Computer Security & Privacy

Melissa Winstanley (mwinst@cs.washington.edu)

(based on slides by Daniel Halperin)

How exploration sessions work

- You get 1/3 point of extra credit for each session
  - Attendance and homework
  - So you probably aren't doing this for the extra credit…
- Variety of topics
  - Any you particularly desire?

Overview

What is computer security?

- There are many reasons for failure
- **Reliability**
  - Accidental failures
- **Usability**
  - Operating mistakes by users
- **Security**
  - *Intentional* failures caused by *intelligent* parties
  - Involves an *adversary*
- All three are connected

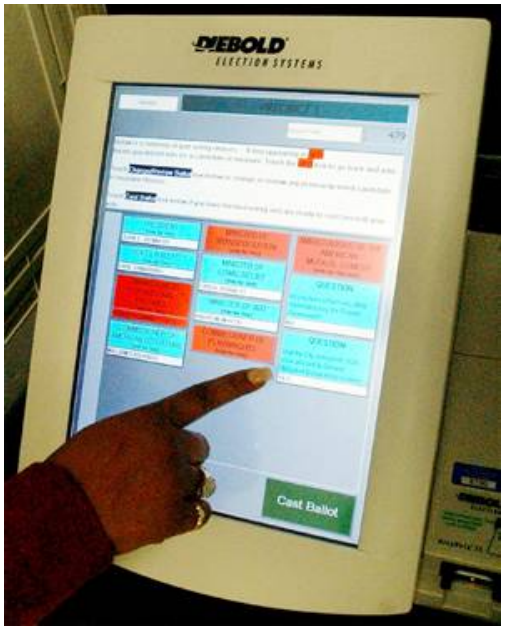
Security Mindset

- Composed of 5 parts
  - Security goals
  - Assets
  - Adversaries
  - Threats
  - Risks
- Perfect security DOES NOT exist
  - Risk management, not “yes or no”
  - Security mindset helps us evaluate risks

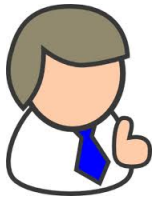
Approaches

- Prevention
  - Stop the attack
- Detection
  - Detect ongoing or past attack
- Response
  - Respond to attacks
- Different approaches for different situations and systems

