# ECE 547/647: Security Engineering

Software Security and E-Voting example

© 2018 UMass Amherst Global. All rights reserved.

# Equifax breach indictment,  Feb 10, 2020

- The **Equifax breach**, disclosed in September 2017, exposed the sensitive financial records of nearly 150 million Americans and many other foreigners. After nearly two years of state and federal lawsuits, the company agreed to pay a settlement of at least $650 million. “The scale of the theft was staggering,” Barr said.
- Victim: Months after massive **Equifax data breach**, **victims** struggling to recover. WASHINGTON -- Last year's massive **Equifax data breach** exposed the personal information of 145 million Americans. Despite the company's promises to help, plenty of **victims** have struggled to regain their identities and clean up their credit reports.Jan 9, 2018
- **YESTERDAY:** WASHINGTON—Four members of China’s military have been indicted by the U.S. government on charges of hacking into Equifax Inc. and plundering sensitive data on nearly 150 million Americans as part of a massive heist that officials said also stole trade secrets from the credit-reporting agency.
- In an escalation of U.S. efforts to counter China’s alleged attempts to use **cyber theft** and other means of technology acquisition to become the world’s dominant economic power, a federal grand jury in Atlanta returned a nine-count indictment made public Monday against the **four Chinese nationals working for the People’s Liberation Army**. They are accused of conspiring to steal reams of data as part of a sophisticated hacking operation that exploited a major vulnerability in the software used by Equifax’s online dispute portal.
- The charges for the 2017 breach came as the **U.S. and China remain locked in negotiations over trade** after recently hammering out the first phase of an agreement. In brief remarks on Monday, Attorney General William Barr sought to **distinguish the alleged Equifax theft from accepted intelligence gathering that governments conduct.**
- “This was a deliberate and sweeping intrusion into the private information of the American people,” Mr. Barr said. “We collect information only for legitimate national security purposes; we don’t indiscriminately violate the **privacy of ordinary citizens**,” he said. China has historically denied involvement in hacks on U.S. businesses. The Chinese Embassy in Washington didn’t respond to a request for comment.

© 2018 UMass Amherst Global. All rights reserved.

- Let’s Review from Lesson 5: Human Behavior
  - Security Properties
    - Confidentiality
    - Authentication
    - Integrity
  - The Human Factor
    - Deception and Hoaxes
    - Passwords and Phishing
    - CAPTCHAs
    - SOUPS

© 2018 UMass Amherst Global. All rights reserved.

# Rationale

- Software has major vulnerabilities for a variety of reasons, not all technical.
- Electronic voting provides an example a fairly simple system with complex security issues.

© 2018 UMass Amherst Global. All rights reserved.

# Readings

- Read the Design for Audit paper from Johns Hopkins University

© 2018 UMass Amherst Global. All rights reserved.

# Practice Quiz

- What is a TCB and why should it be minimal for security?
- Why is “secure operating system” probably an oxymoron?
- What is the source of physical entropy in the voting machine paper. How is it used?

© 2018 UMass Amherst Global. All rights reserved.

- **'You can't hack paper': How Oregon fights election meddling**

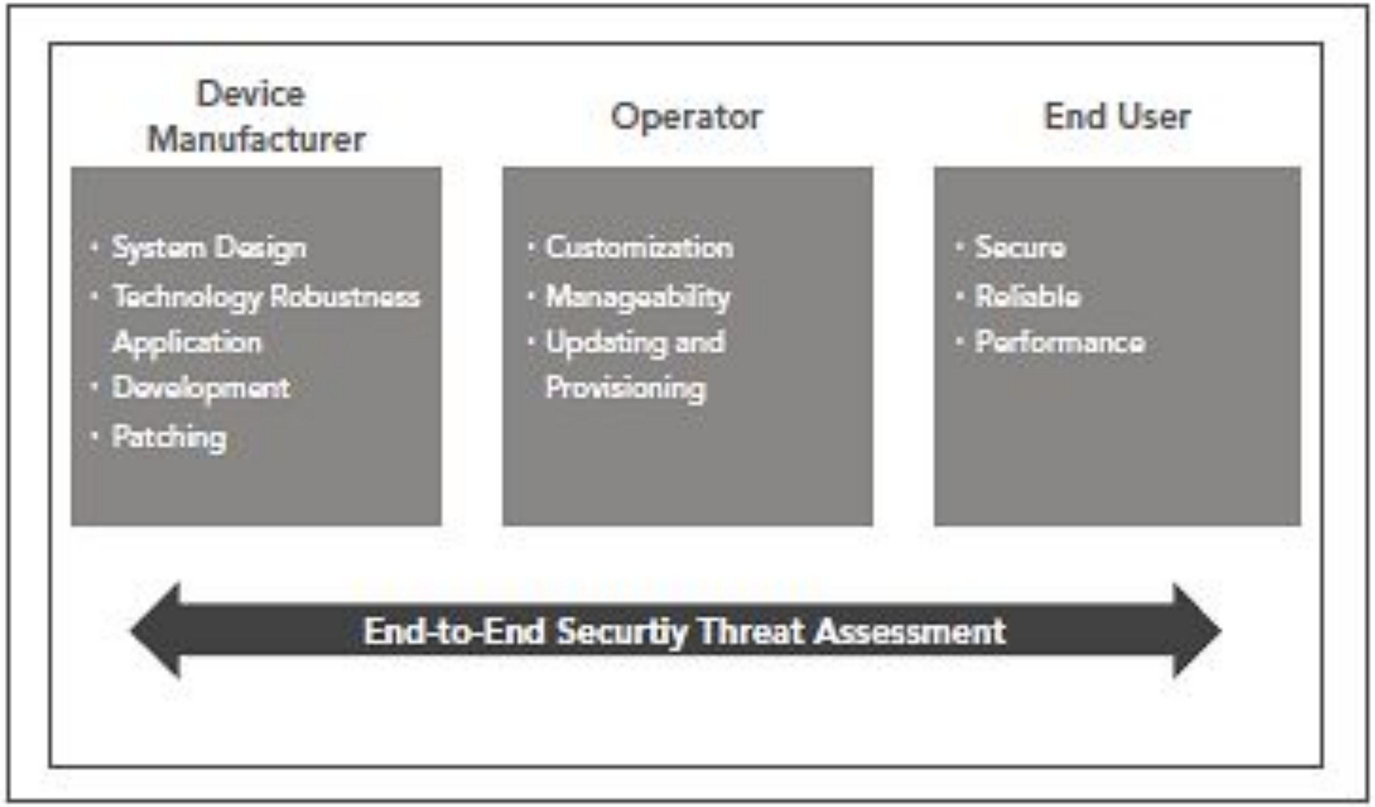
"Throw them on the scrap pile." Oregon officials of both parties say voting machines are inferior to their vote-by-mail system.

https://www.nbcnews.com/politics/elections/you-can-t-hack-paper-how-oregon-fights-election-meddling-n930481

© 2018 UMass Amherst Global. All rights reserved.

