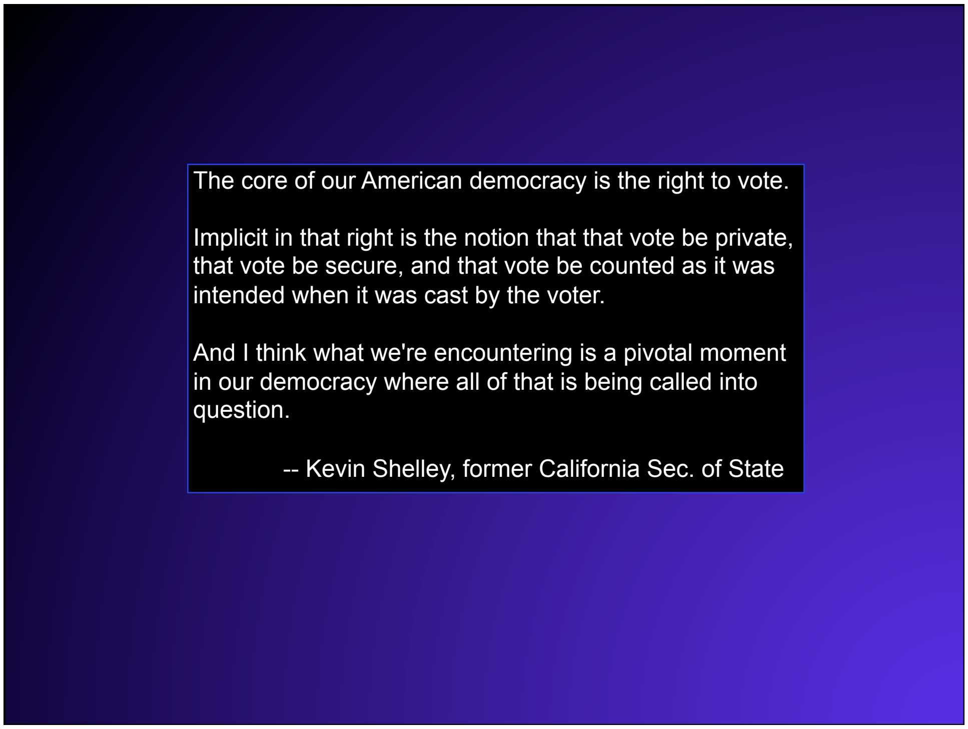
Argonne National Laboratory

~$750 million annual budget
1500 acres, 3500 employees, 5200 facility users, 1000 students & postdocs
R&D and technical assistance for government and industry

Argonne
NATIONAL LABORATORY
... for a brighter future
VAT
U.S. Department of Energy
UChicago Argonne LLC
A U.S. Department of Energy laboratory managed by UChicago Argonne, LLC



http://www.youtube.com/watch?v=frBBGJqkz9E

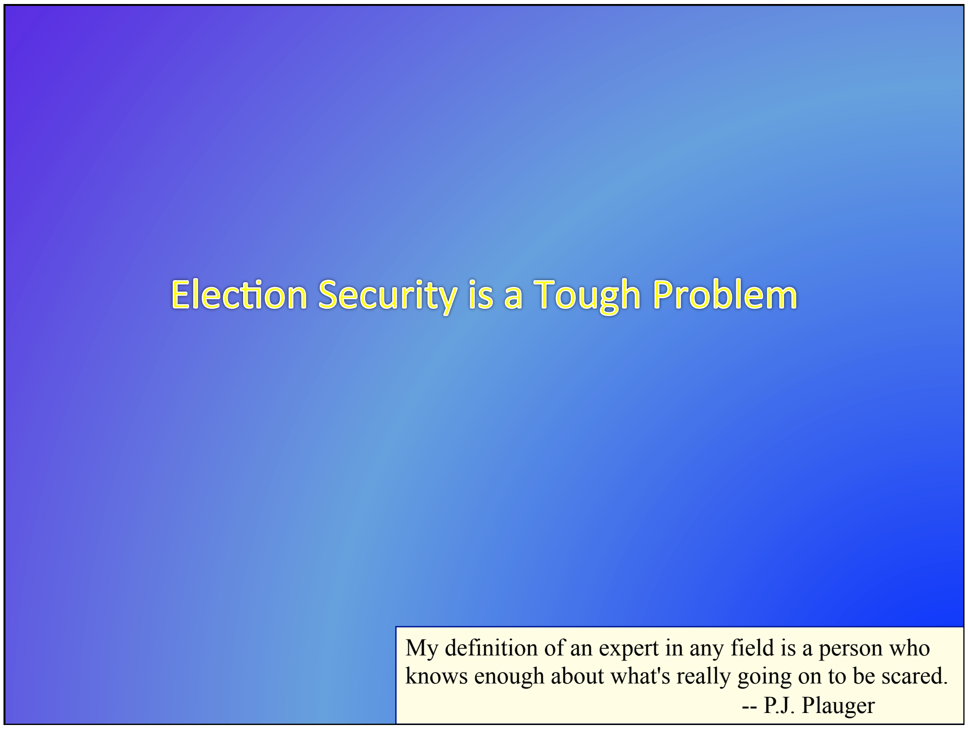


The core of our American democracy is the right to vote.

Implicit in that right is the notion that that vote be private, that vote be secure, and that vote be counted as it was intended when it was cast by the voter.

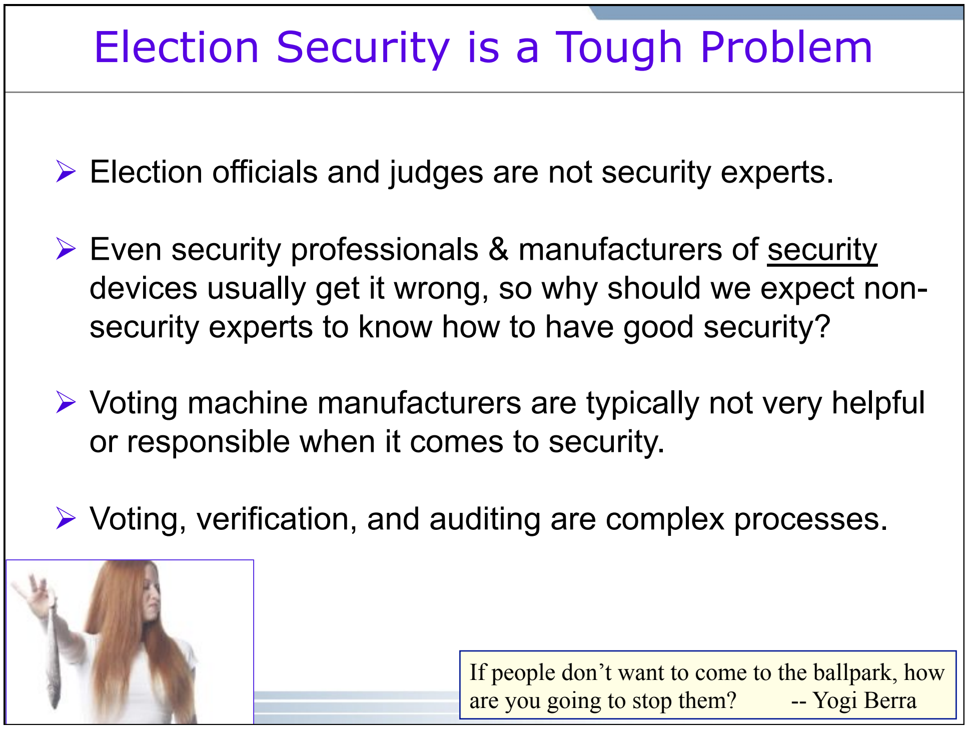
And I think what we're encountering is a pivotal moment in our democracy where all of that is being called into question.

-- Kevin Shelley, former California Sec. of State



Election Security is a Tough Problem

> My definition of an expert in any field is a person who knows enough about what's really going on to be scared.
> -- P.J. Plauger



Election Security is a Tough Problem

- Election officials and judges are not security experts.
- Even security professionals & manufacturers of security devices usually get it wrong, so why should we expect non-security experts to know how to have good security?
- Voting machine manufacturers are typically not very helpful or responsible when it comes to security.
- Voting, verification, and auditing are complex processes.

> If people don't want to come to the ballpark, how are you going to stop them? -- Yogi Berra

Election Security is a Tough Problem

- Many thousands of people have access to the devices & user friendliness is essential (often not the case for other security applications).
- The public doesn’t like security, but demands full election integrity.
- There are major time constraints.
- Budgets are brutally tight.
- You must often rely on amateur poll workers.

Radisson Welcomes
Emerging Infectious Diseases

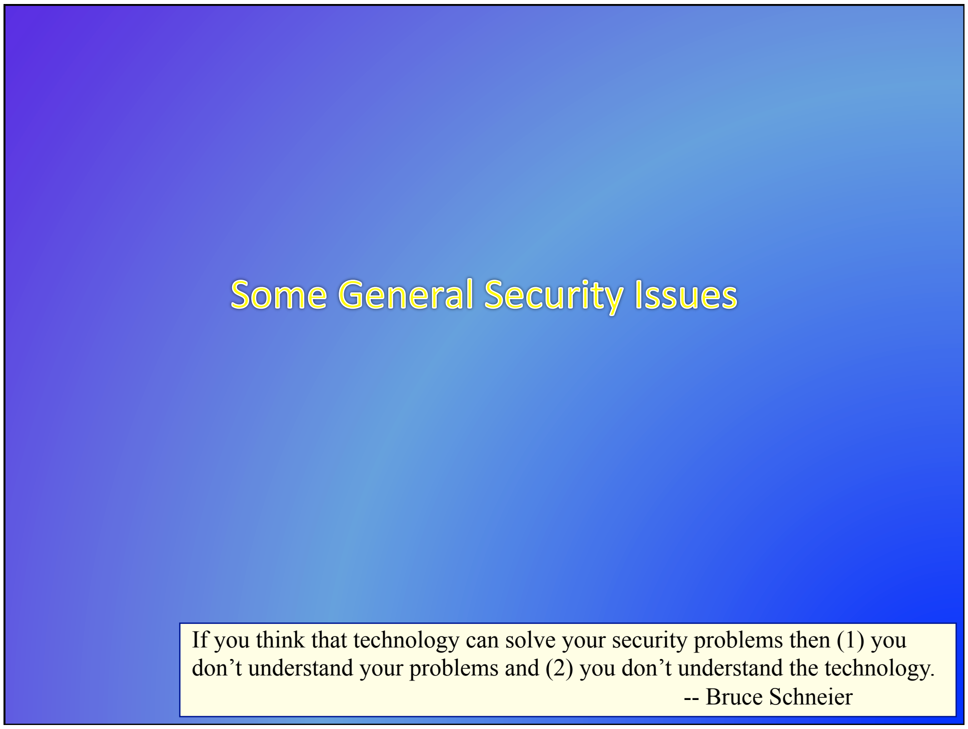
-- Sign outside a Radisson Hotel

Probably Wrong Assumptions

UK Game Show Host: Watling Street, which now forms part of the A5, was built by which ancient civilization?
Contestant: Apes?

