CSEP 564
Computer Security and Privacy

Fall 2022

David Kohlbrenner
dkohlbre@cs

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, David Kohlbrenner, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Hello ☺

Instructor:

David Kohlbrenner (he/him)

dkohlbre.com

TA:

Michael Flanders (he/him)

Course Plan

- Lectures in-person
  - Lectures will have some form of break (vote!)
  - Lectures are recorded (please attend live!)
    - Recordings include student speech and will not be shared outside the class
  - Lectures are livestreamed via YouTube
  - Access all links via Canvas
- Office Hours will be *remote*
  - On Zoom, via Canvas
  - Not recorded
- Labs and readings; **no exams**

Discussion

- **Everyone** in this class **deserves** to be in this class
- We are **all** coming to this course with **different backgrounds** and experiences
- There are **no bad questions**; never belittle a questioner or their question; always be supportive
- Instructors / staff aren't always aware of everything, so **please call our attention to things as needed**
  - E.g., someone might harm someone else with what they say without ever realizing that what they said is harmful; that harm still exists, regardless of whether there was an intent to harm

Course Resource Cheat Sheet

- **Classrooms:** Lectures
- **Zoom:** Office hours
- **Canvas:** Links to recordings, assignment submissions, grades
- **Course website:** Schedule, assignment details, readings, policies
- **Ed:** Discussion board
- **Email:** Reach course staff privately

Who has taken a “Computer Security” course before?

What Does “Computer Security” Mean to You?

I can’t Zoom breakout anymore.

Talk to your neighbors!

Try putting some answers in https://pollev.com/dkohlbre

What are topics you are excited about?

- It is also okay if you don’t know what topics you are interested in yet!
- We can ask this question again at the end of the course, after you know more about different topics.

How Systems Fail

Systems may fail for many reasons, including:

- Reliability deals with accidental failures
- Usability deals with problems arising from operating mistakes made by users
- Design and goal oversights deals with the design process
- Security deals with intentional failures created by intelligent parties
  - But security, reliability, usability, and design/goals oversights are all related

Challenges: What is “Security”?

- What does security mean?
  - Often the hardest part of building a secure system is figuring out what security means (“threat modeling”)
  - Who are the **stakeholders** for which we are considering “security”?
  - What are the **assets** to protect?
  - What are the **threats** to those assets?
  - Who are the **adversaries**, and what are their **resources**?
  - What is the **security policy or goals**?
- **Perfect security does not exist!**
  - Security is not a binary property
  - Security is about risk management

Multiple assignments and activities are designed to exercise your thinking about these issues.

Privacy?

- Privacy often strongly overlaps security
- Privacy may also consider when systems *work as intended!*
- Not a hard-and-fast distinction
  - Privacy and security are generally intertwined

Lea Kissner 
@LeaKissner

I was just asked what the differences are between the fields of privacy, security, and health/trust&safety. Here's my best shot -- do you have better?

Security: our products/systems behave how they're supposed to, even in the presence of adversaries

10:37 AM · Sep 14, 2022 · Twitter for Android

Lea Kissner 
@LeaKissner

Privacy: our products/systems behave respectfully towards the people who use and are affected by them

T&S: users interact respectfully with each other through our products/systems

10:37 AM · Sep 14, 2022 · Twitter for Android

https://twitter.com/LeaKissner/status/1570104506477867008

Two Key Themes of this Course

1. How to **think** about security and privacy
   - The "Security Mindset" – a "new" way to think about systems

2. **Technical aspects** of security and privacy
   - Vulnerabilities and attack techniques
   - Defensive technologies
   - Topics including: software security, cryptography, malware, web security, web privacy, smartphone security, authentication, usable security, anonymity, physical security, security for emerging technologies, …

Theme 1: Security Mindset

- Thinking critically about designs, challenging assumptions
- Being curious, thinking like an attacker
- Exploring use cases not considered by the designers

"That new product sounds awesome, I can't wait to use it!"

versus

"That new product sounds cool, but I wonder what would happen if someone did Y with it; I wonder if the designers thought of Z…"

Why apply this mindset?

- Why it's important
  - Technology changes, so learning to think like a security person is more important than learning specifics of today's systems
  - Will help you design better systems/solutions
  - Interactions with broader context: law, policy, ethics, etc.

- Applies far beyond "just" computer security

Security Mindset Example

Security Mindset Example

And we’re done!

- Enjoy the rest of the quarter off

Learning the Security Mindset

- Several approaches for developing “The Security Mindset” and for exploring the broader contextual issues surrounding computer security
  - In class discussions and activities (e.g. The one later today!)
  - Participation in Ed discussion board (e.g., asking about news stories, technologies)

What This Course is Not About

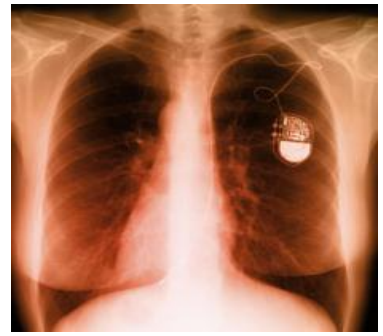
- Not a comprehensive course on computer security
  - Computer security is a broad discipline!
  - Impossible to cover everything in one quarter
  - So be careful in industry or wherever you go!
- Not about all of the latest and greatest attacks
  - Read news, ask questions, discuss on Ed
- Not a course on ethical, legal, or economic issues
  - We will touch on these issues, but the topic is huge
- Not a course on how to "break into" systems
  - Yes, we will learn about attacks ... but the ultimate goal is to develop an understanding of attacks so that you can build more secure systems

Security: Not Just for PCs

smartphones

voting machines

EEG headsets



medical devices

wearables

RFID

mobile sensing platforms

cars

game platforms

airplanes

Communication

- dkohlbre@cs.washington.edu
  - Use this if something is sensitive, personal, confidential, etc.

- Ed Discussion Board
  - Use this for the majority of assignment/etc. questions and discussion
    - Remember to mark private only if needed!
  - **Also will be used for announcements** (x-posted to email)

- We will do our best to be responsive, but **please be professional**, and plan ahead!

Course Materials

- Readings:
  - I'll be posting reading materials as we go
  - Feel like we're missing something? Let me know!
- Attend lectures
  - Lectures will not follow any textbooks
  - Lectures will focus on "big-picture" principles and ideas
- Attend sections (if you have questions about assignments, best to attend rather than watch later)
  - Details not covered in lecture, especially about homeworks and labs
  - More opportunity for discussion

Guest Lectures

- We may have a few guest lectures throughout the quarter
  - Useful to give you a different perspective: research, industry, government, legal

Course Logistics

Security is a contact sport!

- Labs (55% of the grade)
- Readings (35% of grade)
- Participation and in-class activities (10% of the grade)

Labs

- General plan:
  - "5" labs
    - Two are 2-parts of one lab
    - First lab out next week
    - Partnered or solo
  - Topics:
    - Software security (Buffer overflows, …)
    - Web security (XSS attacks, SQL injections, …)
    - Evaluating and patching vulnerabilities
  - Submit to Canvas

Ethics

- To learn to defend systems, you will learn to attack them. You should consider carefully how you use this knowledge.