# End-to-End Security

- Who is responsible for security?
- Who suffers?
- Incentives are needed for each to take security seriously



Device Manufacturer

- System Design
- Technology Robustness Application
- Development
- Patching

Operator

- Customization
- Manageability
- Updating and Provisioning

End User

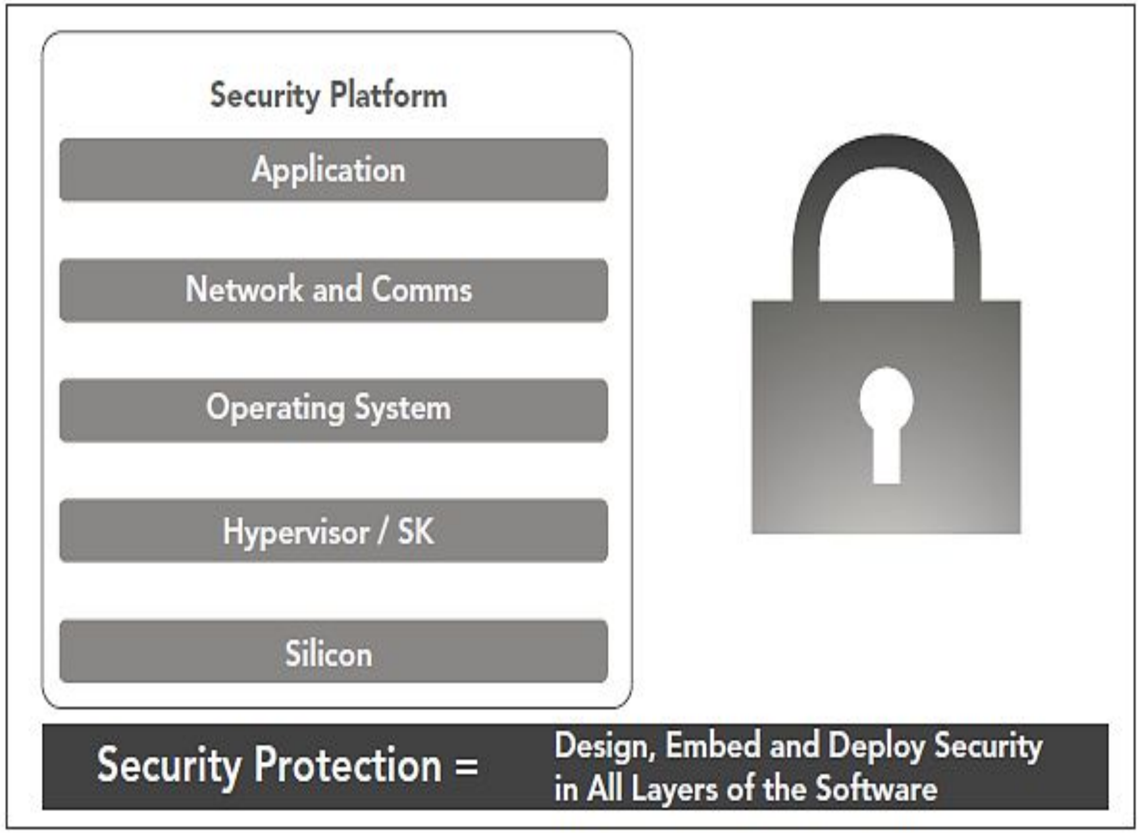
- Secure
- Reliable
- Performance

End-to-End Securtiy Threat Assessment

Wind River, Inc

© 2018 UMass Amherst Global. All rights reserved.

# Software Security Across Layers



- Certification provides:
  - Independent validation
  - From a trusted expert
  - A given component or platform meets specified standards

© 2018 UMass Amherst Global. All rights reserved.

# Security at Every Level

- Applications:
  - Developed with security in mind from the start
  - Utilize new technologies being developed to aid in security robustness
    - Leveraging "gray-listing" or white-listing
  - Design applications with strict security principles
    - Otherwise, the device applications they deliver may be used as back doorways, ultimately for malicious use

- Operating system and communications stacks:
  - Certified communication stack
  - Market segment security validation suites (e.g. Wurldtech Achilles)

© 2018 UMass Amherst Global. All rights reserved.

# Security at Every Level (cont'd)

- Hypervisor: Virtualization is being used more and more to
  - Separate device use
  - Separate human machine interface (HMI)
  - Operating systems from the control operating system
  - Separate the physical interface from the control operating system, etc.

- Silicon: Integrate into the firmware
  - Virtualization,
  - Trusted delivery
  - Trusted boot, etc.

© 2018 UMass Amherst Global. All rights reserved.

# [Discuss:]

- What are the costs of ensuring Security at every level? Who should pay? Microsoft, Facebook, Google and others might not be so profitable if they had to incur the true costs of their products/services…?

© 2018 UMass Amherst Global. All rights reserved.

# Trusted Computing Base (TCB)

- Definition: Parts of a system (hardware, firmware, software) that enforce a security policy

- A good security design should attempt to:
  - Make the TCB as small as possible
  - Minimize the chance for errors in its implementation
  - Simplify careful verification

- Faults outsides the TCB will not help an attacker to violate the security policy enforced by it.

© 2018 UMass Amherst Global. All rights reserved.

# Trusted Computing Base (TCB) (cont’d)

- Example: In a Unix workstation, the TCB includes at least:
    - The operating system kernel including all its device drivers
    - All processes that run with root privileges
    - All program files owned by root with the set-user-ID-bit set
    - All libraries and development tools that were used to build the above
    - The CPU
    - The mass storage devices and their firmware
    - The file servers and the integrity of their network links

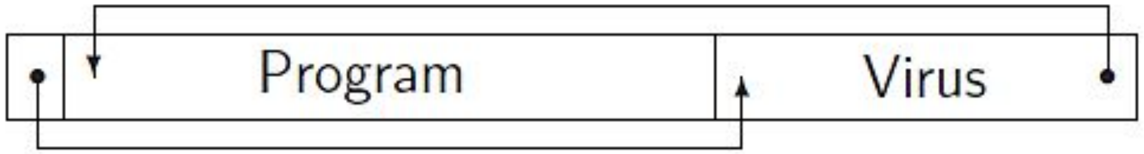
- A security vulnerability in any of these could be used to bypass the entire Unix access control mechanism

© 2018 UMass Amherst Global. All rights reserved.