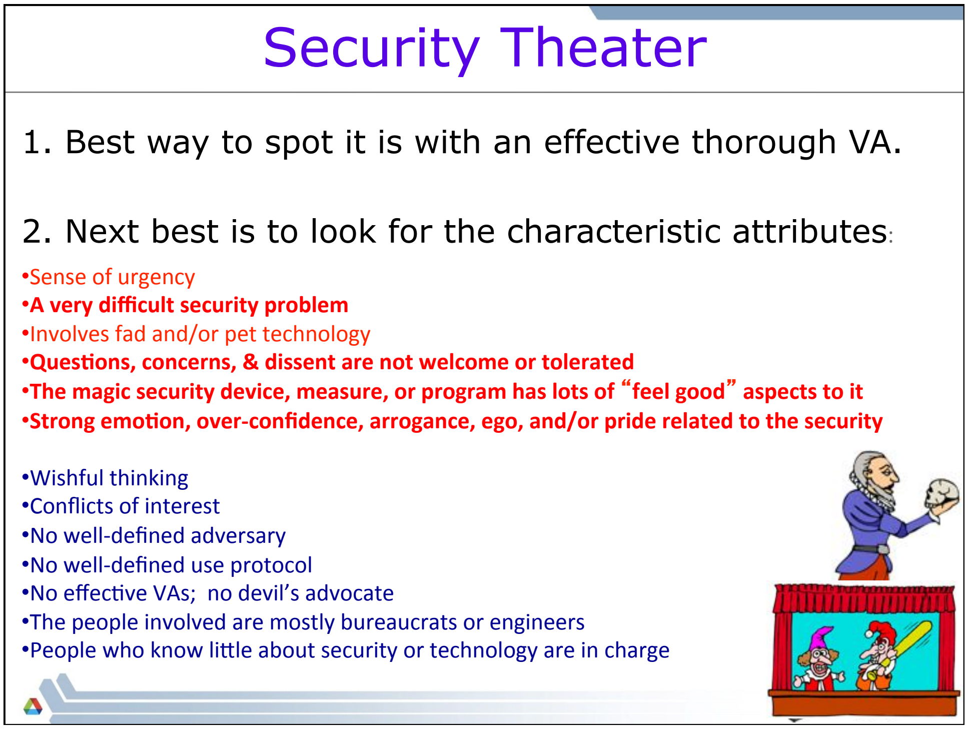
My Observations

You can observe a lot just by watching.
-- Yogi Berra



Some General Security Issues

> If you think that technology can solve your security problems then (1) you don’t understand your problems and (2) you don’t understand the technology.
> -- Bruce Schneier



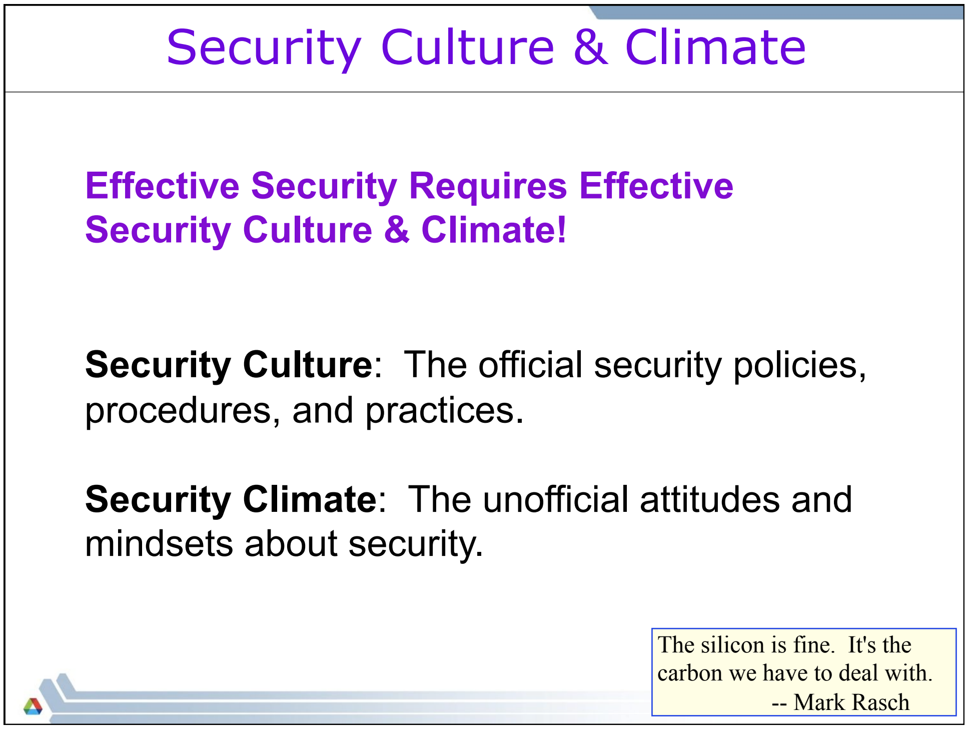
Security Theater

1. Best way to spot it is with an effective thorough VA.

2. Next best is to look for the characteristic attributes:

•Sense of urgency
•A very difficult security problem
•Involves fad and/or pet technology
•Questions, concerns, & dissent are not welcome or tolerated
•The magic security device, measure, or program has lots of “feel good” aspects to it
•Strong emotion, over-confidence, arrogance, ego, and/or pride related to the security

•Wishful thinking
•Conflicts of interest
•No well-defined adversary
•No well-defined use protocol
•No effective VAs; no devil’s advocate
•The people involved are mostly bureaucrats or engineers
•People who know little about security or technology are in charge



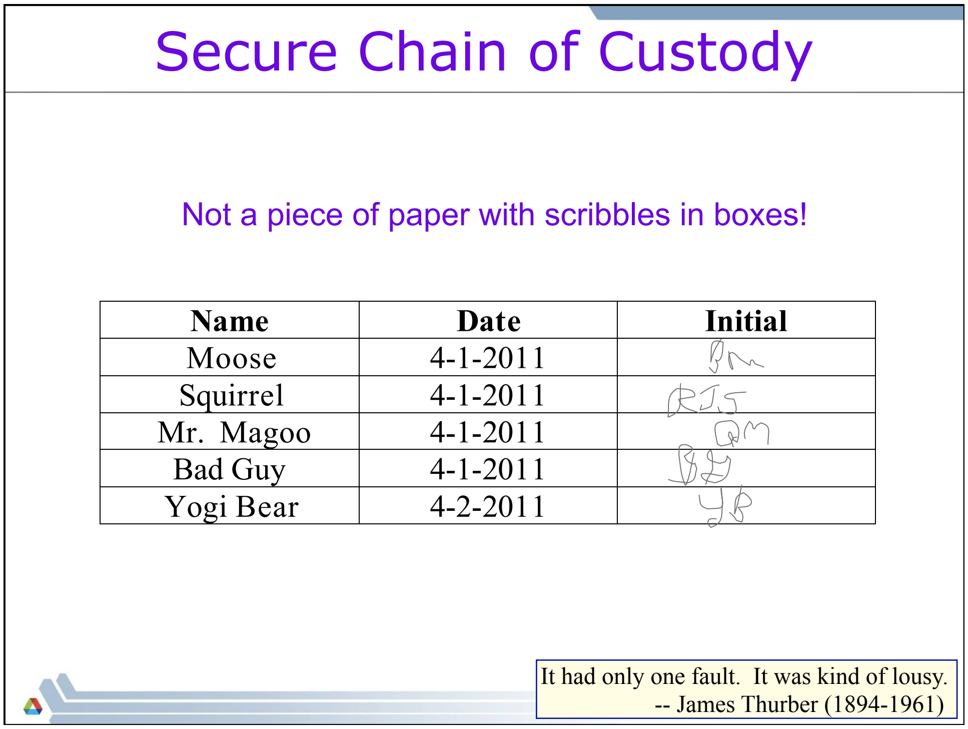
Security Culture & Climate

Effective Security Requires Effective Security Culture & Climate!

Security Culture: The official security policies, procedures, and practices.

Security Climate: The unofficial attitudes and mindsets about security.

> The silicon is fine. It's the carbon we have to deal with.
> -- Mark Rasch



Secure Chain of Custody

Not a piece of paper with scribbles in boxes!

Name	Date	Initial
Moose	4-1-2011	Bm
Squirrel	4-1-2011	RJS
Mr. Magoo	4-1-2011	QM
Bad Guy	4-1-2011	BG
Yogi Bear	4-2-2011	YB

> It had only one fault. It was kind of lousy.
> -- James Thurber (1894-1961)

Facts About Security Devices & Systems

For most security devices (including biometrics and access control devices), it's easy to:

- clone the signature of an authorized person
- do a man-in-the-middle (MM) attack
- access the password or key
- copy or tamper with the database
- "counterfeit" the device
- install a backdoor
- replace the microprocessor
- tamper with the software

Backdoor, MM, or Counterfeit Attacks

The importance of a cradle-to-grave, secure chain of custody:

Most security devices can be compromised in 15 seconds (at the factory or vendor, on the loading dock, in transit, in the receiving department, in storage, or after being installed).

Most "security" devices have little built-in security or ability to detect intrusion/tampering.

> The Air Force is pleased with the performance of the C-5A cargo plane, although having the wings fall off at eight thousand hours is a problem.
> -- Major General Charles F. Kyunk, Jr.

