CSE 484 / CSE M 584: Computer Security and Privacy

Fall2016

Adam (Ada) Lerner
lerner@cs.washington.edu

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

Announcements

- CSE M 584 research readings are posted, with due dates. Get started, the first paper review is due October 7!

More Announcements

- Form groups of up to 3 and start working on your security reviews!

- Please write your student number on your worksheets, and **please write your last name VERY CLEARLY**. It helps us out **a lot** when recording them in the gradebook.

Answers to Questions from the Survey

- There is no written midterm or final exam

Answers to Questions from the Survey

- All the labs and the final project are for groups of 1-3. You may have the same group each time, or you may have different groups each time.
- Working alone is fine, though it may be challenging!

Answers to Questions from the Survey

- Hours per week will vary dramatically through the quarter – expect to work a lot on the labs, and somewhat less on other things.

Answers to Questions from the Survey

- I use
  they/them
  or
  she/her
  pronouns.

  Both are great. Thanks for asking!

Last Time

- "You won't believe what happens when you adopt this mindset! Engineers hate it!")
  - (challenging design assumptions, thinking like an attacker)

- #ClickbaitSyllabus
  - Post up to 2 on the forums for extra **credit** (and tweet @AdamRLerner, if you like)

Security Mindset Anecdote

- SmartWater?

- No, a liquid with a unique identifier, sold to mark your stuff as yours

Topics du Jour

- There is no perfect security
- The attacker's asymmetric advantage
- Confidentiality, Integrity, Authenticity
  - Side dish: Availability
- People are important
- Threat modeling

There is no perfect security

- "Security is not a binary property"

- But, attackers have limited resources
  - Make them pay unacceptable costs to succeed

There is no perfect security

- **Example:** Pharmaceutical spam is a business
  - They sell real (possibly unsafe) medications

- If operating costs > income, they can't profit and won't spam

There is no perfect security

- **Example:** CAPTCHAs

- CAPTCHA solving is a *service* you can pay for! Economics (labor availability, supply, demand) determine the price!

Approaches to Security

- Prevention
  - Stop an attack
- Detection
  - Detect an ongoing or past attack
- Response
  - Respond to attacks
- The threat of a response may be enough to deter some attackers

Attackers Need Motivation

- Adversarial motivations:
  - **Money**, fame, malice, revenge
  - Curiosity, politics, terror
  - International relations, war, convenience…

Whole System is Critical

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

Whole System is Critical

- Sec
  - C
  - I
  - P
  - P
  - E

Topics du Jour

- ~~There is no perfect security~~
- The attacker's asymmetric advantage
- Confidentiality, Integrity, Authenticity
  - Side dish: Availability
- People are important
- Threat modeling

The Attacker's Asymmetric Advantage

The Attacker's Asymmetric Advantage

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

Defense in Depth

- Answer Q1 on your worksheet.

Defense In Depth

- **Example:** Two-factor authentication
- **Example:** Account compromise defenses