Example: Electronic Voting



The System

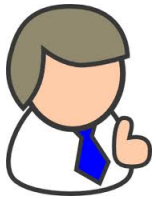


Poll worker

Poll workers load "ballot definition files" on voting machine

The System

Ballot definition file

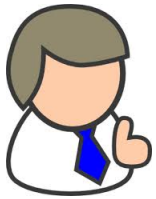


Poll worker

Poll workers load "ballot definition files" on voting machine

The System

Ballot definition file

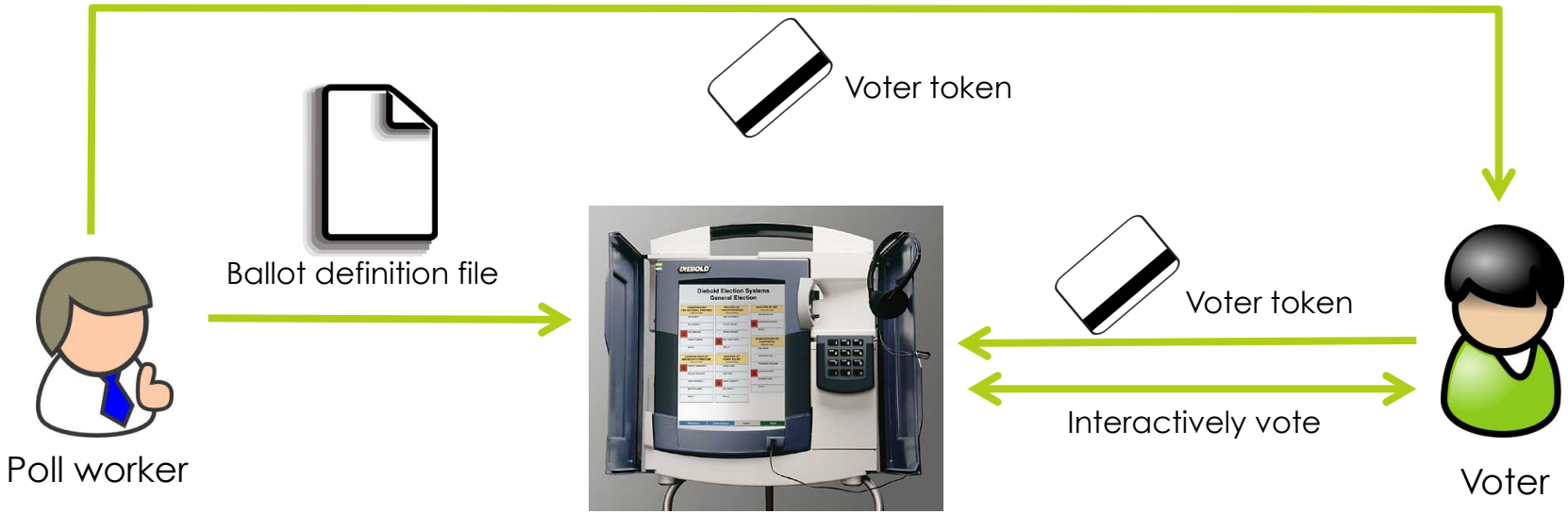


Poll worker

Voter

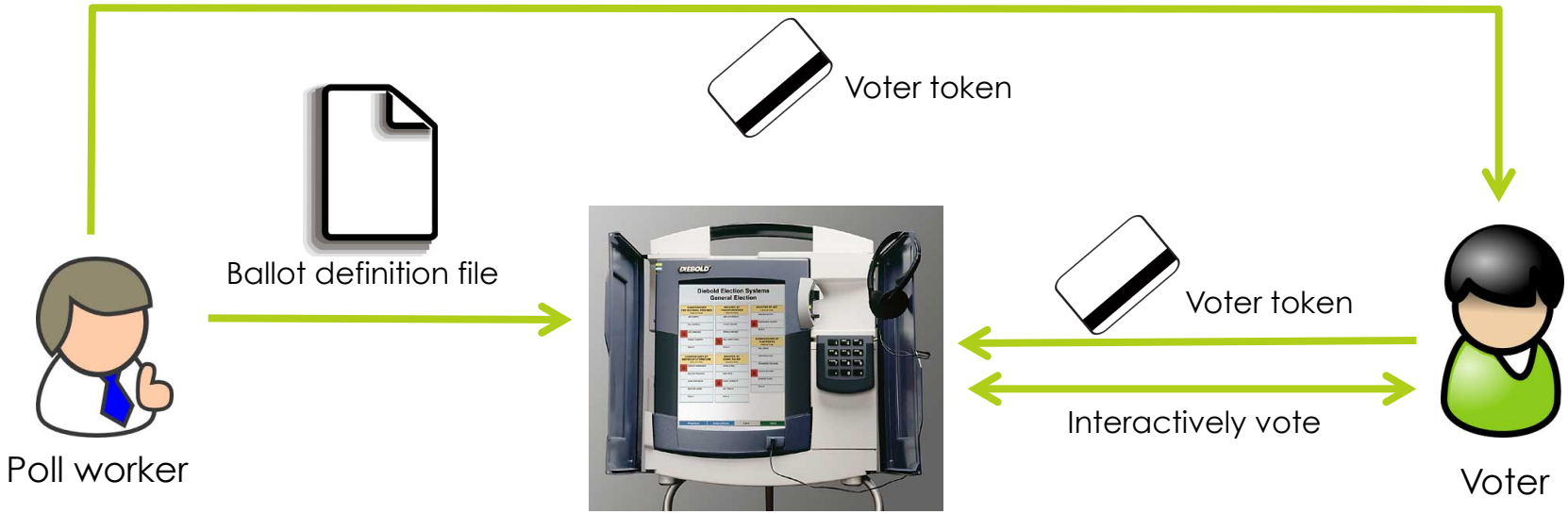
Voters obtain "single-use" tokens from poll workers. Voters use tokens to activate machines and vote.