Security of Security Products

Physical, Man-In-The-Middle Attacks on Electronic Voting Machines

If the only tool you have is a hammer,
you tend to see every problem as a nail.
-- Abraham Maslow (1908-1970)

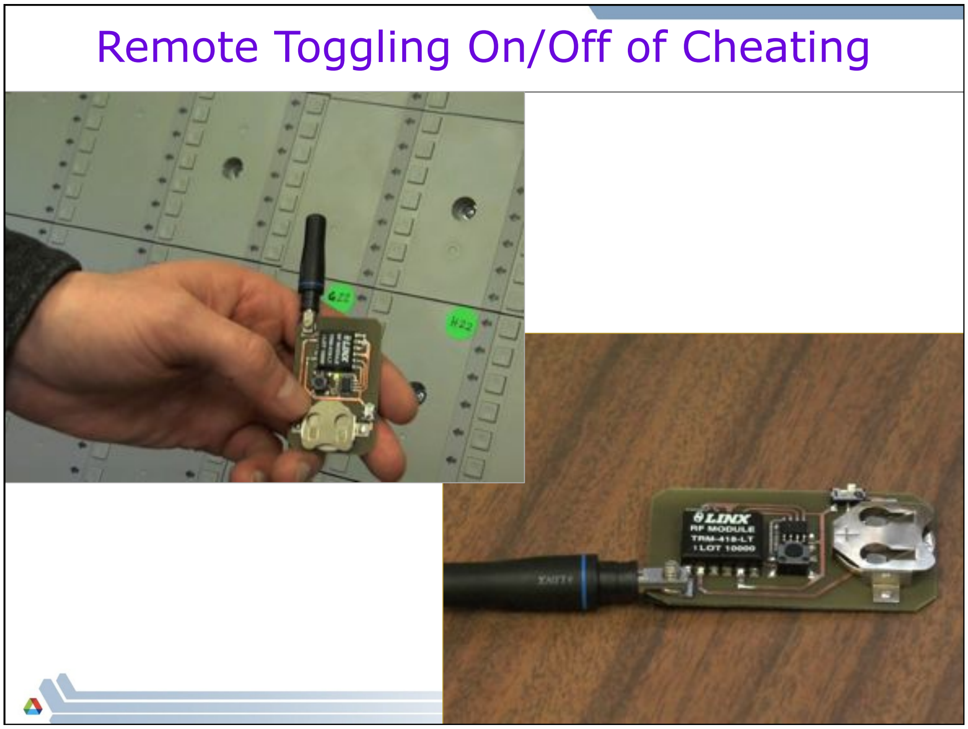
Diebold AccuVote-TS

Used in 3 states by 3.5 million voters.

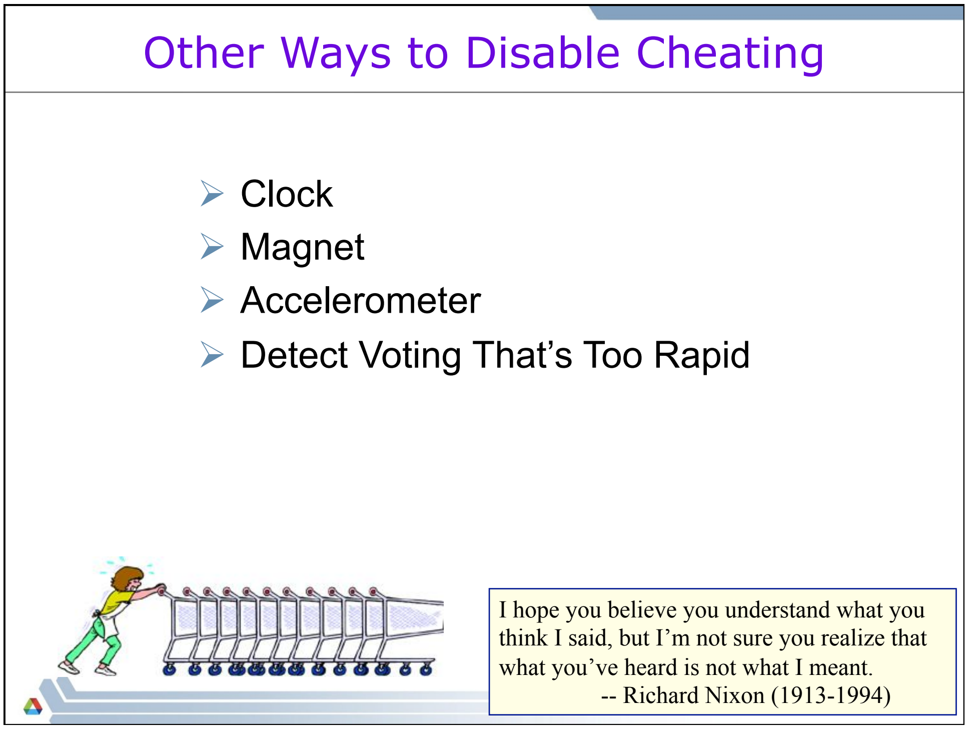
The closely related TSX is used in 20 states by 21 million voters (2.3 million of them in Illinois).

Sequoia Advantage AVC

Used in 6 states
by 9 million voters



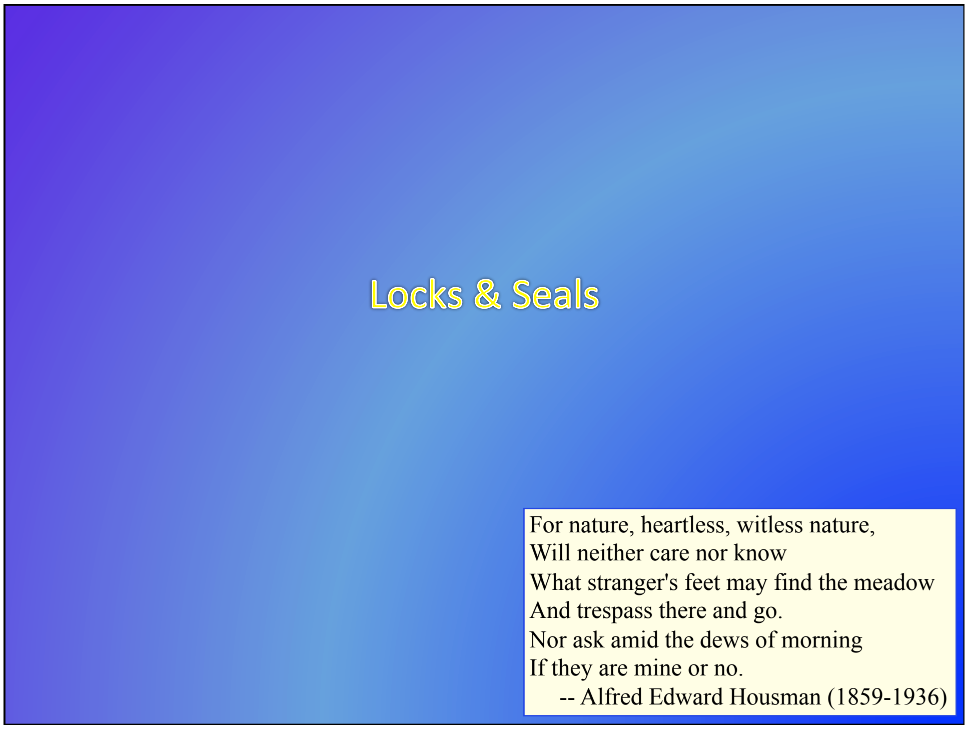
Remote Toggling On/Off of Cheating



Other Ways to Disable Cheating

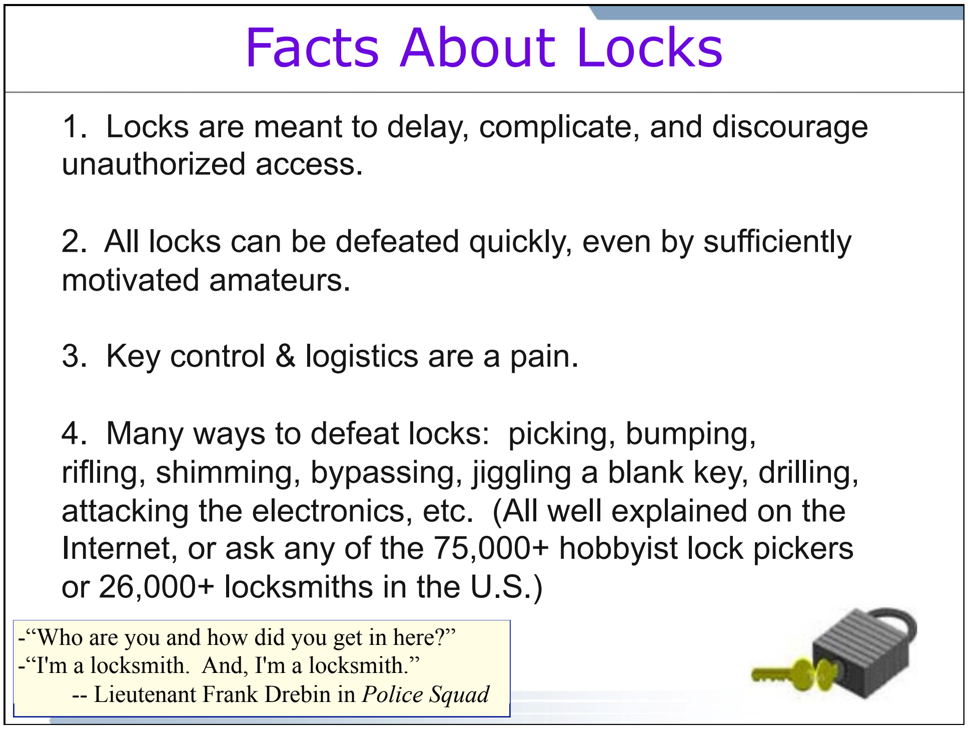
- Clock
- Magnet
- Accelerometer
- Detect Voting That’s Too Rapid

I hope you believe you understand what you think I said, but I’m not sure you realize that what you’ve heard is not what I meant.
-- Richard Nixon (1913-1994)



Locks & Seals

For nature, heartless, witless nature,
Will neither care nor know
What stranger's feet may find the meadow
And trespass there and go.
Nor ask amid the dews of morning
If they are mine or no.
-- Alfred Edward Housman (1859-1936)



Facts About Locks

1. Locks are meant to delay, complicate, and discourage unauthorized access.

2. All locks can be defeated quickly, even by sufficiently motivated amateurs.

3. Key control & logistics are a pain.

4. Many ways to defeat locks: picking, bumping, rifling, shimming, bypassing, jiggling a blank key, drilling, attacking the electronics, etc. (All well explained on the Internet, or ask any of the 75,000+ hobbyist lock pickers or 26,000+ locksmiths in the U.S.)