In-Class Participation

- Trying to bring the best of online, in-person
  - In-class discussions, polls, and other online tools
  - More use of the online discussion board
  - Questions live and via pollev
- **Main component: Lightly graded in-class activities**
  - Specific pollev components will count
  - These will be labeled specifically
  - They are graded on effort/participation, not ‘correctness’

Late Submission Policy

- 3 free late days, no questions asked
  - Cumulative, throughout the quarter
  - Use up to 3 for one submission
  - If in a group, all members use days at once

- After that, late assignments will be dropped 20% per calendar day.
  - Late days will be rounded up
  - So an assignment turned in 26 hours late will be downgraded 40%

Discussion Board

- We've set up a Ed Discussion Board for this course
- Please use it to discuss the labs and other general class materials
- You can also use it to exercise the "security mindset"
  - Discussions of how movies get security right or wrong
  - Discussions of news articles about security (or not about security, but that miss important security-related things)
  - Discussions about security flaws you observe in the real world

Prerequisites (CSEP 564)

- Most of all: Eagerness to learn!
  - This is a graduate course
  - We expect you to push yourself to learn as much as possible.
  - We expect you to be a strong, independent learner capable of learning new concepts from the lectures, the readings, and on your own.
- We expect some familiarity with:
  - Basics of C programming
  - Very basic assembly
  - Basics of webpages/servers

Non-requisites

- Useful (not required): Computer Networks; Operating Systems
  - Will help provide deeper understanding of security mechanisms and where they fit in the big picture
- Useful (not required): Complexity Theory; Discrete Math; Algorithms
  - Will help with the more theoretical aspects of this course.
- Not useful (not required): …?

12 minute break, be back soon. (Prefer two breaks? We'll poll after class)

BREAK TIME

THREAT MODELING

Threat Modeling (Security Reviews)

- Assets: What are we trying to protect? How valuable are those assets?
- Adversaries: Who might try to attack, and why?
- Vulnerabilities: How might the system be weak?
- Threats: What actions might an adversary take to exploit vulnerabilities?
- Risk: How important are assets? How likely is exploit?
- Possible Defenses
- Not "traditional" threat modeling, but important (both in general, and to help better understand the system prior to threat modeling):
  - Benefits: Who might the system benefit, and how?
  - Harms: Who might the system harm, and how?

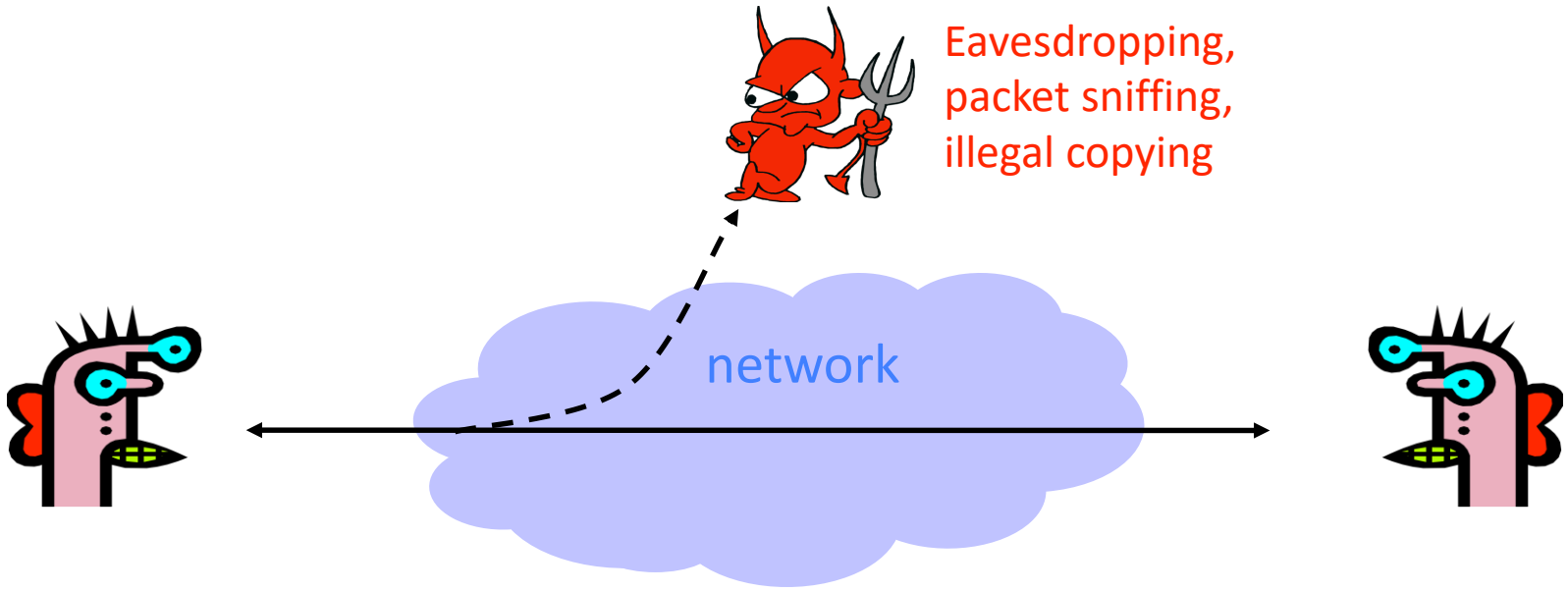
What's *Security*, Anyway?

- Common general security goals: "CIA"
  - Confidentiality
  - Integrity
  - Availability

- Or the extension: CPIAAU (Parkerian Hexad)
  - Control
  - Authenticity
  - Utility

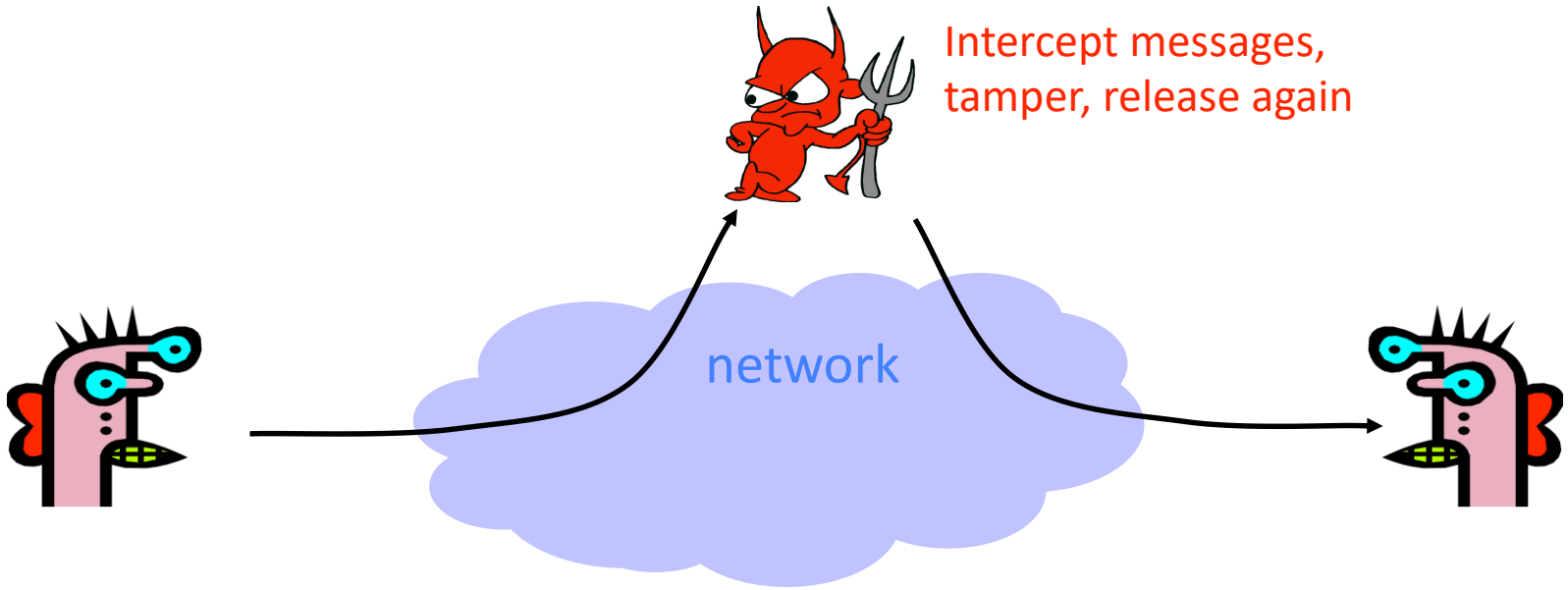
Confidentiality (Privacy)