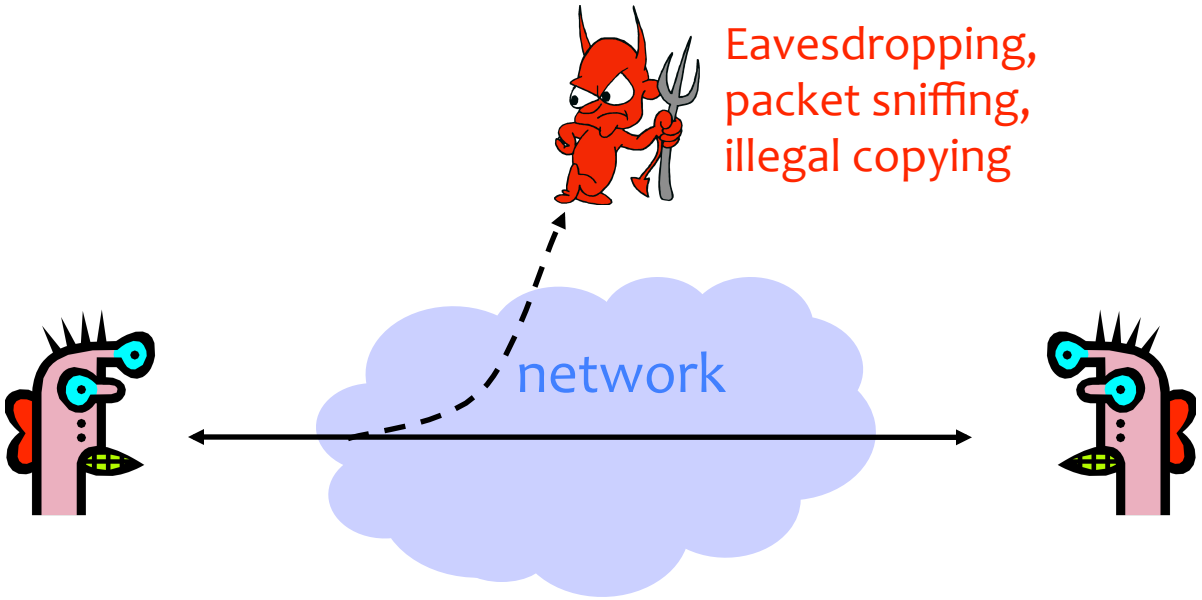
Topics du Jour

- ~~There is no perfect security~~
- ~~The attacker's asymmetric advantage~~
- Confidentiality, Integrity, Authenticity
  - Side dish: Availability
- People are important
- Threat modeling

Confidentiality (Privacy)

- **Confidentiality:**

  concealing information



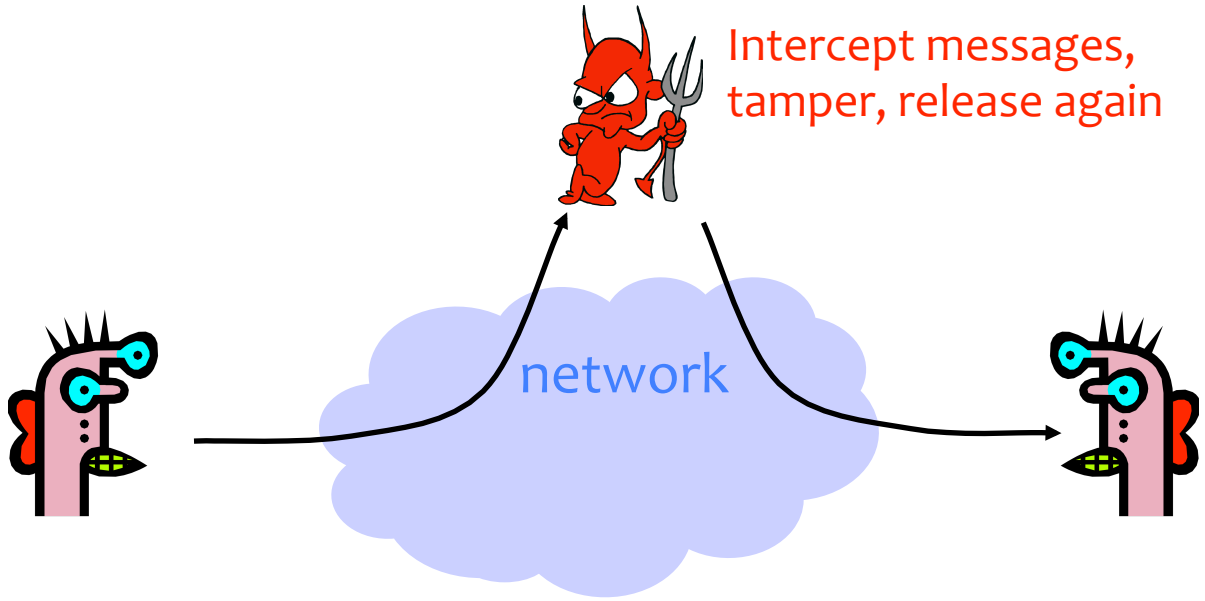
Confidentiality (Privacy)

- I send an email which is meant only for the class.
  - If someone outside the class can read it, they've violated the message's **confidentiality**.

- Many security goals rely on confidentiality. This is one reason security and privacy are so closely related.