# Common Terms for Malicious Software

© 2018 UMass Amherst Global. All rights reserved.

# Computer Viruses



- Viruses only able to spread in environments where
  - The access control policy allows application programs to modify the code of other programs (e.g., MS-DOS and Windows)
  - Programs are exchanged frequently in binary form
- The original main virus environment (MS-DOS) supported transient, resident, and boot sector viruses
- As more application data formats (e.g., Microsoft Word) become extended with sophisticated macro languages, viruses appear in these languages as well

© 2018 UMass Amherst Global. All rights reserved.

# Computer Viruses (cont’d)

- Viruses are mostly unknown under Unix. Most installed application programs are owned by `root` with `rwxr-xr-x` permissions and used by normal users
- Unix programs are often transferred as source code, which is difficult for a virus to infect automatically
- Virus scanners use databases with characteristic code fragments of most known viruses and Trojans, which are according to some scanner-venders over 180,000 today (□ polymorphic viruses)
- Virus scanners – like other intrusion detectors – fail on very new or closely targeted types of attacks and can cause disruption by giving false alarms occasionally
- Some virus intrusion-detection tools monitor changes in files using cryptographic checksums

© 2018 UMass Amherst Global. All rights reserved.

# Common Software Vulnerabilities

- Missing checks for data size (□ stack buffer overflow)
- Missing checks for data content (e.g., shell meta characters)
- Missing checks for boundary conditions
- Missing checks for success/failure of operations

- Missing locks – insufficient serialization
- Race conditions – time of check to time of use
- Incomplete checking of environment
- Unexpected side channels (timing, etc.)
- Lack of authentication
- The **“curses of security”** (Gollmann): change, complacency, convenience (software reuse for inappropriate purposes, too large TCB, etc.)

© 2018 UMass Amherst Global. All rights reserved.

# Example for a Missing Check of Data Size

A C program declares a local short string variable

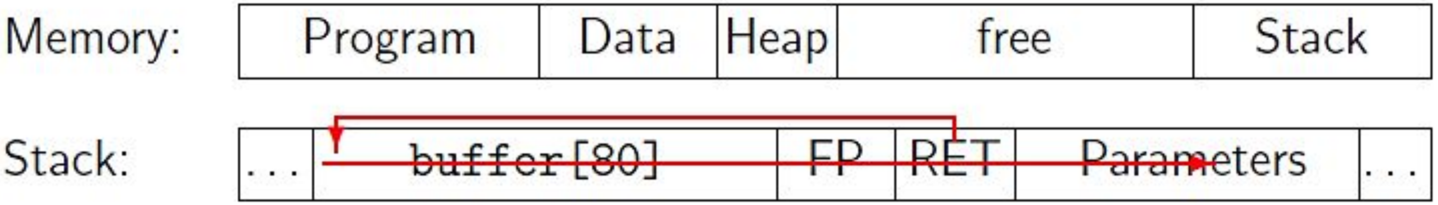
```
char buffer[80];
```

and then uses the standard C library routine call

```
gets(buffer);
```

to read a single text line from standard input and save it in `buffer`

This works fine for normal-length lines but corrupts the stack if the input is longer than 79 characters. Attacker load malicious code into buffer and redirects return address to its start:



© 2018 UMass Amherst Global. All rights reserved.

# Example for a Missing Check of Data Size (cont'd)

- Overwriting the return address is the most common form of a buffer overflow attack. If the return address cannot be reached, alternatives include:
  - Overwrite a function pointer variable on the stack
  - Overwrite previous frame pointer
  - Overwrite security-critical variable value on stack

- Some possible countermeasures (in order of preference):
  - Use programming language with array bounds checking (Java, Ada, C#, Perl, Python, etc.)
  - Configure memory management unit to disable code execution on the stack
  - Compiler adds integrity check values before return address

© 2018 UMass Amherst Global. All rights reserved.

# Integer Overflows

- Integer numbers in computers behave differently from integer numbers in mathematics. For an unsigned 8-bit integer value, we have:

$$\mathbf{255 + 1 == 0}$$

$$\mathbf{0 - 1 == 255}$$

$$\mathbf{16 * 17 == 16}$$

and likewise for a signed 8-bit value, we have

$$\mathbf{127 + 1 == -128}$$

$$\mathbf{-128 / -1 == -128}$$

and what looks like an obvious endless loop

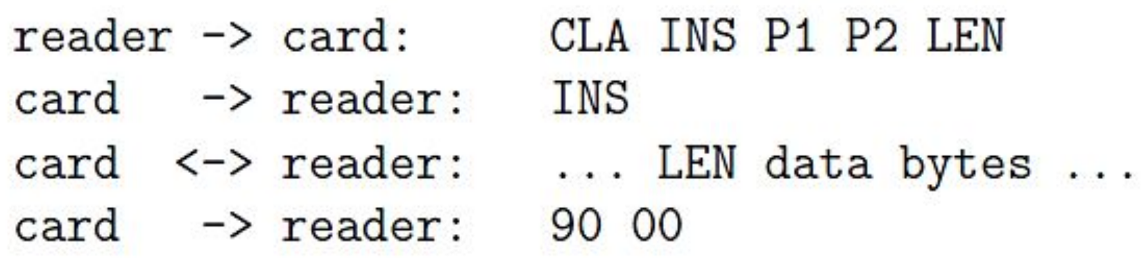
```
int I = 1;
while (i > 0)
  i = i * 2;
```

terminates after 15, 31, or 63 steps (depending on the register size)

© 2018 UMass Amherst Global. All rights reserved.