- Confidentiality is concealment of information.



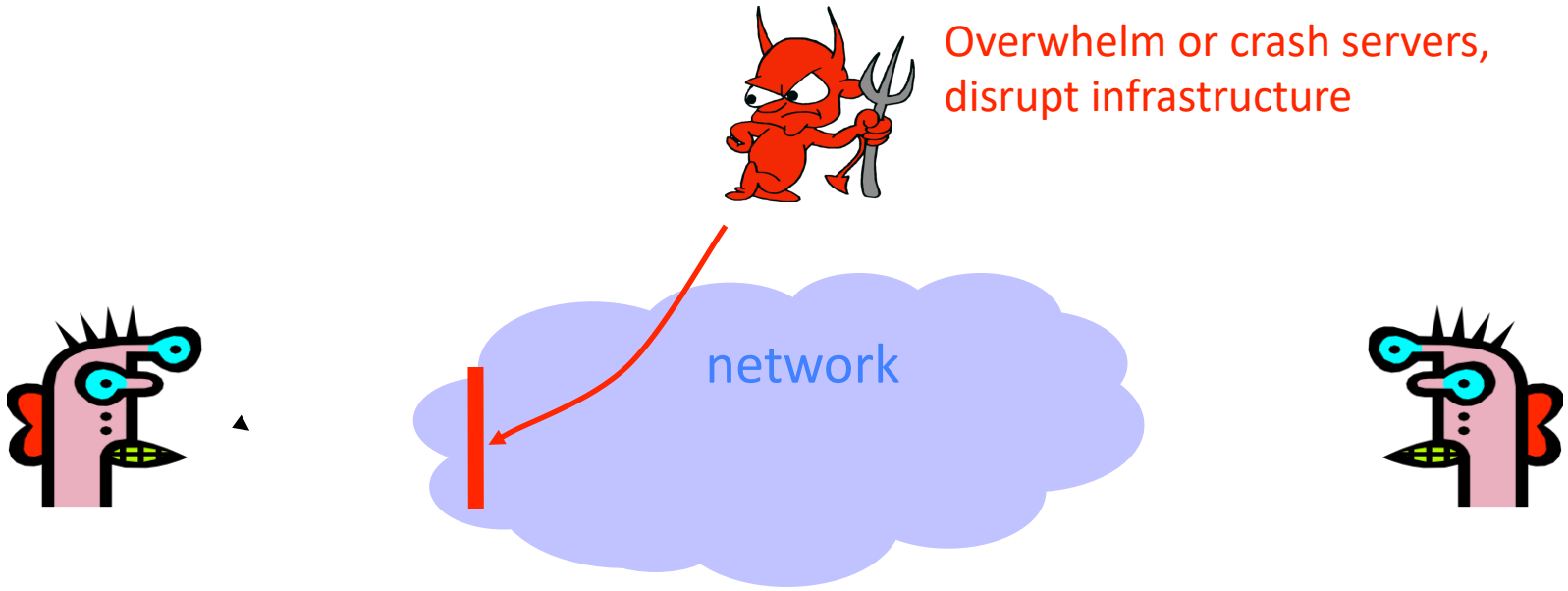
Integrity

- Integrity is prevention of unauthorized changes.



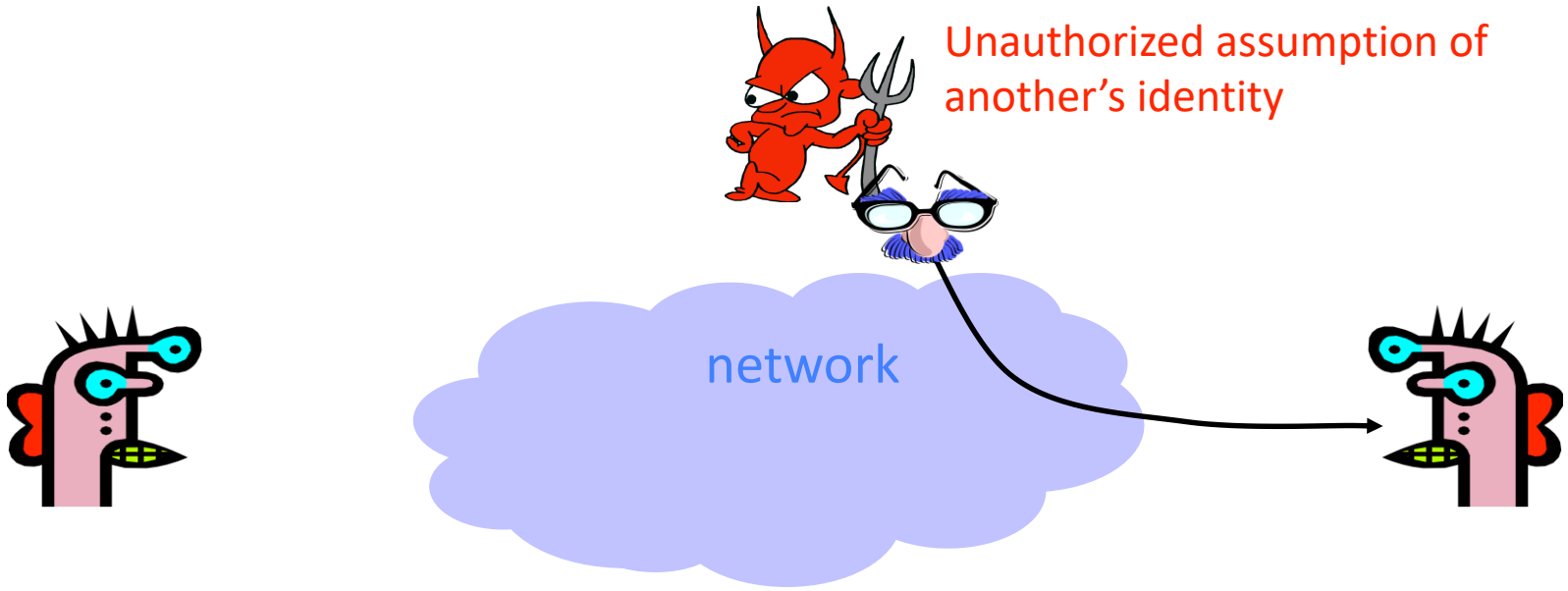
Availability

- Availability is ability to use information or resources.