Integrity

- **Integrity:**
  prevention of unauthorized changes



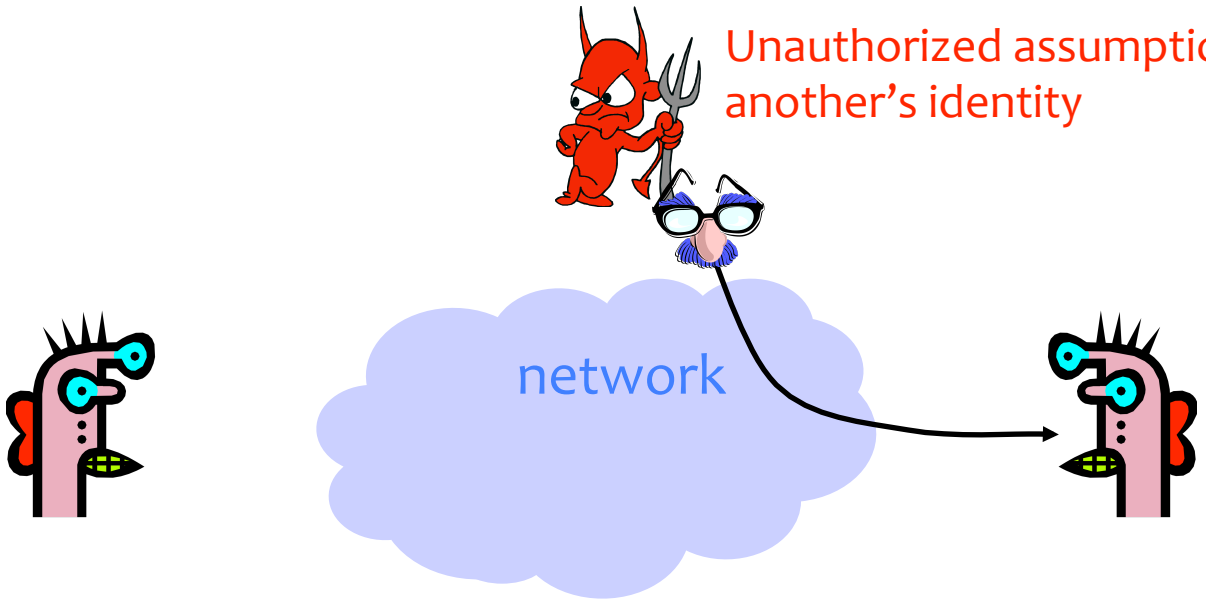
Integrity

- If someone can edit my email before it gets to the class, they've violated the message's integrity.

- Imagine taking whiteout to a postcard.

Authenticity

- **Authenticity:**
  knowing who you're talking to.

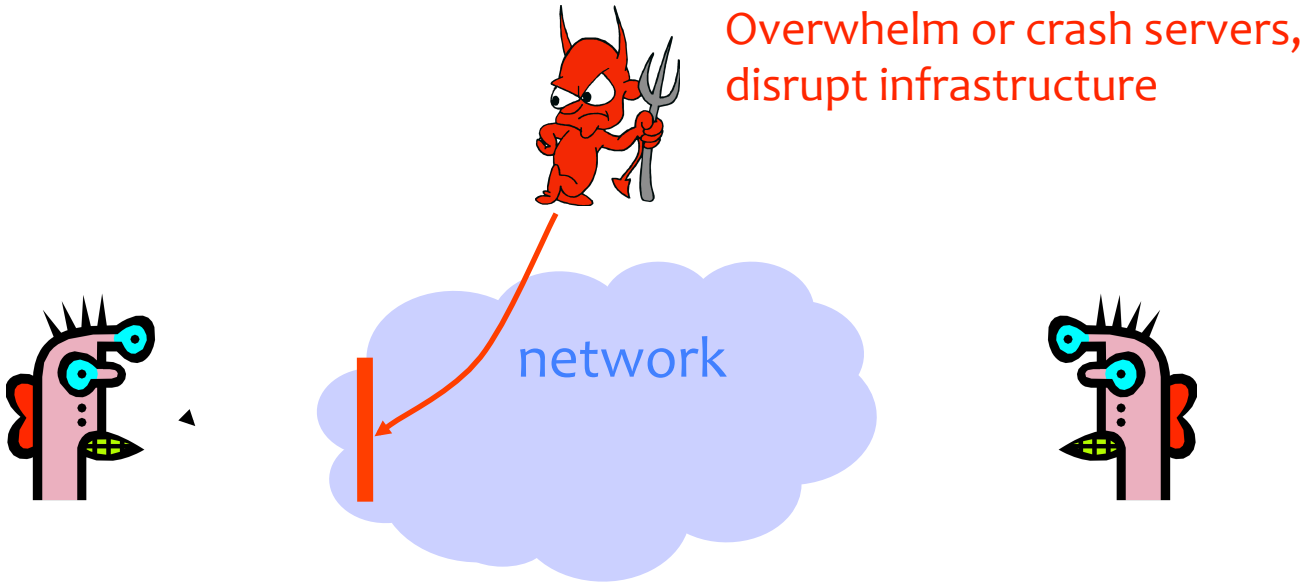


Authenticity

- If someone else can send email that appears to be from me, they've violated the authenticity of our email system.