# Insufficient Parameter Checking

- Historic example:
  - Smartcards that use ISO 7816-3 T=0 protocol exchange data like this:



```
reader -> card:     CLA INS P1 P2 LEN
card   -> reader:   INS
card  <-> reader:   ... LEN data bytes ...
card   -> reader:   90 00
```

  - All exchanges start with a 5-byte header in which the last byte identifies the number of bytes to exchanged
  - In many smartcard implementations, the routine for sending data from the card to the reader blindly trusts the LEN value received
  - Attackers succeeded in providing longer LEN values than allowed by the protocol
  - They then received RAM content after the result buffer, including areas which contained secret keys

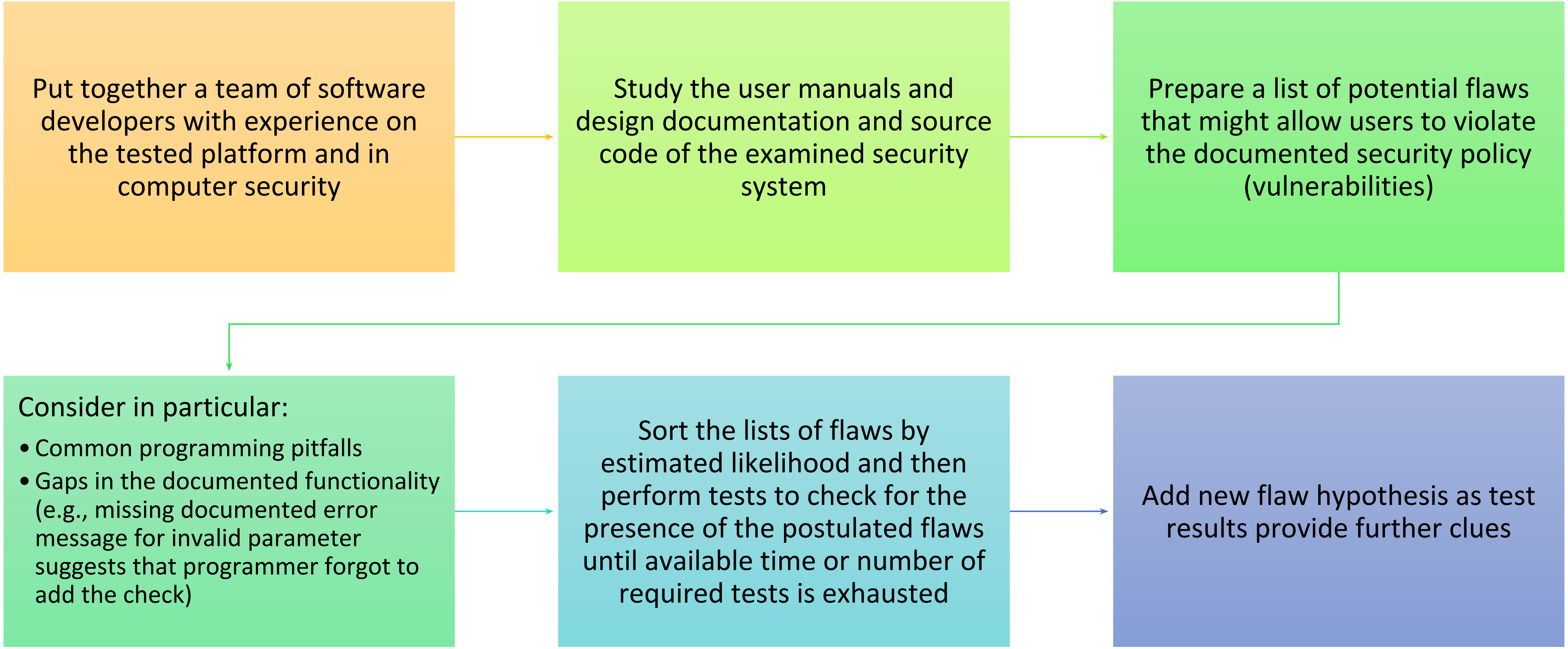
© 2018 UMass Amherst Global. All rights reserved.

# Penetration Analysis/Flaw Hypothesis Testing

- Put together a team of software developers with experience on the tested platform and in computer security
- Study the user manuals and where available the design documentation and source code of the examined security system
- Based on the information gained, prepare a list of potential flaws that might allow users to violate the documented security policy (vulnerabilities). Consider in particular:
    - Common programming pitfalls
    - Gaps in the documented functionality (e.g., missing documented error message for invalid parameter suggests that programmer forgot to add the check)
- Sort the lists of flaws by estimated likelihood and then perform tests to check for the presence of the postulated flaws until available time or number of required tests is exhausted.
- Add new flaw hypothesis as test results provide further clues

© 2018 UMass Amherst Global. All rights reserved.

# Penetration Analysis/Flaw Hypothesis Testing



Put together a team of software developers with experience on the tested platform and in computer security

Study the user manuals and design documentation and source code of the examined security system

Prepare a list of potential flaws that might allow users to violate the documented security policy (vulnerabilities)

Consider in particular:

- Common programming pitfalls
- Gaps in the documented functionality (e.g., missing documented error message for invalid parameter suggests that programmer forgot to add the check)

Sort the lists of flaws by estimated likelihood and then perform tests to check for the presence of the postulated flaws until available time or number of required tests is exhausted

Add new flaw hypothesis as test results provide further clues

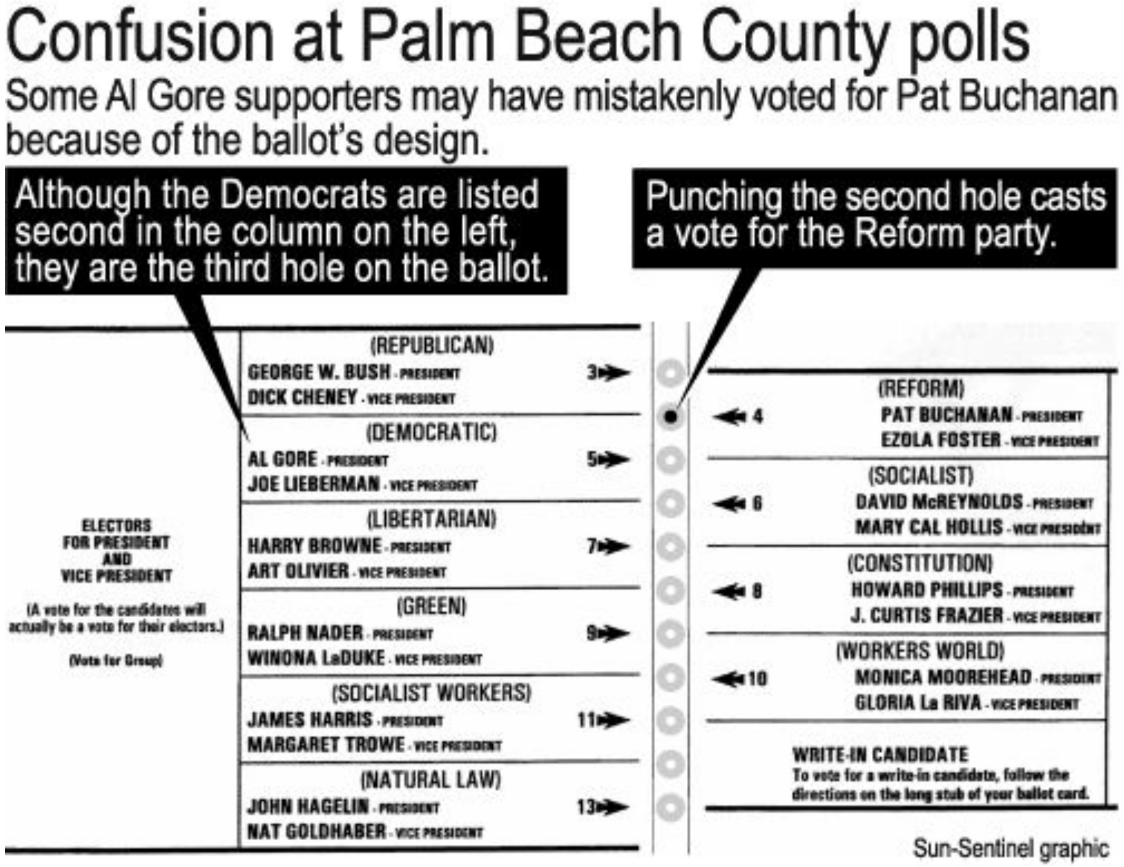
© 2018 UMass Amherst Global. All rights reserved.