-“Who are you and how did you get in here?”
-“I'm a locksmith. And, I'm a locksmith.”
-- Lieutenant Frank Drebin in *Police Squad*

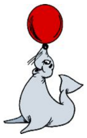
Terminology

(tamper-indicating) seal: a device or material that leaves behind evidence of unauthorized entry.

I'd say, "It's a Buttmaster, Your Holiness."
-- Suzanne Somers on how she would respond if the Pope asked her the name of the exercise machine she promotes

Terminology (con't)

defeating a seal: opening a seal, then resealing (using the original seal or a counterfeit) without being detected.



attacking a seal: undertaking a sequence of actions designed to defeat it.

"Do not eat if seal is missing!"
-- Actual printing on the tamper-evident seal of a food product.

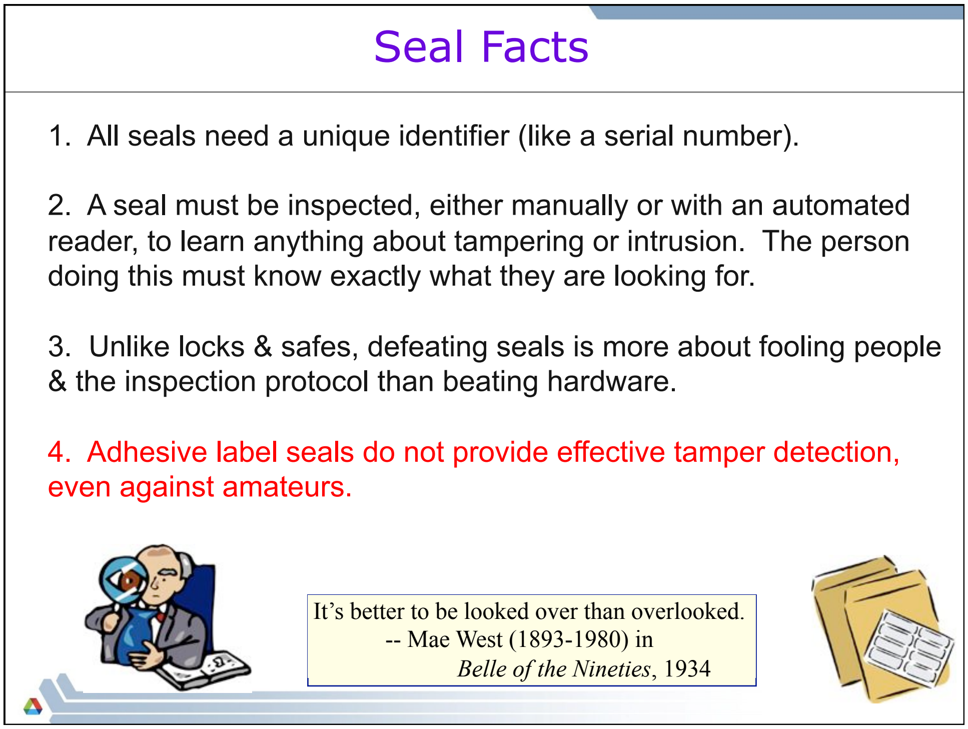
Seal Fact

A seal is not a lock.

Yanking a seal off a container is not defeating it!

Summary of Seals Results

parameter	mean	median
attack time	1.4 mins	43 secs
cost of tools & supplies	$78	$5
marginal cost of attack	62¢	9¢
time to devise successful attack	2.3 hrs	12 mins



Seal Facts

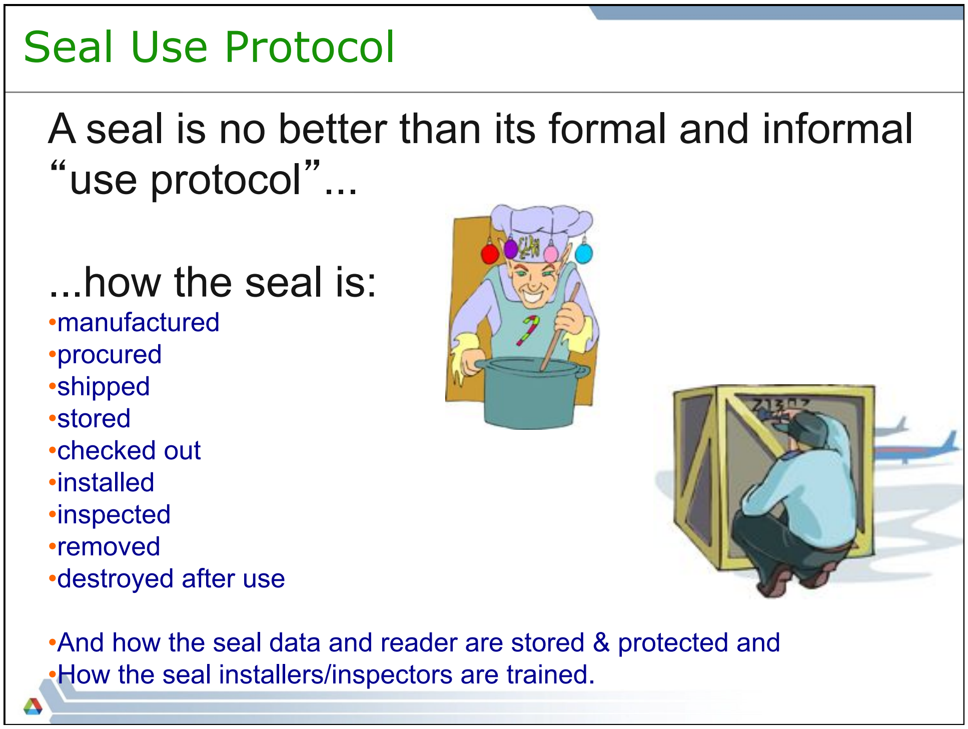
1. All seals need a unique identifier (like a serial number).

2. A seal must be inspected, either manually or with an automated reader, to learn anything about tampering or intrusion. The person doing this must know exactly what they are looking for.

3. Unlike locks & safes, defeating seals is more about fooling people & the inspection protocol than beating hardware.

4. Adhesive label seals do not provide effective tamper detection, even against amateurs.

It's better to be looked over than overlooked.
-- Mae West (1893-1980) in
Belle of the Nineties, 1934



Seal Use Protocol

A seal is no better than its formal and informal "use protocol"...

...how the seal is:

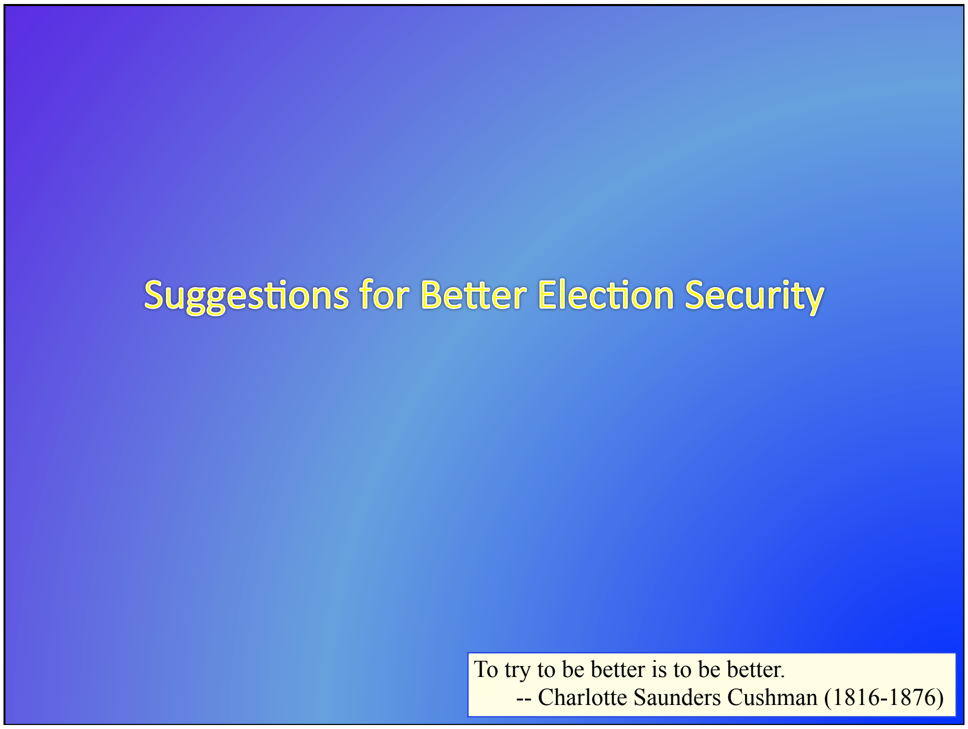
- manufactured
- procured
- shipped
- stored
- checked out
- installed
- inspected
- removed
- destroyed after use

- And how the seal data and reader are stored & protected and
- How the seal installers/inspectors are trained.