Authenticity

- Authenticity is knowing who you're talking to.



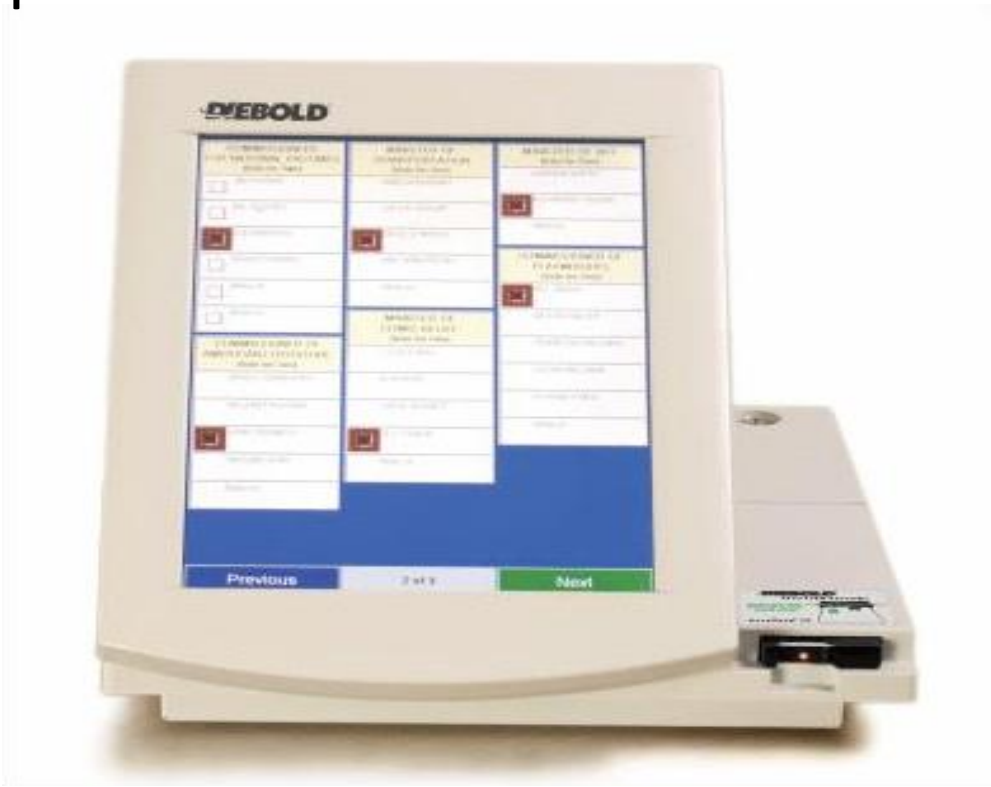
Threat Modeling

- There's no such thing as perfect security
  - But, attackers have limited resources
  - **Make them pay unacceptable costs / take on unacceptable risks to succeed!**

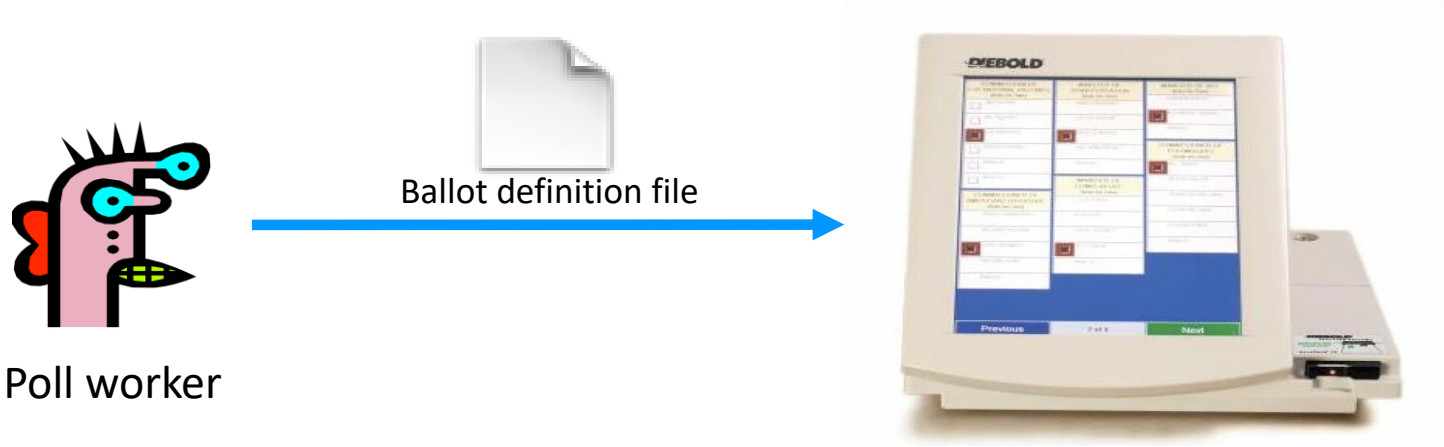
- Defining security per context: identify assets, adversaries, motivations, threats, vulnerabilities, risk, possible defenses