# Security Considerations for E-voting

© 2018 UMass Amherst Global. All rights reserved.

# Motivation for E-voting

- National election debacle
    - Outcry for improved process



## Confusion at Palm Beach County polls

Some Al Gore supporters may have mistakenly voted for Pat Buchanan because of the ballot's design.

Although the Democrats are listed second in the column on the left, they are the third hole on the ballot.

Punching the second hole casts a vote for the Reform party.

ELECTORS
FOR PRESIDENT
AND
VICE PRESIDENT

(A vote for the candidates will actually be a vote for their electors.)

(Vote for Group)

(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT 3➜
DICK CHENEY - VICE PRESIDENT

(DEMOCRATIC)
AL GORE - PRESIDENT 5➜
JOE LIEBERMAN - VICE PRESIDENT

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT 7➜
ART OLIVIER - VICE PRESIDENT

(GREEN)
RALPH NADER - PRESIDENT 9➜
WINONA LaDUKE - VICE PRESIDENT

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT 11➜
MARGARET TROWE - VICE PRESIDENT

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT 13➜
NAT GOLDHABER - VICE PRESIDENT

(REFORM)
← 4 PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

(SOCIALIST)
← 6 DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

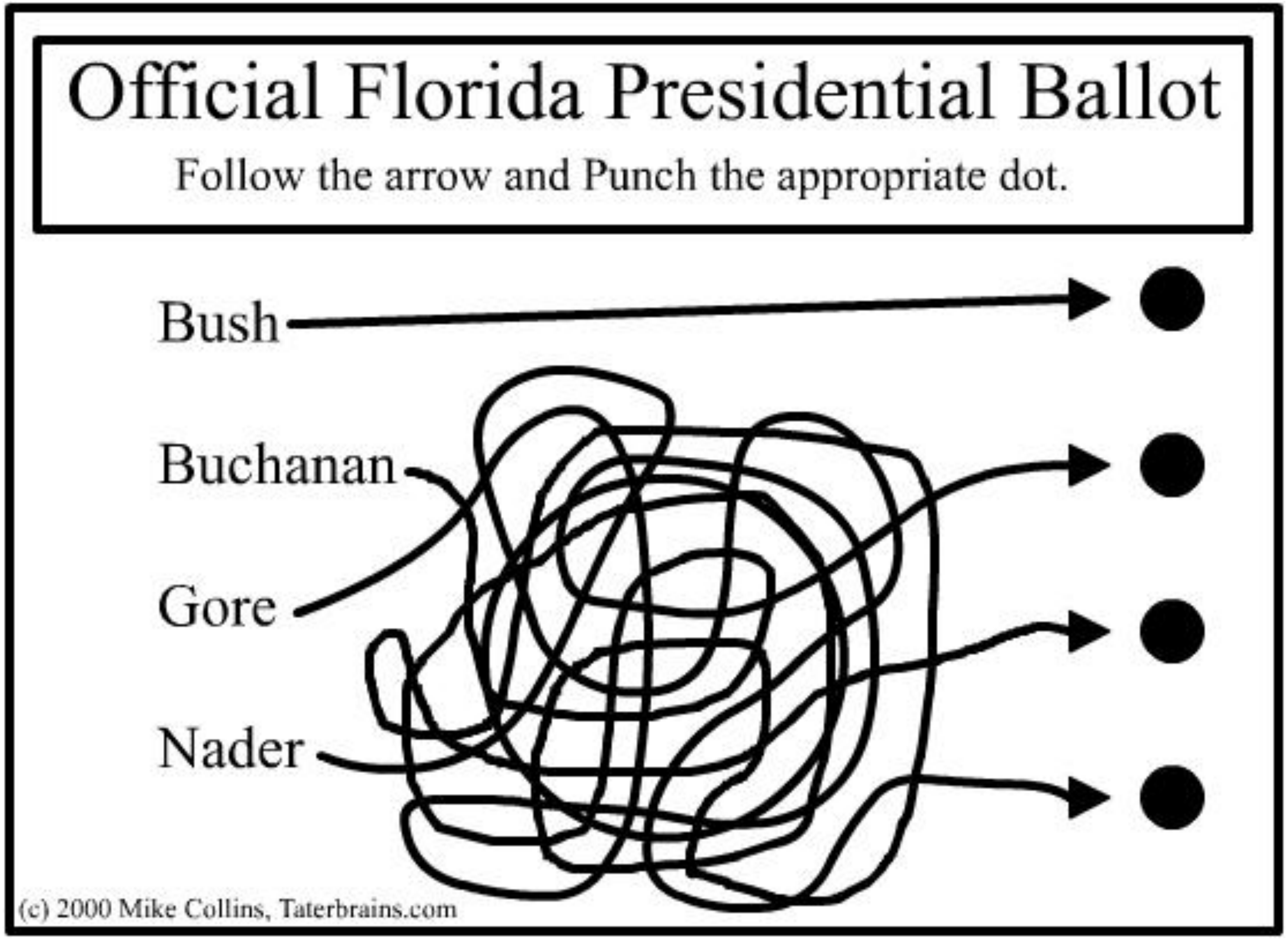
(CONSTITUTION)
← 8 HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

(WORKERS WORLD)
← 10 MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

Sun-Sentinel graphic

© 2018 UMass Amherst Global. All rights reserved.