The System



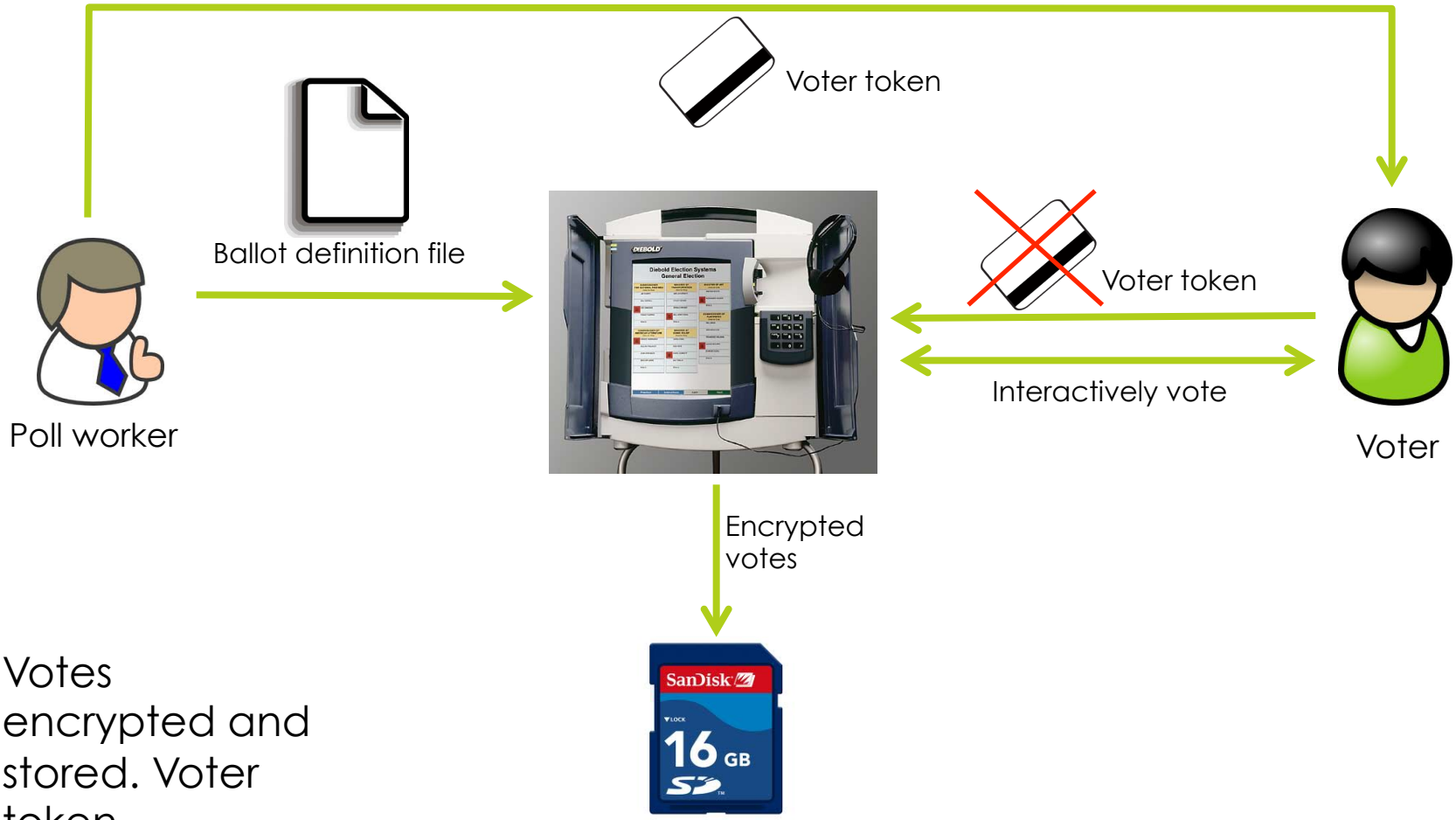
Voters obtain "single-use" tokens from poll workers. Voters use tokens to activate machines and vote.

The System



Votes encrypted and stored. Voter token cancelled.

The System



Votes encrypted and stored. Voter token cancelled.

The System

Stored votes transported to tabulation center.

The System

Stored votes transported to tabulation center.

What about our model?