Threat Modeling Example: Electronic Voting

- Popular replacement to traditional paper ballots

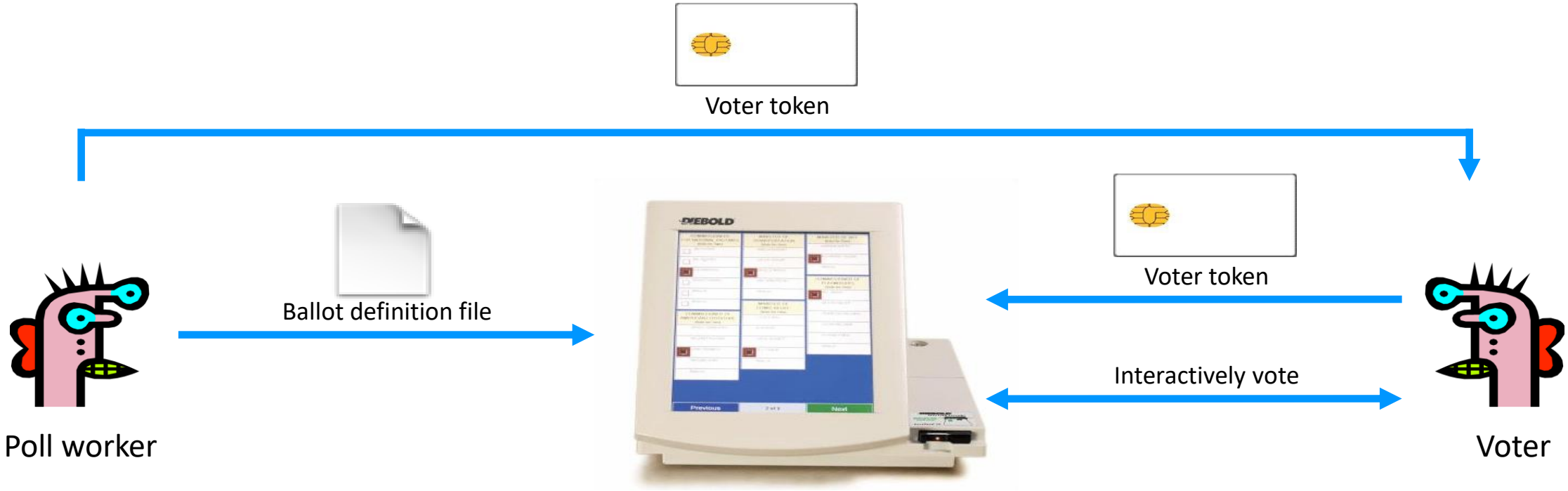


Pre-Election



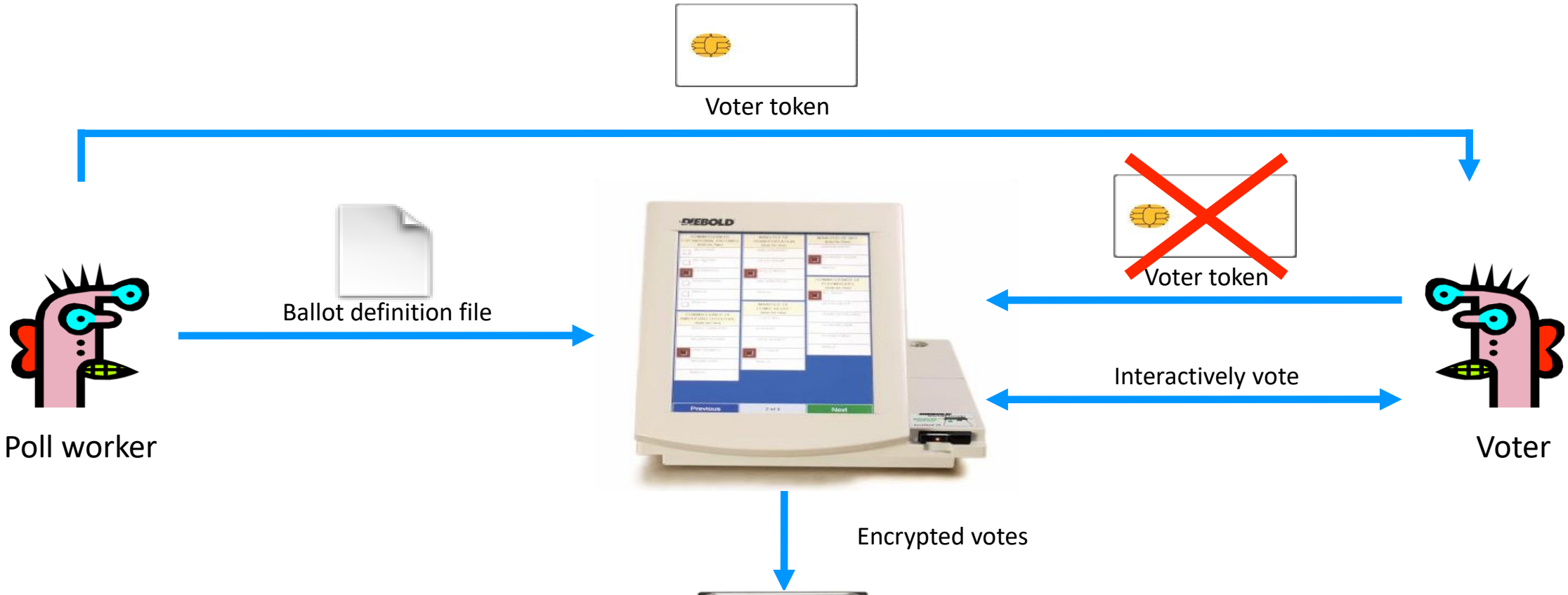
Pre-election: Poll workers load "ballot definition files" on voting machine.

Active Voting



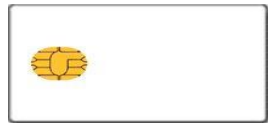
Active voting: Voters obtain single-use tokens from poll workers. Voters use tokens to activate machines and vote.

Active Voting



Active voting: Votes encrypted and stored.
Voter token canceled.

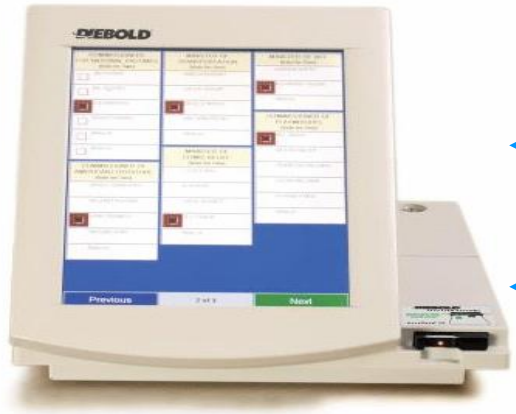
Post-Election



Voter token

Ballot definition file

Poll worker



Voter token

Voter

Interactively vote

Encrypted votes

Recorded votes

Tabulator

Post-election: Stored votes transported to tabulation center.

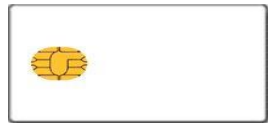
In-Class “Worksheet” Experiment

- Polleverywhere
- Fill out the questions while discussing with your breakout group
  - Everyone should submit their own
  - **No need for polish or complete sentences** – jot things down as you would on a piece of paper while chatting in class

Security and E-Voting (Simplified)

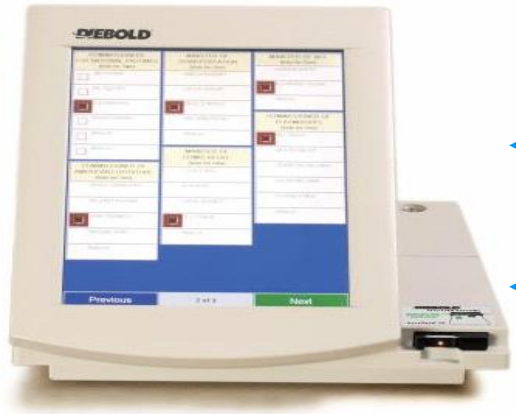
- Functionality goals:
  - Easy to use, reduce mistakes/confusion, make voting more accessible
- Security goals:

Can You Spot Any Potential Issues?



Voter token

Ballot definition file



Voter token

Interactively vote

Poll worker

Voter

Encrypted votes

Recorded votes

Tabulator

Q1: Security goals? Assets?
Q2: Adversaries? Attack goals?