The Good News: Countermeasures

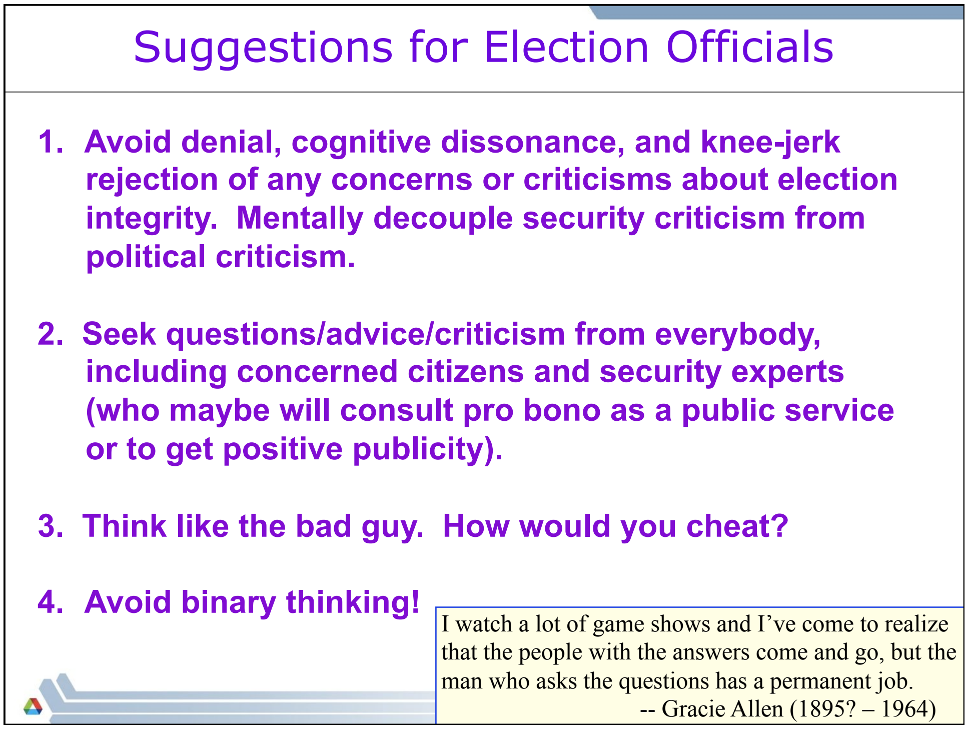
- You can spot seal attacks if you know what you are looking for, and have hands-on training/practice!
- Also: better seals are possible!

> The prophet who fails to present a bearable alternative and yet preaches doom is part of the trap he postulates.
> -- Margaret Mead (1901-1978)



Suggestions for Better Election Security

> To try to be better is to be better.
> -- Charlotte Saunders Cushman (1816-1876)



Suggestions for Election Officials

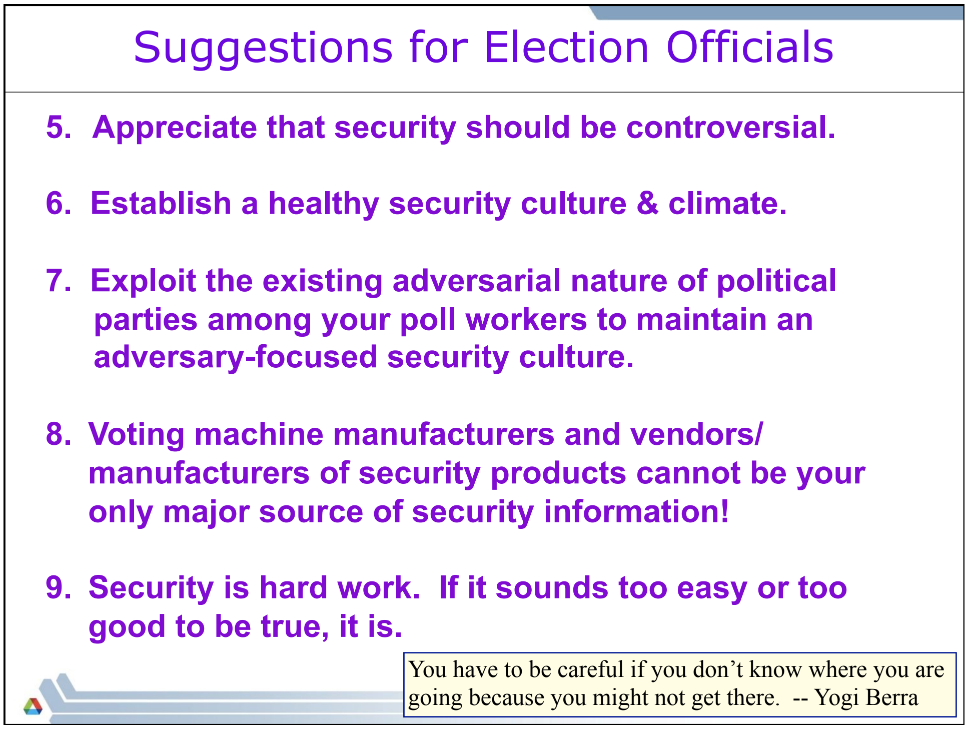
1. **Avoid denial, cognitive dissonance, and knee-jerk rejection of any concerns or criticisms about election integrity. Mentally decouple security criticism from political criticism.**

2. **Seek questions/advice/criticism from everybody, including concerned citizens and security experts (who maybe will consult pro bono as a public service or to get positive publicity).**

3. **Think like the bad guy. How would you cheat?**

4. **Avoid binary thinking!**

I watch a lot of game shows and I've come to realize that the people with the answers come and go, but the man who asks the questions has a permanent job.
-- Gracie Allen (1895? – 1964)



Suggestions for Election Officials

5. **Appreciate that security should be controversial.**

6. **Establish a healthy security culture & climate.**

7. **Exploit the existing adversarial nature of political parties among your poll workers to maintain an adversary-focused security culture.**

8. **Voting machine manufacturers and vendors/ manufacturers of security products cannot be your only major source of security information!**

9. **Security is hard work. If it sounds too easy or too good to be true, it is.**

You have to be careful if you don't know where you are going because you might not get there. -- Yogi Berra

Suggestions for Election Officials

10. Arrange for background checks on the people who move and maintain the voting machines. Use bonded personnel if possible.

11. Escort the machines to and from the polling place if possible.

12. You must know for sure that there was no delay in delivery or return of the voting machines.

13. Make somebody accountable for receiving and at least semi-watching the voting machines at the polling place. Secure them!

Actual Courtroom Testimony:
Witness (a Physician): He was probably going to lose the leg, but at least maybe we could get lucky and save the toes.

Suggestions for Election Officials

14. Watch out for swapping with "counterfeit" voting machines, and counterfeit used or unused ballots (including at the polls).

15. Don't rely on initialed-only seals or seals lacking serial numbers. Check the serial numbers. Protect the database of serial numbers from tampering!

16. Minimize the number of seals!

17. Do serious seals training. Have good manuals, posters, & hands-on exercises.

"Product not actual size."
-- Disclaimer on a TV ad for Burger King
that showed a giant Whopper crushing a car

Suggestions for Election Officials

18. Have a unique secret password of the day for each polling station for officials. (Different each election.)

19. Enlist staff, custodians, admins, teachers, and students to watch the voting machines when the polling place is a school, church, etc. (A good civics learning experience!)

20. Recognize that a secure chain of custody is a PROCESS, not a piece of paper with initials or scribbled signatures (rarely if ever checked)!

21. Do not allow technicians to work on a specific voting machine in the warehouse without authorization and oversight.

Always strive to be the person your dog already thinks you are. -- Anonymous

Suggestions for Election Officials

22. Arrange for periodic background checks for technicians who work on the voting machines.

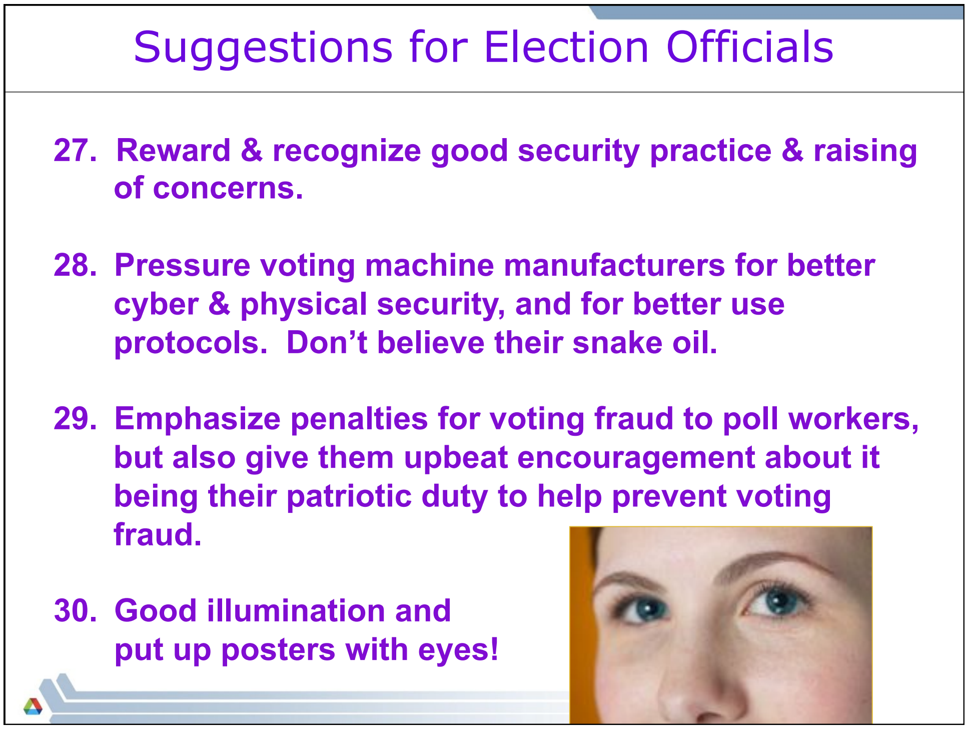
23. Deploy VVPR.