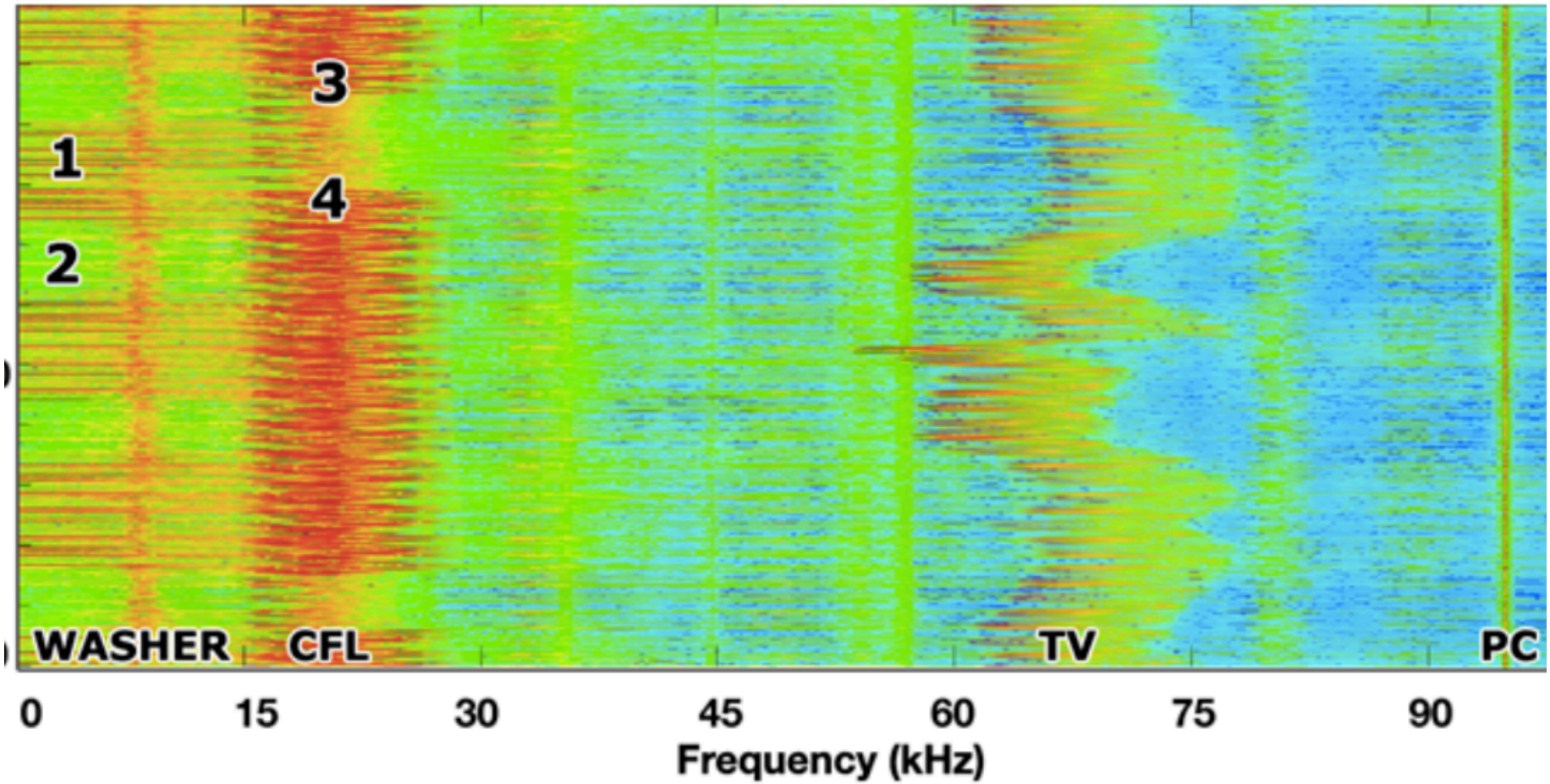
- What are the **goals** of this system?
- What are the **assets**?
- Who are the **adversaries**?
- What are the potential **threats**?

Overall security goals

- Confidentiality / privacy
- Integrity
- Authenticity
- Availability

An example: Does your TV leak information?

Electromagnetic signals



Washer cycle on (1) and off (2). Light off (3) and on (4).