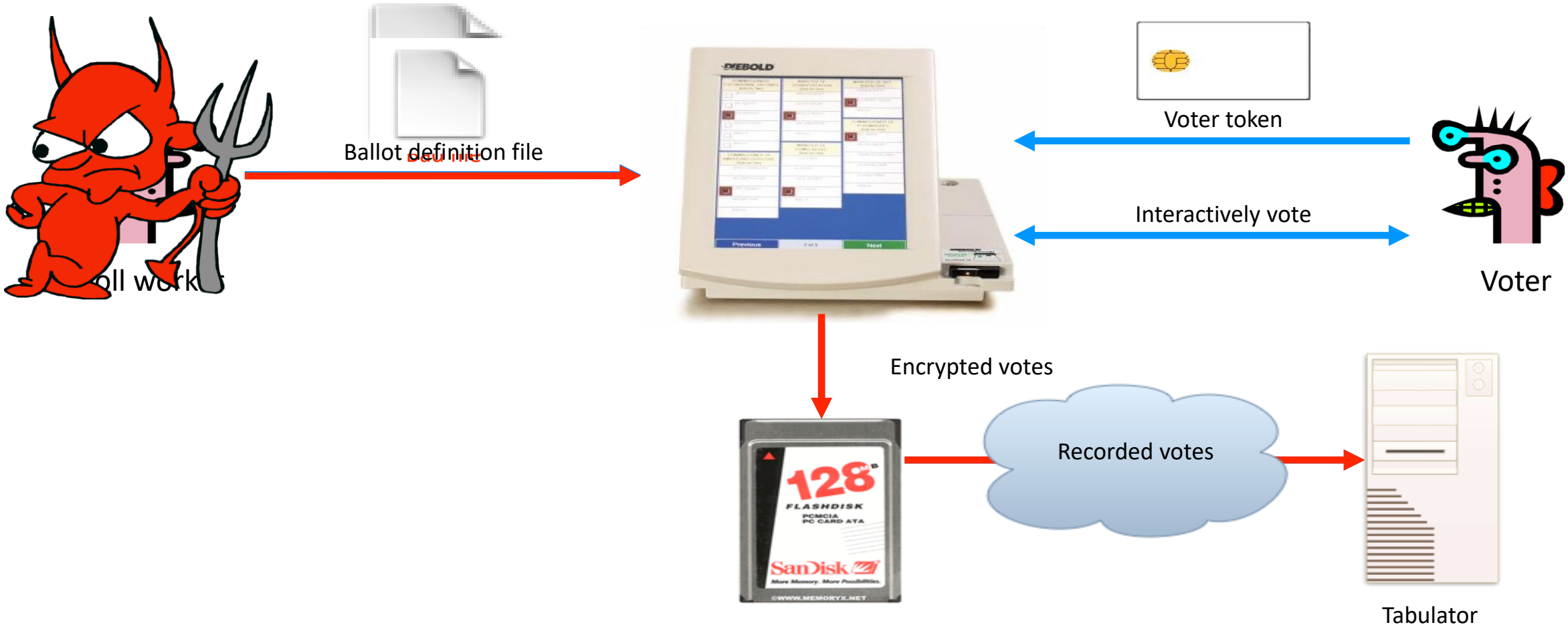
What Software is Running?

Problem: An adversary (e.g., a poll worker, software developer, or company representative) able to control the software or the underlying hardware could do whatever they wanted.


KEYS TO THE KINGDOM
Photo taken from Diebold's online store. The keys that open every Diebold touch-screen voting machine. Working copies have been made from the photo.

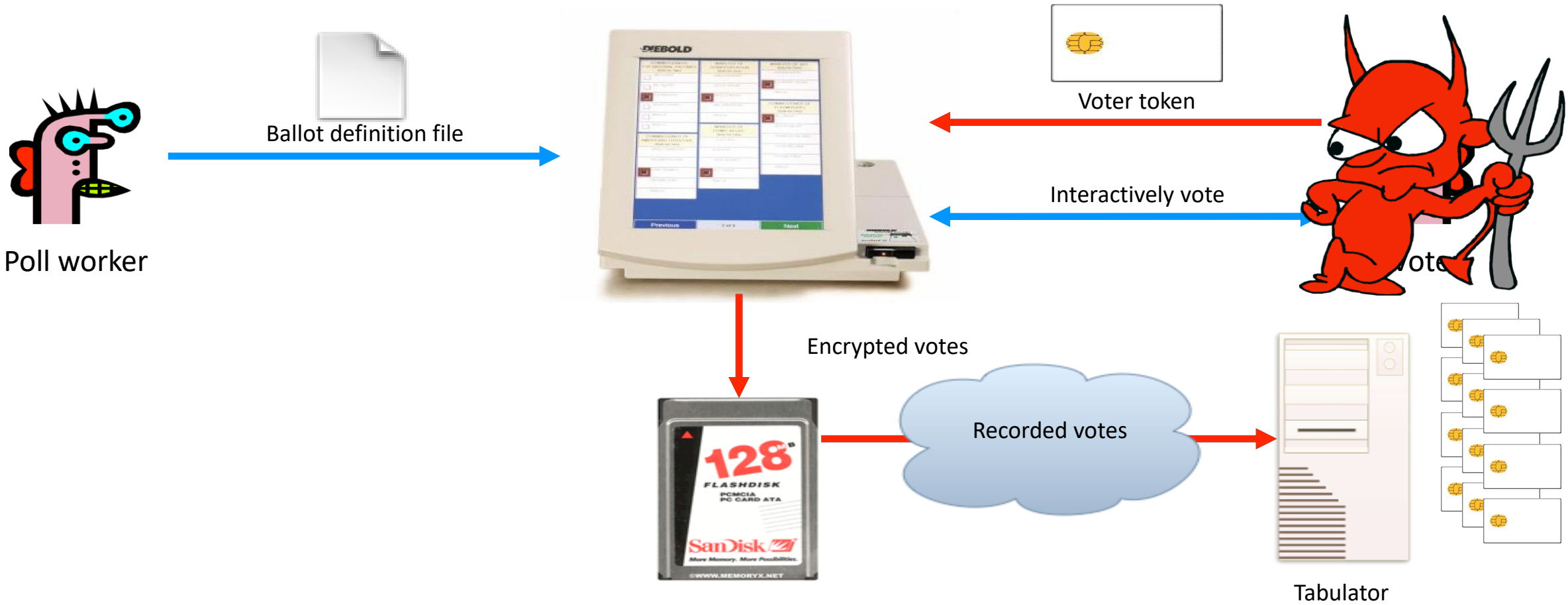
Problem: Ballot definition files are not authenticated.

Example attack: A malicious poll worker could modify ballot definition files so that votes cast for "Mickey Mouse" are recorded for "Donald Duck."



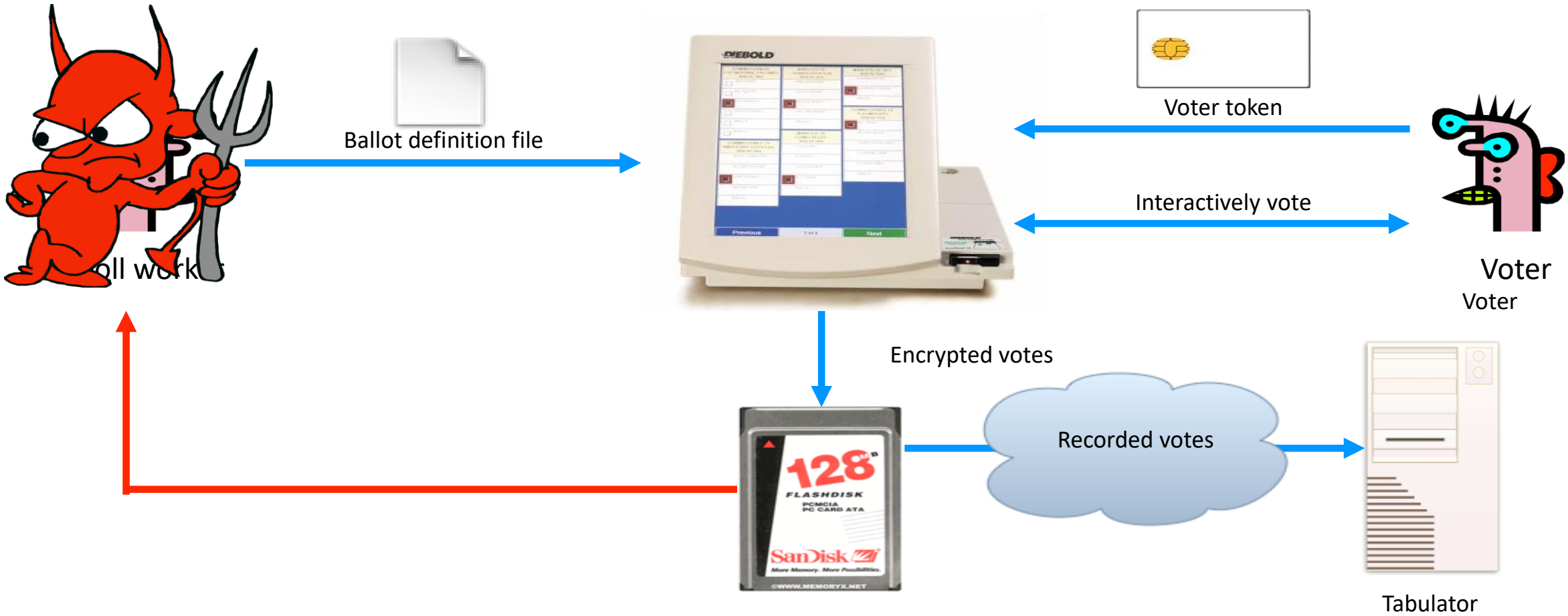
Problem: Smartcards can perform cryptographic operations. But there is no authentication from voter token to terminal.