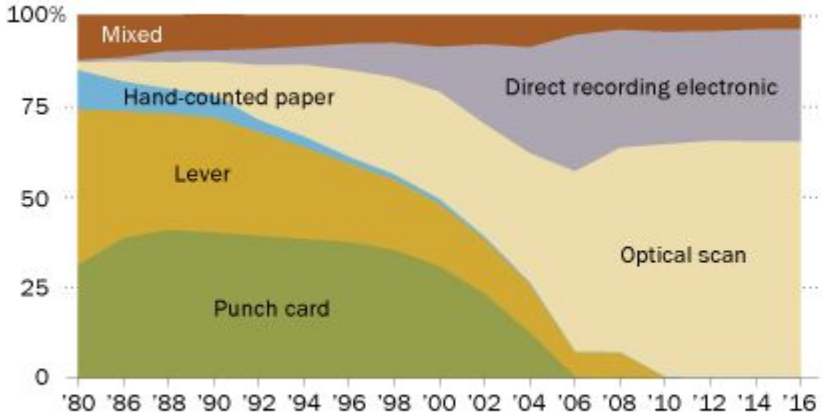

Official Florida Presidential Ballot
Follow the arrow and Punch the appropriate dot.
Bush
Buchanan
Gore
Nader
(c) 2000 Mike Collins, Taterbrains.com

© 2018 UMass Amherst Global. All rights reserved.

# Types of Voting Machines

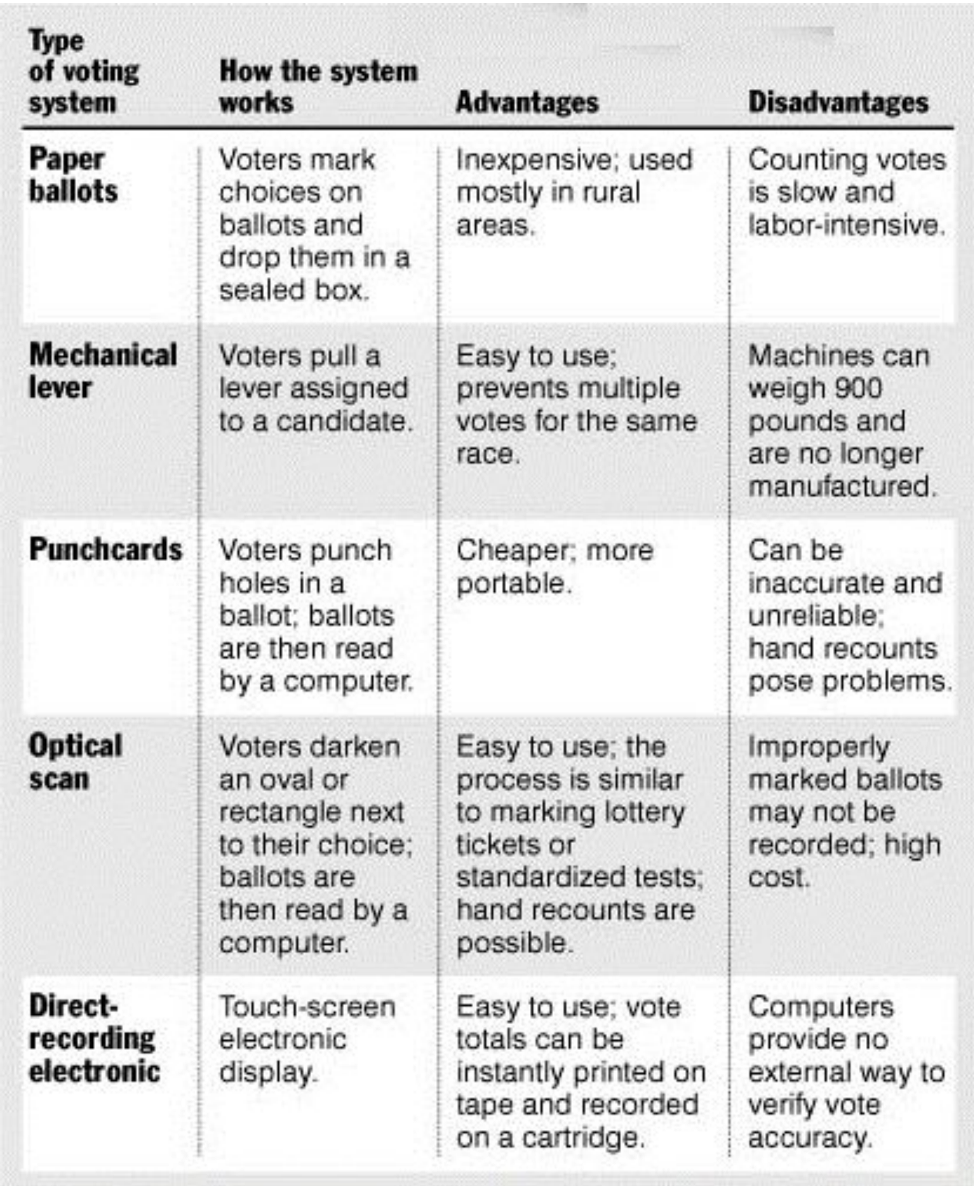
**Where did all the punch-card and lever machines go?**

*Estimated share of registered voters in precincts using ...*



Notes: Excludes precincts that are entirely vote-by-mail. The estimated share of registered voters in precincts using hand-counted paper ballots is 0.1% in 2016.
Source: Election Data Services.

PEW RESEARCH CENTER



| Type of voting system | How the system works | Advantages | Disadvantages |
|---|---|---|---|
| **Paper ballots** | Voters mark choices on ballots and drop them in a sealed box. | Inexpensive; used mostly in rural areas. | Counting votes is slow and labor-intensive. |
| **Mechanical lever** | Voters pull a lever assigned to a candidate. | Easy to use; prevents multiple votes for the same race. | Machines can weigh 900 pounds and are no longer manufactured. |
| **Punchcards** | Voters punch holes in a ballot; ballots are then read by a computer. | Cheaper; more portable. | Can be inaccurate and unreliable; hand recounts pose problems. |
| **Optical scan** | Voters darken an oval or rectangle next to their choice; ballots are then read by a computer. | Easy to use; the process is similar to marking lottery tickets or standardized tests; hand recounts are possible. | Improperly marked ballots may not be recorded; high cost. |
| **Direct-recording electronic** | Touch-screen electronic display. | Easy to use; vote totals can be instantly printed on tape and recorded on a cartridge. | Computers provide no external way to verify vote accuracy. |

© 2018 UMass Amherst Global. All rights reserved.