Availability

- **Availability:**
  ability to use information or resources



Topics du Jour

- ~~There is no perfect security~~
- ~~The attacker's asymmetric advantage~~
- ~~Confidentiality, Integrity, Authenticity~~
  - ~~Side dish: Availability~~
- People are important
- Threat modeling

From Policy to Implementation

- Security problems can originate at all stages of a project:
  - Requirements/goals
    - Incorrect or problematic goals
  - Design bugs
    - Poor use of cryptography
    - Poor sources of randomness
    - …
  - Implementation bugs
    - Buffer overflow attacks
    - …
  - Usability bugs

Don't forget the users! They are a critical component!

People are important

- Many parties involved
  - System developers
  - Companies deploying the system
  - The end users
  - The adversaries (possibly one of the above)

People are Important

- Different parties have different goals
  - System developers and companies may wish to optimize cost
  - End users may desire security, privacy, and usability
  - But the relationship between these goals is quite complex (will customers choose not to buy the product if it is not secure?)

Topics du Jour

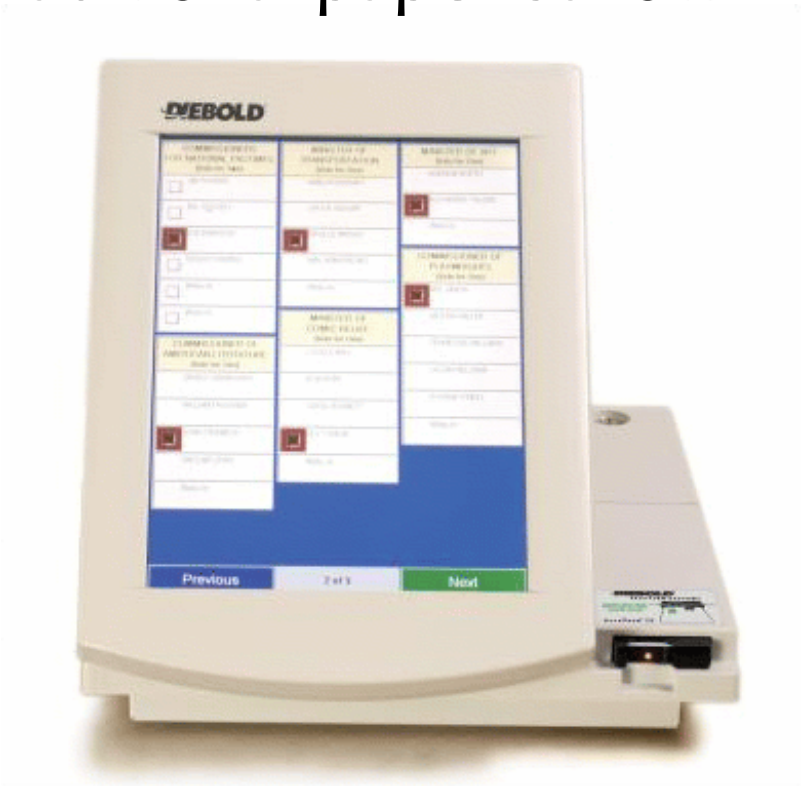
- ~~There is no perfect security~~
- ~~The attacker's asymmetric advantage~~
- ~~Confidentiality, Integrity, Authenticity~~
  - ~~Side dish: Availability~~
- ~~People are important~~
- Threat modeling