24. Consider optical scan voting systems (But watch for them being rolled away, tampered with, & for loss of privacy.)

25. Try bribes (but wait 1-2 days).

26. Security Management by walking around and talking to people.

Shouldn't the Air and Space Museum be empty? -- Dennis Miller



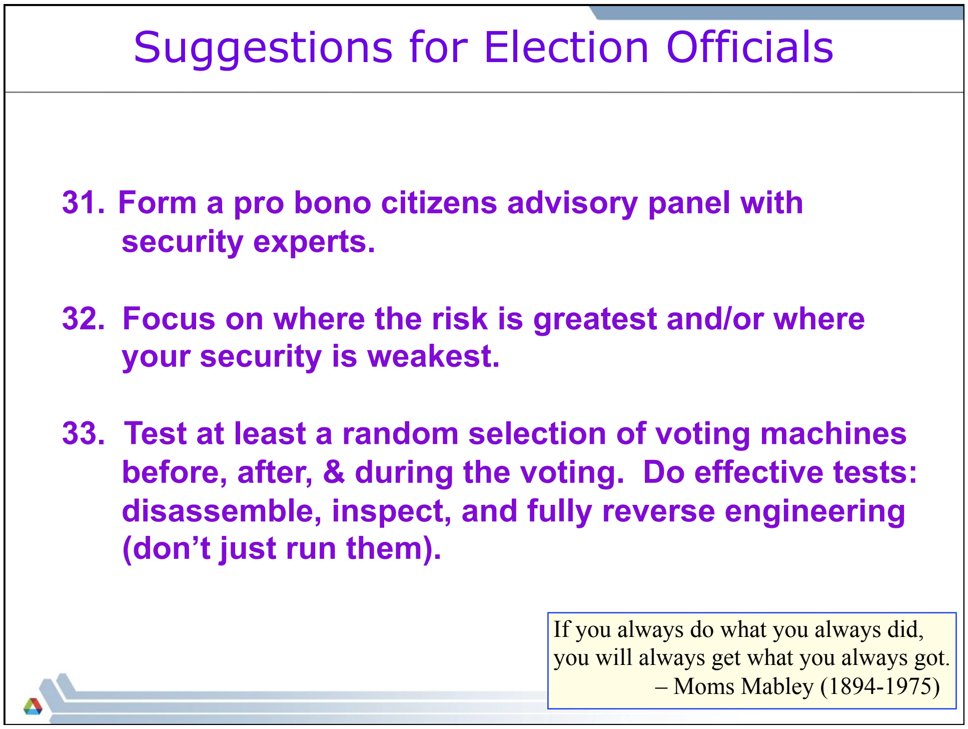
Suggestions for Election Officials

27. Reward & recognize good security practice & raising of concerns.

28. Pressure voting machine manufacturers for better cyber & physical security, and for better use protocols. Don't believe their snake oil.

29. Emphasize penalties for voting fraud to poll workers, but also give them upbeat encouragement about it being their patriotic duty to help prevent voting fraud.

30. Good illumination and put up posters with eyes!



Suggestions for Election Officials

31. Form a pro bono citizens advisory panel with security experts.

32. Focus on where the risk is greatest and/or where your security is weakest.

33. Test at least a random selection of voting machines before, after, & during the voting. Do effective tests: disassemble, inspect, and fully reverse engineering (don't just run them).

> If you always do what you always did,
> you will always get what you always got.
> – Moms Mabley (1894-1975)

Suggestions for Election Officials

34. Protect ballot secrecy by watching for improper voter use of cell phone cameras (especially for VVPR) and for planted mini wireless video cameras.

wireless, battery-powered, color video cameras, 100’-400’ range; $25-$200

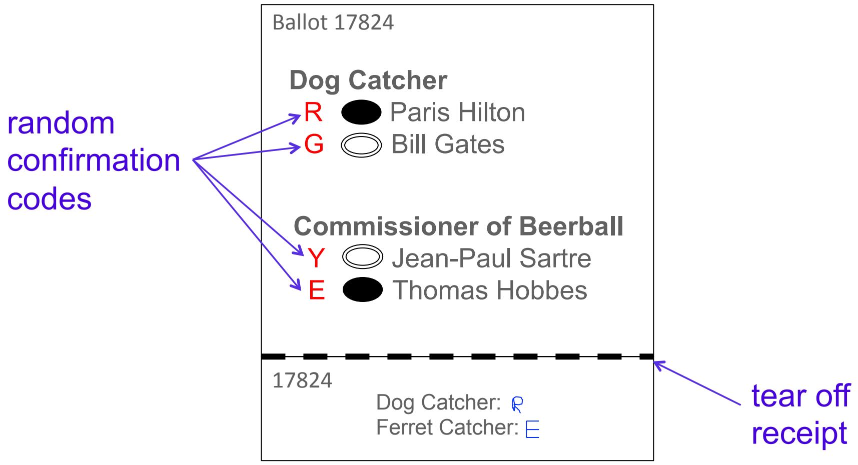
Question on a job application form: Do you support the overthrow of the government by force, subversion, or violence? Answer from one applicant: Violence.

Suggestions for Election Officials

35. Consider Random Alpha-Numeric Tokens.

Actual overheard conversation between two teenage girls:
--So he’s like, ‘nuh uh,’ and I’m like, ‘uh huh,’ and he’s like, ‘nuh uh,’ and I’m like, ‘um…uh huh,’ and he’s like, ‘nuh uh.’
--No way!
--Way.

Random Alpha-Numeric Tokens (Scantegrity I & II, etc.)



Ballot 17824

Dog Catcher

R ● Paris Hilton

G ○ Bill Gates

Commissioner of Beerball

Y ○ Jean-Paul Sartre

E ● Thomas Hobbes

17824

Dog Catcher: R

Ferret Catcher: E

random confirmation codes

tear off receipt

Important part of the concept: spoiled audit ballots!

Random Alpha-Numeric Tokens (Scantegrity I & II, etc.)

Advantages

- Better security
- Better transparency
- Inexpensive
- More centralization of the insider threat

Disadvantages

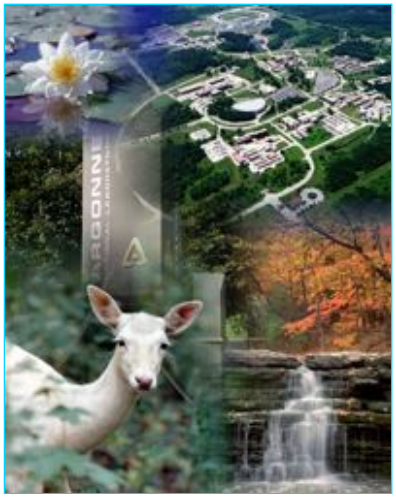
- More centralization of the insider threat
- Confusing for voters (Concentrate more on sophisticated voters & watchdogs?)
- Will slow down voting
- Problematic privacy preservation?
- Over-hyped
- Too much faith placed on encryption
- Invisible ink is probably not worth it

Suggestions for Citizens

1. Keep your eyes open, ask questions, and point out concerns.
2. Insist on transparency.
3. Demand good election security.
4. Join, support, or form public interest groups supporting election integrity.

> Sometimes security implementations look fool proof. And by that I mean proof that fools exist.
> -- Dan Philpott

For More Information...



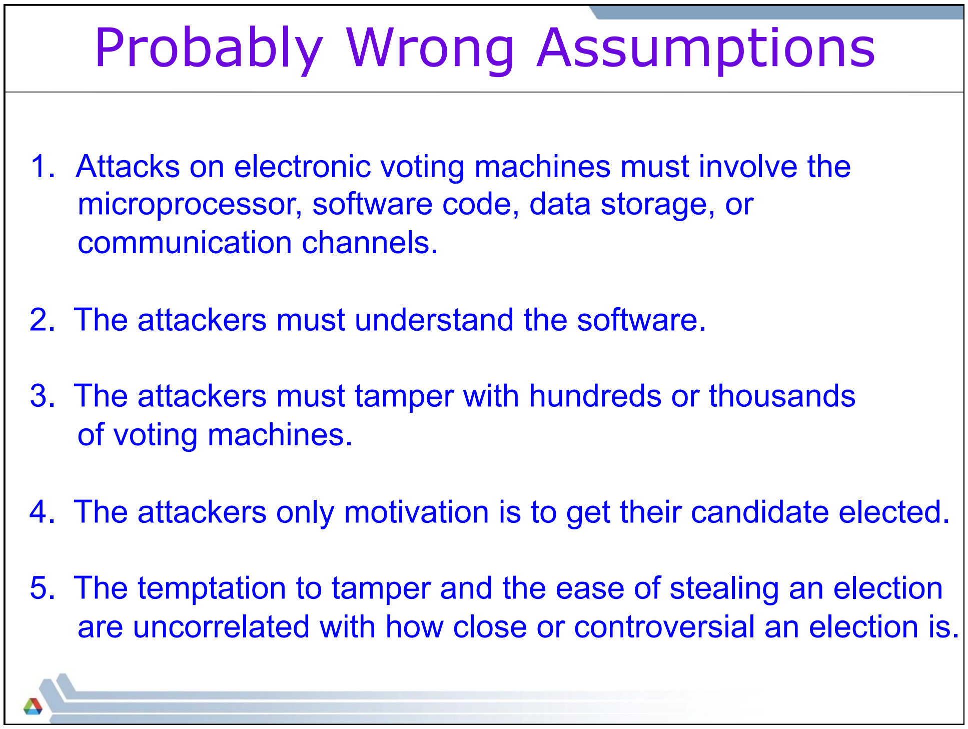
http://www.ne.anl.gov/capabilities/vat

rogerj@anl.gov

Argonne NATIONAL LABORATORY

VAT

> If you look for truth, you may find comfort in the end; if you look for comfort you will get neither truth nor comfort…only soft soap and wishful thinking to begin, and in the end, despair.
> -- C.S. Lewis (1898-1963)



Probably Wrong Assumptions

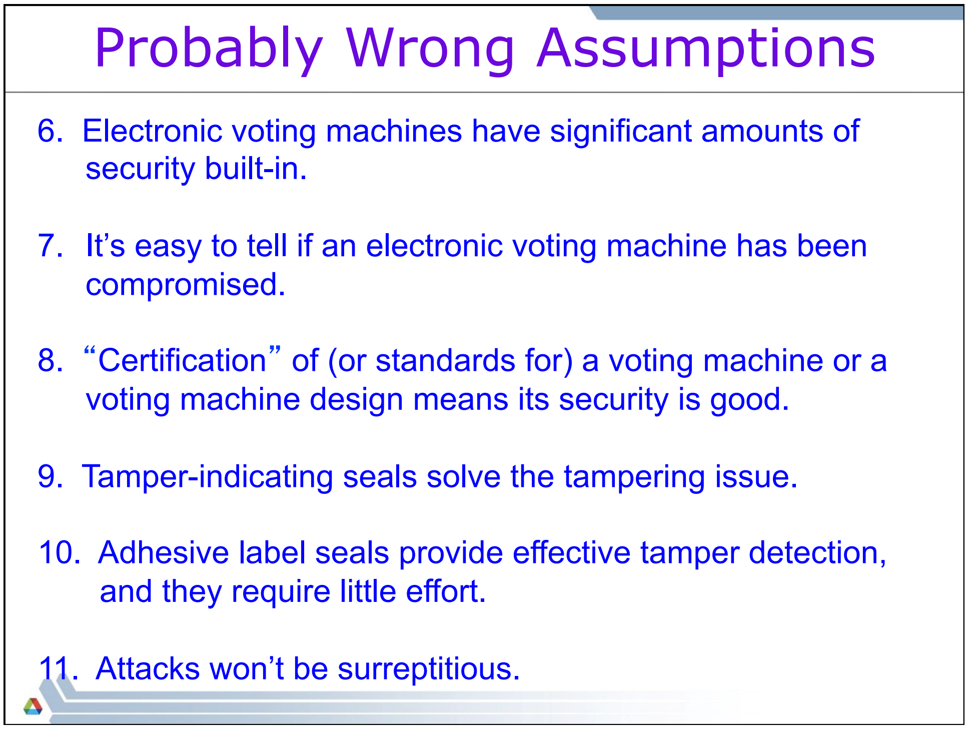
1. Attacks on electronic voting machines must involve the microprocessor, software code, data storage, or communication channels.