Example attack: A regular voter could make their own voter token and vote multiple times.



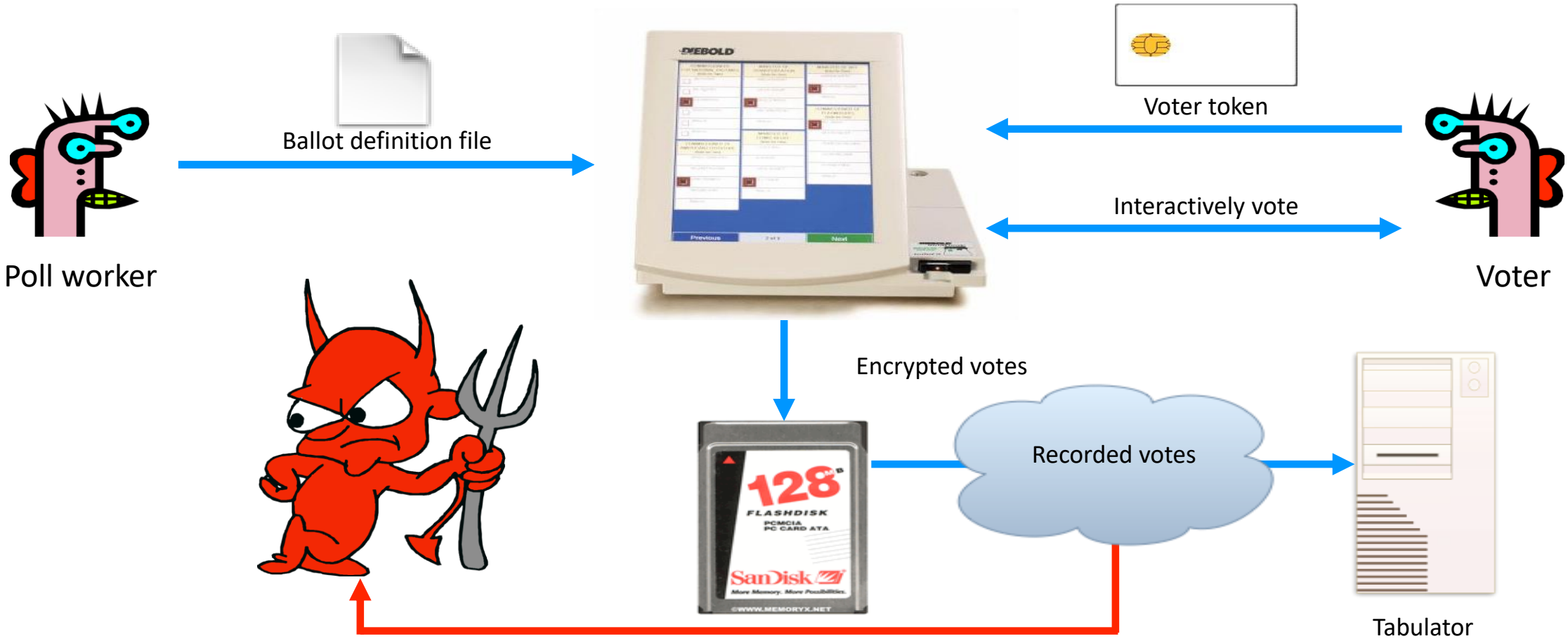
Problem: Encryption key ("F2654hD4") hard-coded into the software since (at least) 1998. Votes stored in the order cast.

Example attack: A poll worker could determine how voters vote.



Problem: When votes transmitted to tabulator over the Internet or a dialup connection, they are decrypted first; the cleartext results are sent to the tabulator.

Example attack: A sophisticated outsider could determine how voters vote.



TOWARDS DEFENSES

Approaches to Security

- Prevention
  - Stop an attack
- Detection
  - Detect an ongoing or past attack
- Response and Resilience
  - Respond to / recover from attacks

- The threat of a response may be enough to deter some attackers

Whole System is Critical

- Securing a system involves a whole-system view
  - Cryptography
  - Implementation
  - People
  - Physical security
  - Everything in between

- This is because "security is only as strong as the weakest link," and security can fail in many places
  - No reason to attack the strongest part of a system if you can walk right around it.

Whole System is Critical

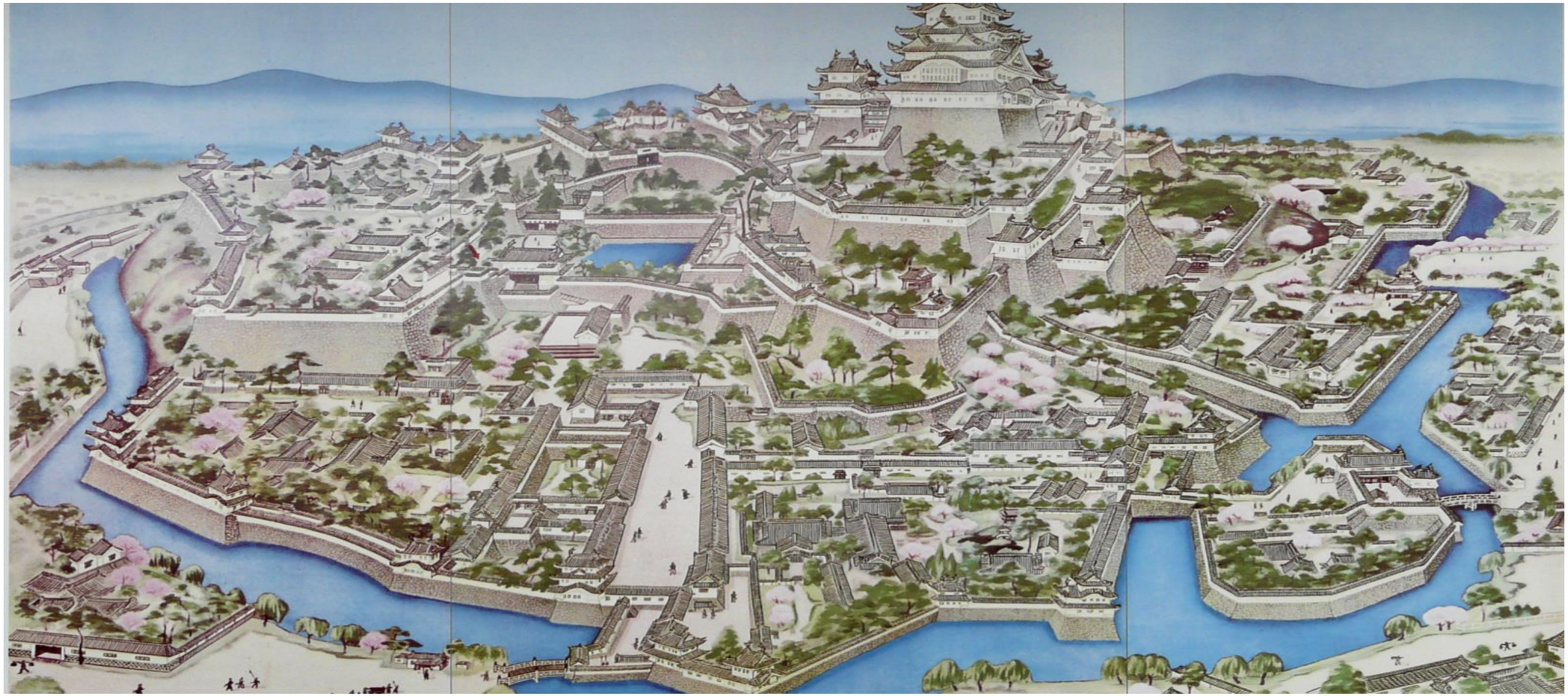
- Securing a system involves a whole-system view
  - Cryptography
  - Implementation
  - People
  - Physical security
  - Everything in between