Predicting TV content

- Modern electronics leak energy on the power lines
  - Often due to highly efficient power supplies
- Can we take the energy signature of your TV and predict what you are watching?
- Answer: YES
  - Given a set of pre-determined signatures for videos, match the sample to something in a set
  - Match rate above 90%
- Not too scary
  - You need that set of videos first
- But think about the possibilities: computer content? Password identification?

User Authentication

(Passwords)

Types of authentication

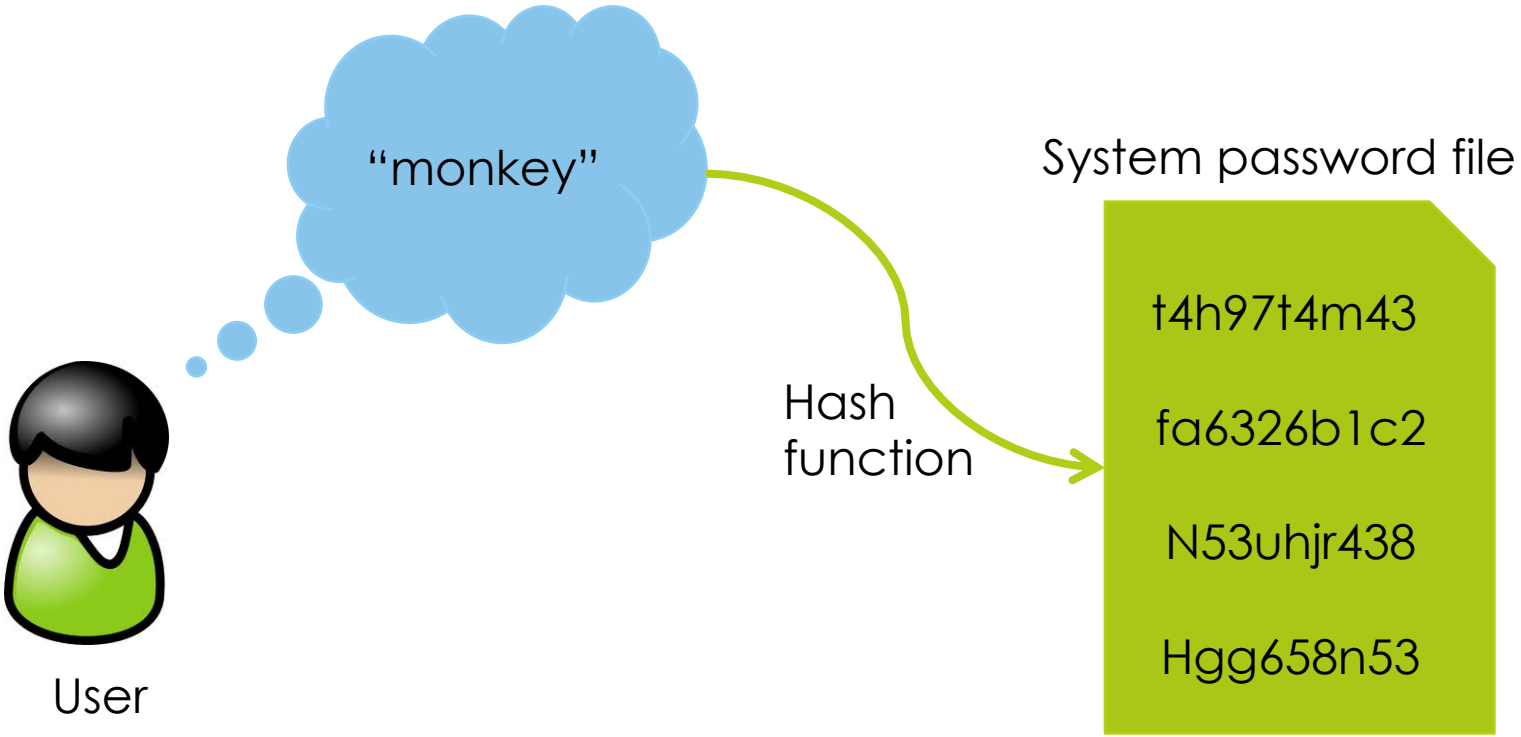
- 3 general types
  - Something you know
  - Something you have
  - Something you are
- Best solution: **multi-factor authentication**