# Poll Site Voting

- Computerized voting machines
  - Automatic counting
  - GUI display with pictures possible
  - Perhaps network linkage across sites
  - Most popular: Direct Recording Electronic (DRE) machines
    - Vote counted in a cartridge
    - Already being deployed in many places

© 2018 UMass Amherst Global. All rights reserved.

# Desirable Properties of Voting Machines

- Voter feels that
  - Vote was counted
  - Vote was private
  - Nobody else can vote more than once
  - Nobody can alter others’ votes
- People believe that the machine works correctly and that its behavior cannot be modified
- These have to do with **perception**.
- It is also important that these perceptions are **true**.

© 2018 UMass Amherst Global. All rights reserved.

# Audit Trail

- It is important that **all** phases of the vote casting and counting be auditable

- Recounts must be possible if results come into question

- For electronic systems, need to audit
  - Hardware and software development
  - System deployment
  - All system binaries (compiled code, as well as compiler)
  - Use of system

Currently, such audit of hardware and software is not common, and is considered very difficult, if not impossible

© 2018 UMass Amherst Global. All rights reserved.

# Electronic Systems

- Several well understood concepts
  - The more software, the more flaws
  - Electronic systems are expected to fail at times
  - We talk about *failure modes*, not whether or not things fail

- Software security
  - It is very difficult to examine software and understand its behavior
    - Especially with malicious programmer
  - It is difficult to know that a particular source code matches a particular binary
  - It is difficult to know that a particular binary is installed on a particular platform

- There are many anecdotes of voting systems failing…

© 2018 UMass Amherst Global. All rights reserved.

- Example: Software glitch in November 2013’s state-wide election in Virginia, USA
  - Advanced Voting Solutions touchscreen machines

  - “Voters in three precincts reported that when they attempted to vote for [School Board member Rita S. Thompson], the machines initially displayed an ‘x’ next to her name but then, after a few seconds, the ‘x’ disappeared.
  - In response to Thompson's complaints, county officials tested one of the machines in question yesterday and discovered that it seemed to subtract a vote for Thompson in about ‘one out of a hundred tries,’ said Margaret K. Luca, secretary of the county Board of Elections.”

(Cho, 2003)

© 2018 UMass Amherst Global. All rights reserved.

# Discussion

- Software security.  Consider the implications of **requiring** UNIX vs. Windows OS.  Consider the implications of using more modern languages like Python and Java vs. C.

© 2018 UMass Amherst Global. All rights reserved.

# Voter Verifiable Audit

- Enables recounts
- Voter confidence
- Harder to tamper with the election
- Probably involves paper
- Surprise recounts

**The piece of paper that is verified by the voter is used in the recount**

© 2018 UMass Amherst Global. All rights reserved.

# Insider Threat

- Easy to hide code in large software packages
- Virtually impossible to detect back doors
- Skill level needed to hide malicious code is much lower than needed to find it
- Anyone with access to development environment is capable
- Requires
  - background checks
  - strict development rules
  - physical security

© 2018 UMass Amherst Global. All rights reserved.

# Software Dangers

- Software is complex
  - Top metric for measuring number of flaws is lines of code
- Windows Operating System
  - Tens of millions of lines of code
  - New “critical” security bug announced every week
- Unintended security flaws **unavoidable**
- Intentional security flaws **undetectable**

© 2018 UMass Amherst Global. All rights reserved.

SYSTEMS
DIEBOLD
Which state is the first in the nation in efforts to reform elections?
(Vote for One)
New York
California
Georgia
Michigan

© 2018 UMass Amherst Global. All rights reserved.

# Code Analysis

- 56-bit DES in CBC mode with static IVs used to encrypt votes and audit logs

```
#define DESKEY ((des_key*)"F2654hD4")
```

- Unkeyed public function (CRC) used for integrity protection
- No authentication of smartcard to voting terminal
    - (the PIN authenticates the terminal to the card)
- Insufficient code review

© 2018 UMass Amherst Global. All rights reserved.

# E-Voter Security Recommendation #1

- Separate vote casting from tabulating
    - Touch screen machine produces paper ballot
        - Need not be as trusted as today's DREs

    - Voter can use or destroy

    - Scanning and tabulating machine
        - Small code base
        - Open source
        - Extensive testing and certification
        - Different manufacturer from touch screen

© 2018 UMass Amherst Global. All rights reserved.

# E-Voter Security Recommendation #2

- Transparency
  - Require designs of machines to be public
  - Require security audit of machines by qualified experts
    - Require public report of this audit
  - Require open source for vote tabulation code
    - necessary but not sufficient

© 2018 UMass Amherst Global. All rights reserved.

# E-Voter Security Recommendation #3

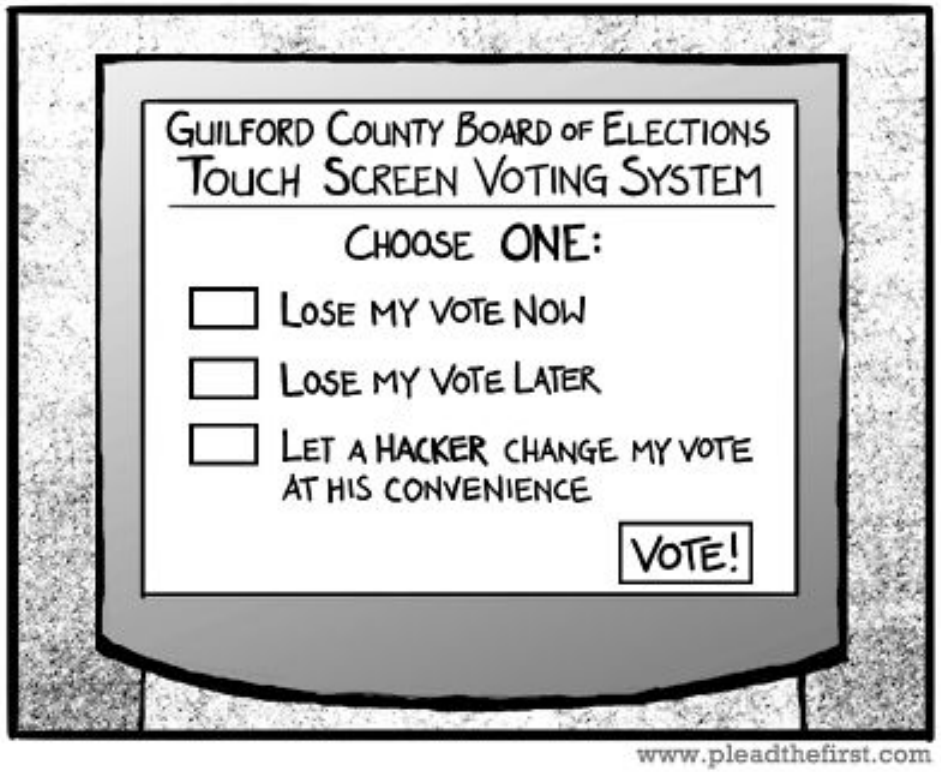
- Quality control
  - Establish criteria for testing the expertise of manufacturers
    - NIST could play this role
  - Require source code analysis for certification
  - Establish standards for policies and procedures
    - Aim for simplicity: The more complicated and burdensome, the less likely to be followed