2. The attackers must understand the software.

3. The attackers must tamper with hundreds or thousands of voting machines.

4. The attackers only motivation is to get their candidate elected.

5. The temptation to tamper and the ease of stealing an election are uncorrelated with how close or controversial an election is.



Probably Wrong Assumptions

6. Electronic voting machines have significant amounts of security built-in.

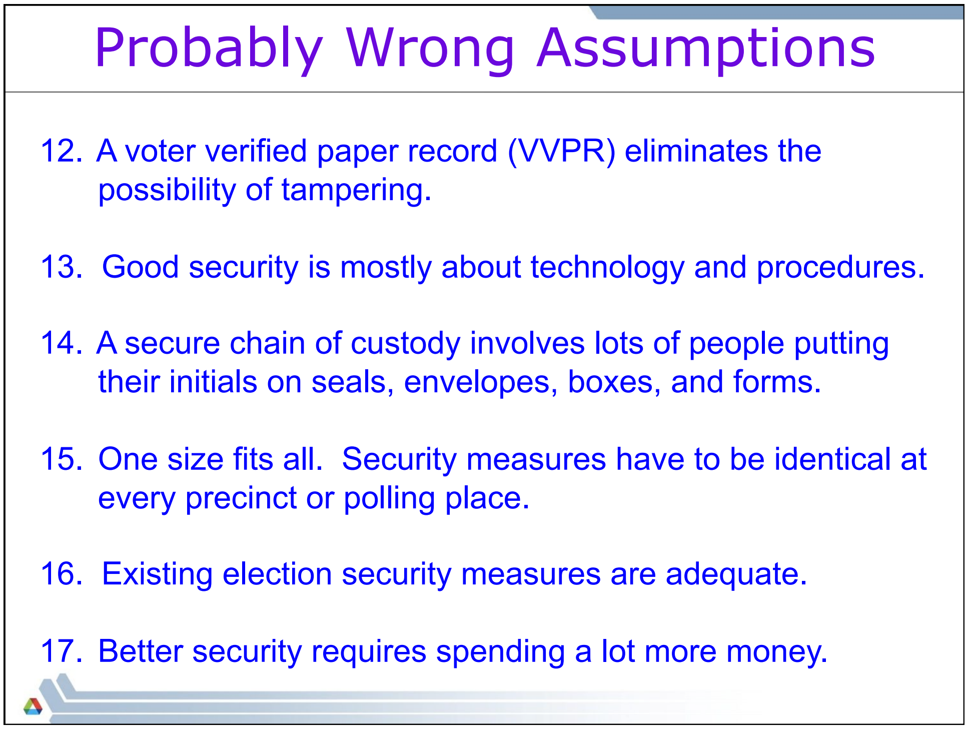
7. It's easy to tell if an electronic voting machine has been compromised.

8. "Certification" of (or standards for) a voting machine or a voting machine design means its security is good.

9. Tamper-indicating seals solve the tampering issue.

10. Adhesive label seals provide effective tamper detection, and they require little effort.

11. Attacks won't be surreptitious.



Probably Wrong Assumptions

12. A voter verified paper record (VVPR) eliminates the possibility of tampering.

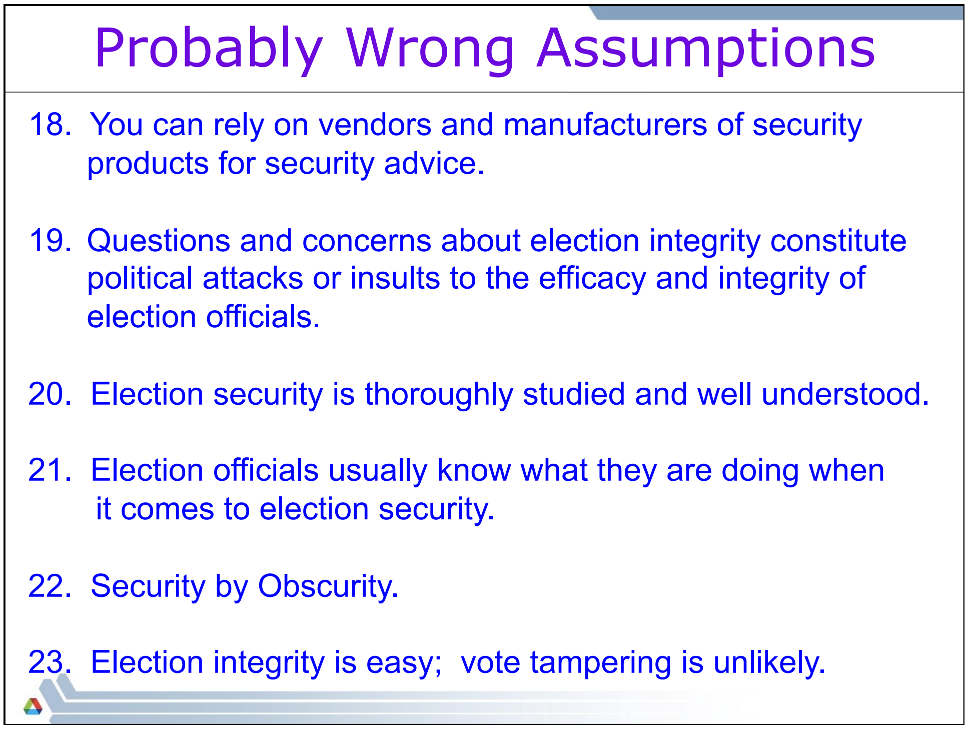
13. Good security is mostly about technology and procedures.

14. A secure chain of custody involves lots of people putting their initials on seals, envelopes, boxes, and forms.

15. One size fits all. Security measures have to be identical at every precinct or polling place.

16. Existing election security measures are adequate.

17. Better security requires spending a lot more money.



Probably Wrong Assumptions

18. You can rely on vendors and manufacturers of security products for security advice.

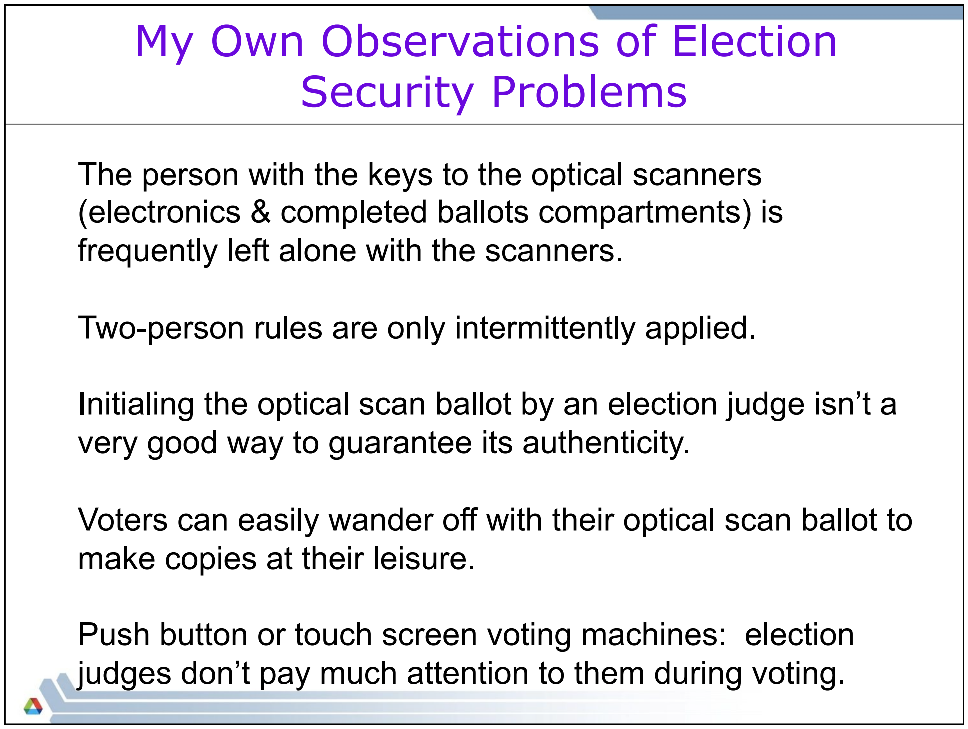
19. Questions and concerns about election integrity constitute political attacks or insults to the efficacy and integrity of election officials.