Passwords

- Most common type of user authentication
- How should we store passwords on the server?
  - In cleartext?
  - Encrypted?
  - Hashed?
- **Hashing** transforms the data into a fixed-length sequence of bits that has the following properties:
  - Seemingly random
  - Hard to reverse
  - Fragile
  - Unlikely to collide
  - Slow to compute

How it works

- Instead of password, store Hash(password)

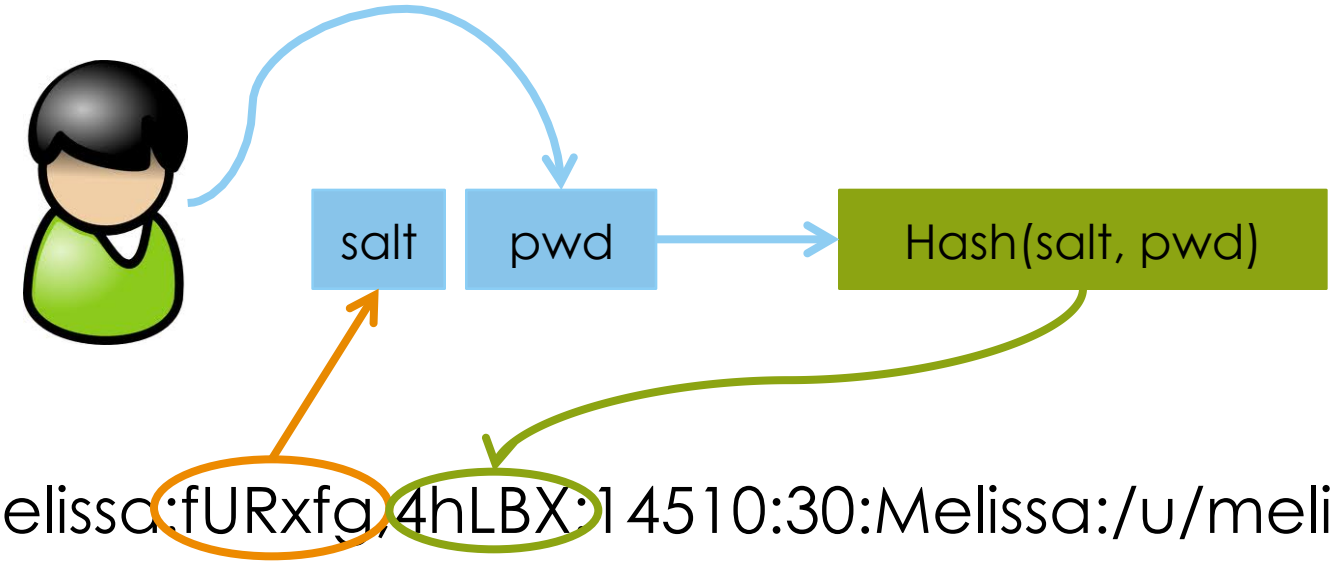


Problem: randomness

- Problem: Passwords are not truly random
  - 26 upper-case, 26 lower-case, 10 digits, 32 punctuation
    - 94^8 = **6 quadrillion** possible 8-character passwords
  - Humans use ~**1 million** common passwords
- Problem: password file /etc/passwd is world-readable
  - Windows: C:\WINDOWS\system32\config\SAM
- **Dictionary attack**
  - Common passwords come from a small "dictionary"
  - Attacker computes hashes of all words in the dictionary
  - For 1,000,000 passwords → about 14 hours
  - Words for *all users*

Solutions

- How could we fix this problem?
- **Salt**: different "dictionary" of hashes for every user



- Dictionary attack not impossible – just much harder!

Other password problems

- K
- Sl
-
-
-

PREVIOUS POST NEXT POST

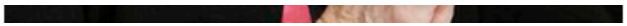
Palin E-Mail Hacker Says It Was Easy

By Kim Zetter ✉ September 18, 2008 | 10:05 am | Categories: Elections, Hacks and Cracks

after the password recovery was reenabled, it took seriously 45 mins on wikipedia and google to find the info, Birthday? 15 seconds on wikipedia, zip code? well she had always been from wasilla, and it only has 2 zip codes (thanks online postal service!)

the second was somewhat harder, the question was "where did you meet your spouse?" did some research, and apparently she had eloped with mister palin after college, if youll look on some of the screenshits that I took and other fellow anon have so graciously put on photobucket you will see the google search for "palin eloped" or some such in one of the tabs.