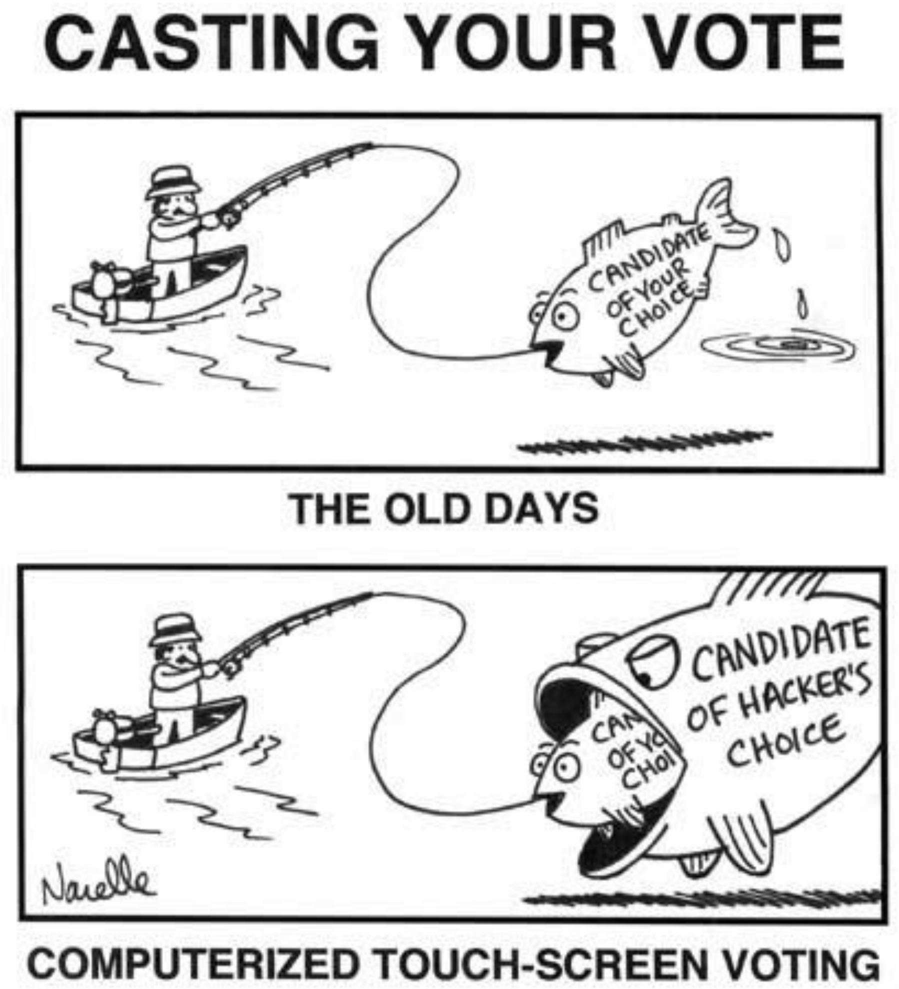
© 2018 UMass Amherst Global. All rights reserved.

# E-Voter Security Threats

- Gauge the threat based on:
  - Type of election (public vs. private)
  - Consequences of a successful attack
  - Value of election outcome to potential adversaries
  - Expertise, skill & resources needed to disrupt
  - Level of motivation of potential attackers
  - Amount of disruption needed to sway the election or call its outcome into doubt
  - Consequences of a perception of unfair outcome

© 2018 UMass Amherst Global. All rights reserved.


GUILFORD COUNTY BOARD OF ELECTIONS
TOUCH SCREEN VOTING SYSTEM
CHOOSE ONE:
□ LOSE MY VOTE NOW
□ LOSE MY VOTE LATER
□ LET A HACKER CHANGE MY VOTE AT HIS CONVENIENCE
VOTE!
www.pleadthefirst.com



© 2018 UMass Amherst Global. All rights reserved.

# Internet Voting in Public Elections

- Social issues:
  - Vote coercion
  - Vote sale
  - Vote solicitation (*click here to vote*, banner ads)

**NOT A GOOD IDEA!**

- Technical issues:
  - Securing the platform
  - Securing the communications channel

© 2018 UMass Amherst Global. All rights reserved.

# Necessary Precautions for Computerized Poll Site Voting

- Care should be taken if voting machines are given network access
- Vote cartridges (for DRE systems)
  - Resistant to dropping, temperature change, magnetic forces
  - Should have physical world backup (paper)
  - Imagine a ruined/lost cartridge from a neighborhood with a particular, known demographic.
- Concentrate effort and funding on audit process, make sure neutral parties are involved, or balance with officials from opposing parties

**Best advice might be to use optical scan with poll site tallying.**

© 2018 UMass Amherst Global. All rights reserved.

# Key Security Concerns

- Insecure platform
  - Trojan horses, viruses, worms
  - Malicious hijacked system
    - In cyber café
    - At neighbor’s house
    - Roaming laptop
- Denial of Service attacks
  - Ex. MyDoom attacking SCO
  - 30 day window, but most people vote on last day
- Phishing/man in the middle attack
  - Especially effective against privacy
  - Allows automated vote selling

© 2018 UMass Amherst Global. All rights reserved.