- This is because "security is only as strong as the weakest link," and security can fail in many places
  - No reason to attack the strongest part of a system if you can walk right around it.

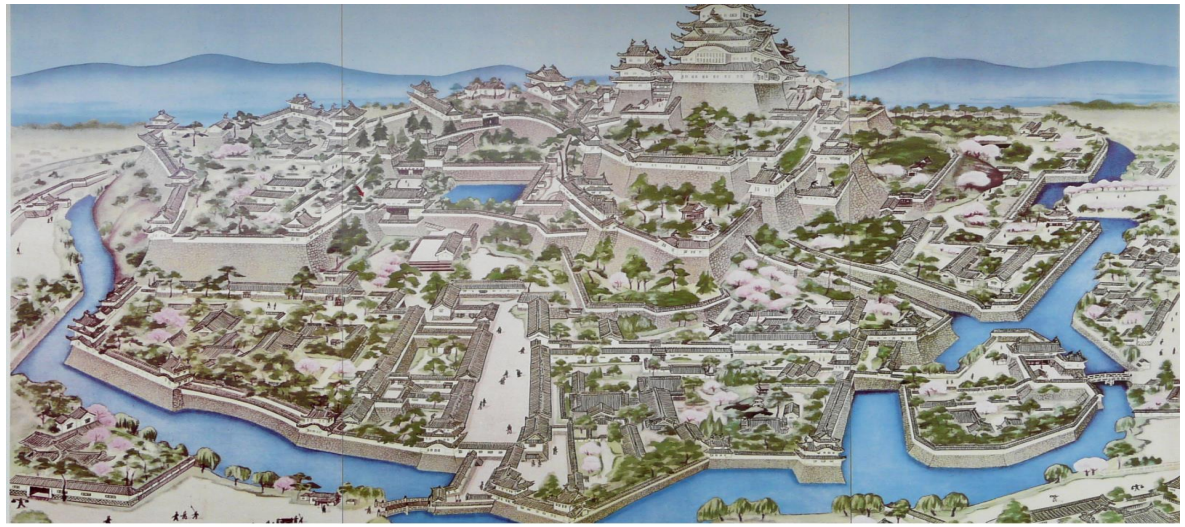
Whole System is Critical

Two viewpoints on “who has the advantage?”

Attacker's Asymmetric Advantage

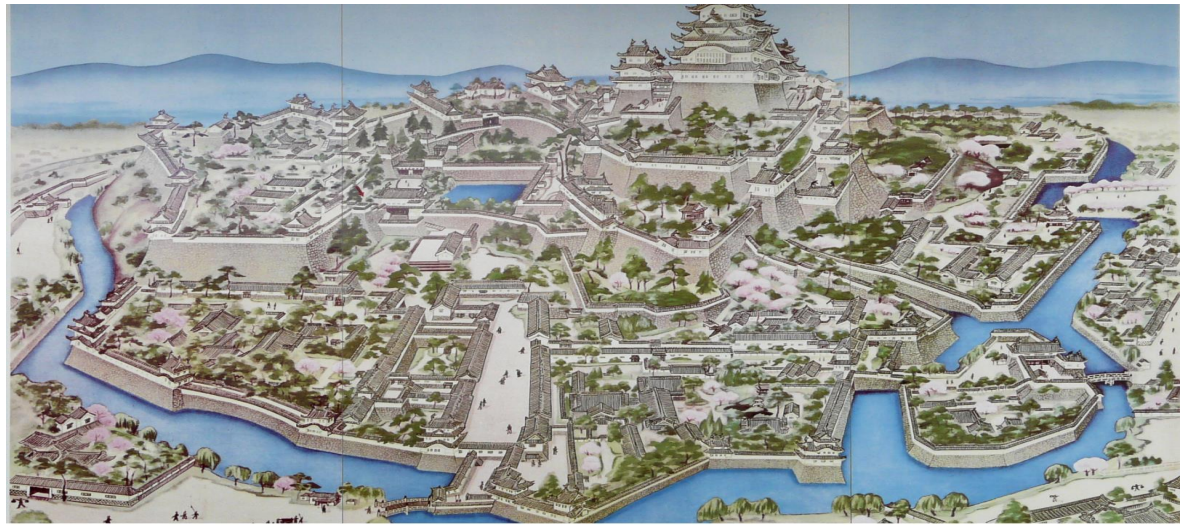


Attacker's Asymmetric Advantage



- Attacker only needs to win in one place
- Defender's response: Defense in depth

Defender's Asymmetric Advantage



- The attacker only succeeds while hidden
- If the defender can spot them one time, they win

From Policy to Implementation

- After you've figured out what security means to your application, there are still challenges:
  - Requirements bugs and oversights
    - Incorrect or problematic goals
  - Design bugs and oversights
    - Poor use of cryptography
    - Poor sources of randomness
    - …
  - Implementation bugs and oversights
    - Buffer overflow attacks
    - …
  - Is the system **usable**?

Many Participants

- Many parties involved
  - System developers
  - Companies deploying the system
  - The end users
  - The adversaries (possibly one of the above)
- Different parties have different goals
  - System developers and companies may wish to optimize cost
  - End users may desire security, privacy, and usability
    - Side question: Do system developers / companies really understand the needs and values of all their users? Or all stakeholders who might be impacted by the system?
  - But the relationship between these goals is quite complex (e.g., will customers choose features or security?)

Better News

- There are a lot of defense mechanisms
  - We'll study some, but by no means all, in this course
- It's important to understand their limitations
  - "If you think cryptography will solve your problem, then you don't understand cryptography… and you don't understand your problem" -- Bruce Schneier

To Do

- Do your weekly readings!
- Fill out this logistics poll!

Questions?

dkohlbre@cs

Ed discussion board