I found out later though more research that they met at high school, so I did variations of that, high, high school, eventually hit on "Wasilla high" I promptly changed the password to popcorn and took a cold shower…



http://www.wired.com/threatlevel/2008/09/palin-e-mail-ha/

Other types of authentication

- Graphical passwords
  - Often have same problems as text passwords
  - Users pick easy things to remember (and guess)
- Biometrics
  - Often much harder to duplicate
  - But can lead to weird situations (car thief cutting off finger to gain access to fingerprint-activated car)
- Handwriting
  - Also good, but computers are getting better
- Key
  - Can be picked

An Example: Cars

From Professor Tadayoshi Kohno
(http://www.pbs.org/wgbh/nova/tech/tadayoshi-kohno.html)

Social Engineering

What is social engineering?

- Manipulating people
  - Actions they wouldn't ordinarily take
  - Information they wouldn't ordinarily reveal
- *Stereotype*: hackers typing away at computers in dark basements
- *Reality*: hackers as social people
- Employees can be a company's worst enemy

A situation

- Imagine Eve wants a phone, but doesn't want the mandatory calling plan
- Eve calls the store and gets the name of an employee
- Eve calls another branch of the store, pretending to be that employee
  - Says that they sold a customer a phone and plan, but were out of the phones
  - "Can you help the customer out?"
- Eve goes to the second branch and picks up the phone
  - Gets it free of charge!

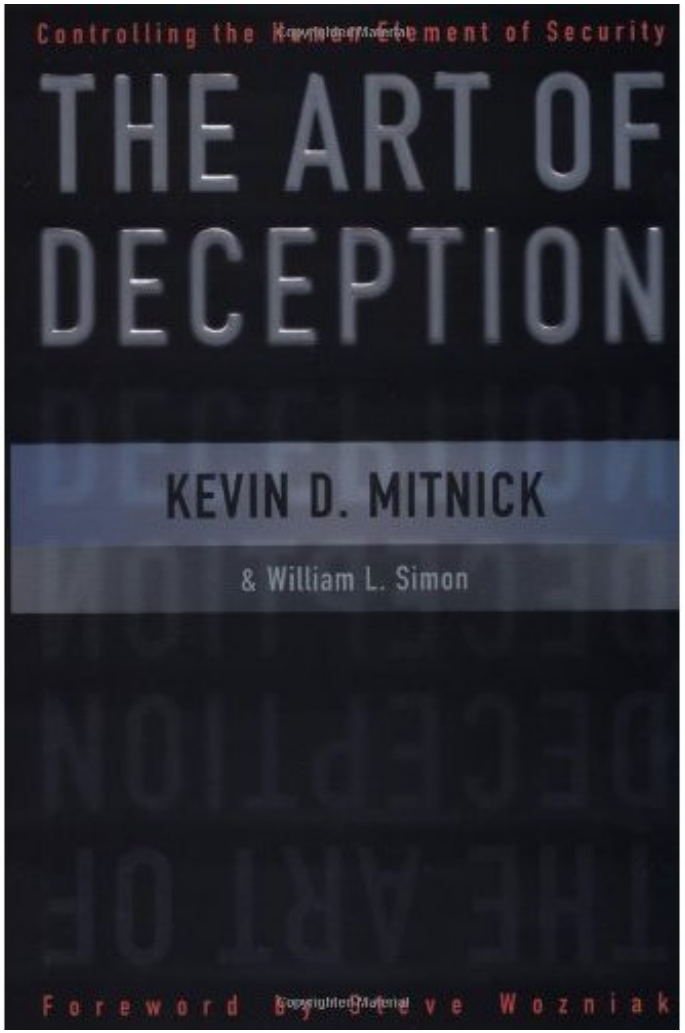
Phishing

- Email pretends to be from a legitimate source
- Asks for private user information
- Surprisingly effective: if it looks legitimate, people believe it

Experiment at Indiana University

- Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster
- Sent 921 Indiana University students a spoofed email that appeared to come from their friend
- Email redirected to a spoofed site inviting the user to enter his/her secure university credentials
  - Domain name clearly distinct from indiana.edu
- **72% of students entered their real credentials into the spoofed site**
- *Only 36% of technology students*

The Art of Deception



Software Security, Physical Security, Web Security, Cryptography…

…and so much more!