20. Election security is thoroughly studied and well understood.

21. Election officials usually know what they are doing when it comes to election security.

22. Security by Obscurity.

23. Election integrity is easy; vote tampering is unlikely.



My Own Observations of Election Security Problems

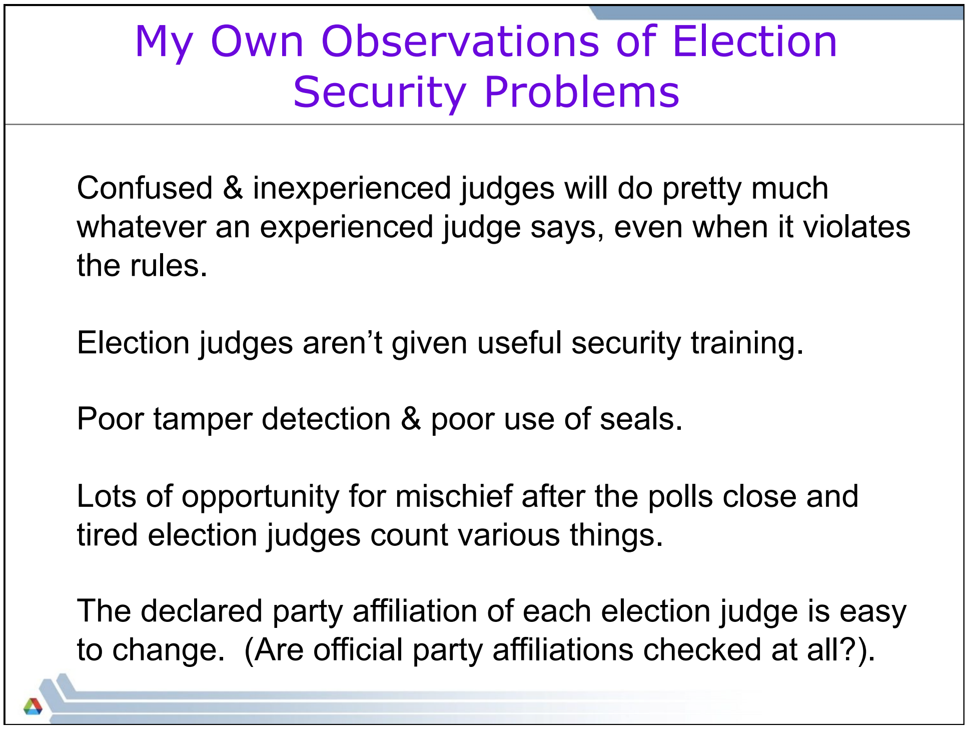
The person with the keys to the optical scanners (electronics & completed ballots compartments) is frequently left alone with the scanners.

Two-person rules are only intermittently applied.

Initialing the optical scan ballot by an election judge isn't a very good way to guarantee its authenticity.

Voters can easily wander off with their optical scan ballot to make copies at their leisure.

Push button or touch screen voting machines: election judges don't pay much attention to them during voting.



My Own Observations of Election Security Problems

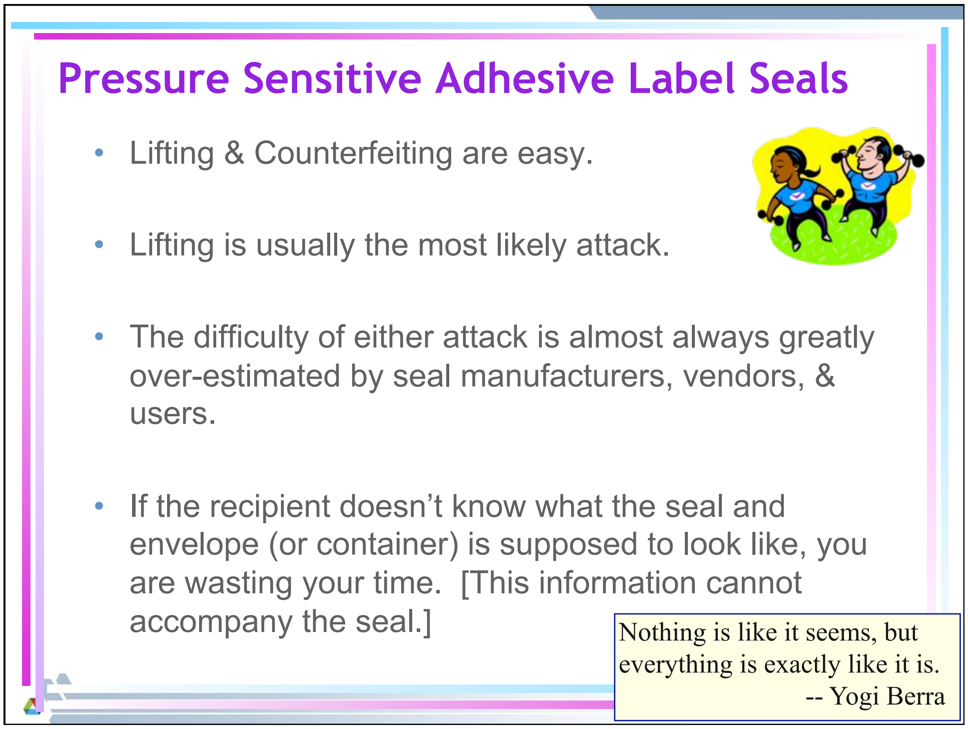
Confused & inexperienced judges will do pretty much whatever an experienced judge says, even when it violates the rules.

Election judges aren't given useful security training.

Poor tamper detection & poor use of seals.

Lots of opportunity for mischief after the polls close and tired election judges count various things.

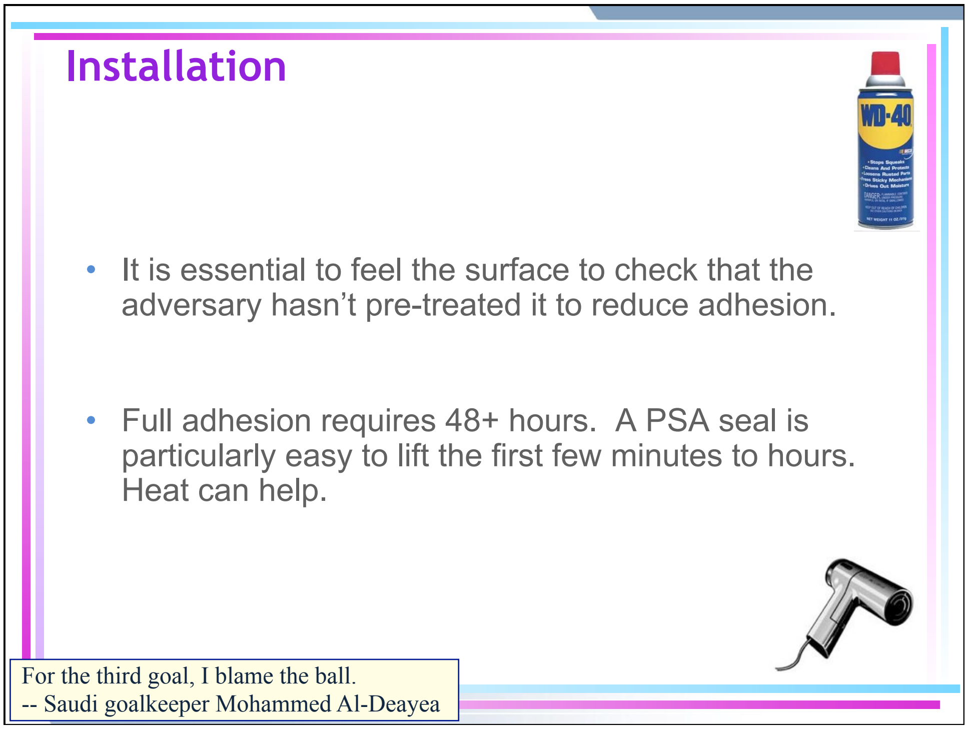
The declared party affiliation of each election judge is easy to change. (Are official party affiliations checked at all?).



Pressure Sensitive Adhesive Label Seals

- Lifting & Counterfeiting are easy.
- Lifting is usually the most likely attack.
- The difficulty of either attack is almost always greatly over-estimated by seal manufacturers, vendors, & users.
- If the recipient doesn't know what the seal and envelope (or container) is supposed to look like, you are wasting your time. [This information cannot accompany the seal.]

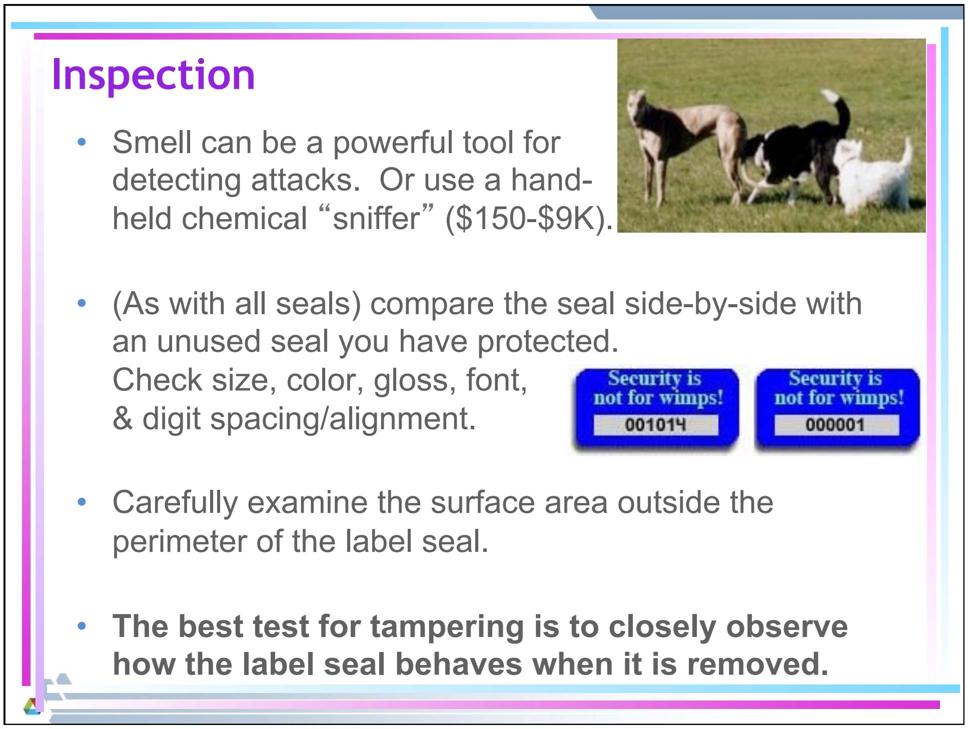
Nothing is like it seems, but
everything is exactly like it is.
-- Yogi Berra



Installation

- It is essential to feel the surface to check that the adversary hasn't pre-treated it to reduce adhesion.
- Full adhesion requires 48+ hours. A PSA seal is particularly easy to lift the first few minutes to hours. Heat can help.

For the third goal, I blame the ball.
-- Saudi goalkeeper Mohammed Al-Deayea



Inspection

- Smell can be a powerful tool for detecting attacks. Or use a hand-held chemical “sniffer” ($150-$9K).

- (As with all seals) compare the seal side-by-side with an unused seal you have protected. Check size, color, gloss, font, & digit spacing/alignment.

- Carefully examine the surface area outside the perimeter of the label seal.

- **The best test for tampering is to closely observe how the label seal behaves when it is removed.**