What is wrong with the following?

```
// Checks whether the user-given string matches the
// password.
public boolean checkPwd(String pwd, String userInput) {
    if (pwd.length() != userInput.length()) {
        return false;
    }
    for (int i = 0; i < pwd.length(); i++) {
        if (pwd.charAt(i) != userInput.charAt(i)) {
            return false;
        }
    }
    return true;
}
```

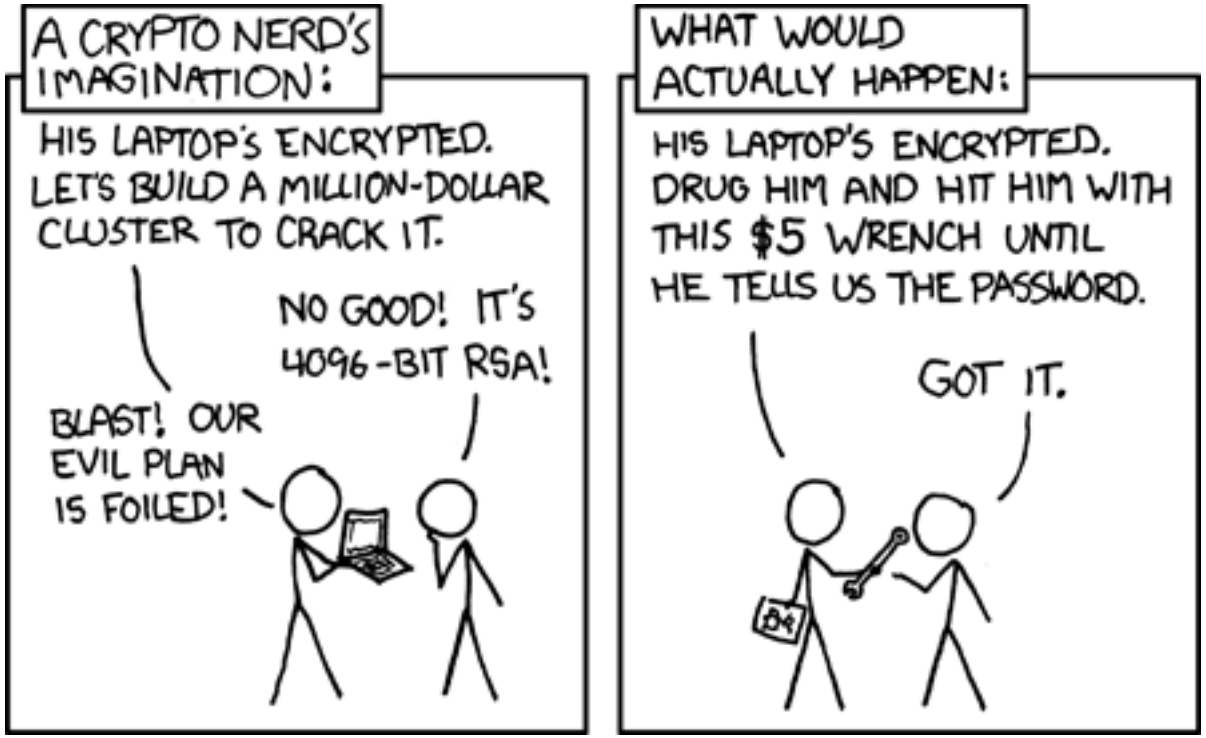
Password checker

- If a password is 8 characters long and each character has 256 options, there are
  - 256^8 = 18,446,744,073,709,551,616 possibilities
- Attacker must guess on average 9 quintillion times
- Right?
- Actually, we can time how long it takes to return a value
  - Try each each character for each digit.
- Now attacker has
  - 256 * 8 = 2048 possibilities

A Bank

Let's try it! Goals, assets, adversaries, threats, risks

xkcd



http://xkcd.com/538/

http://www.realuser.com/index.htm