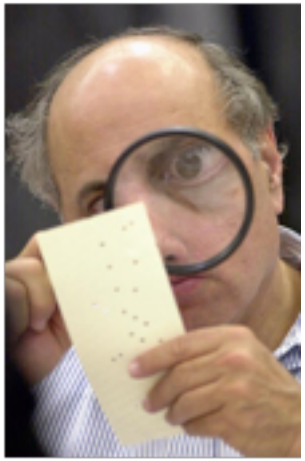
Threat Modeling

- 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

Example: Electronic Voting

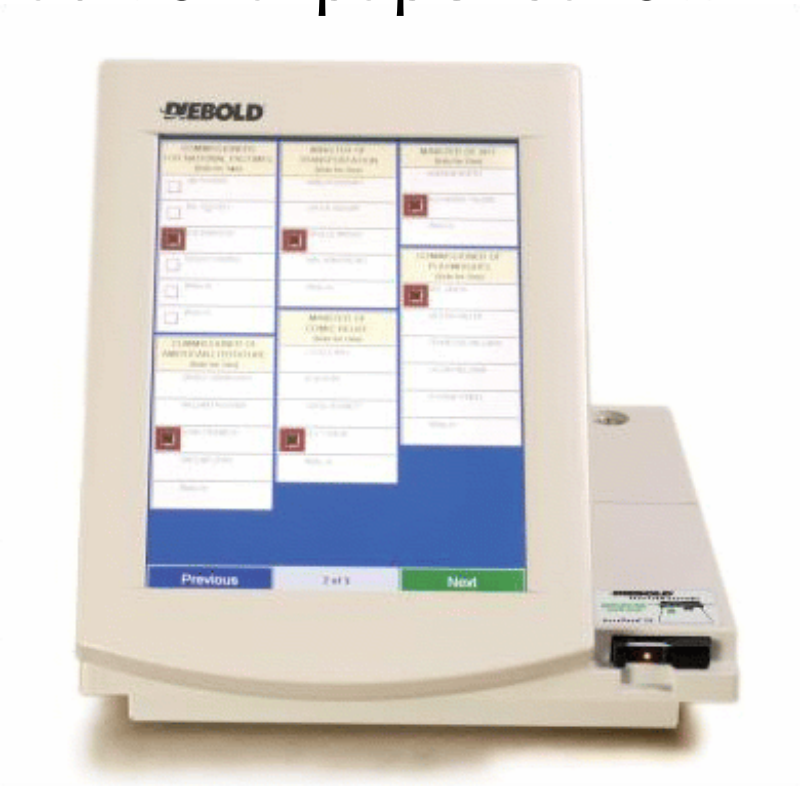
- Popular replacement to traditional paper ballots

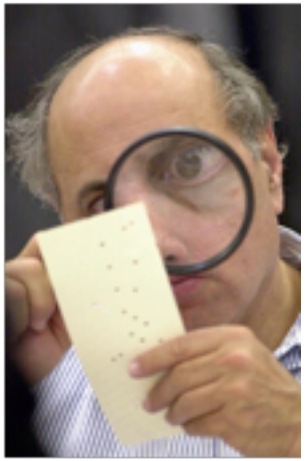




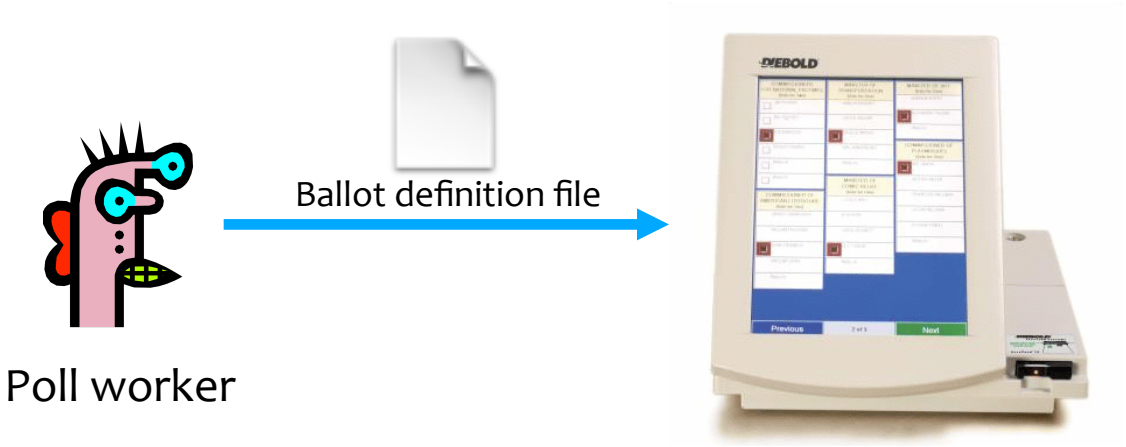
Electronic Voting: Answer Q2

- Popular replacement to traditional paper ballots



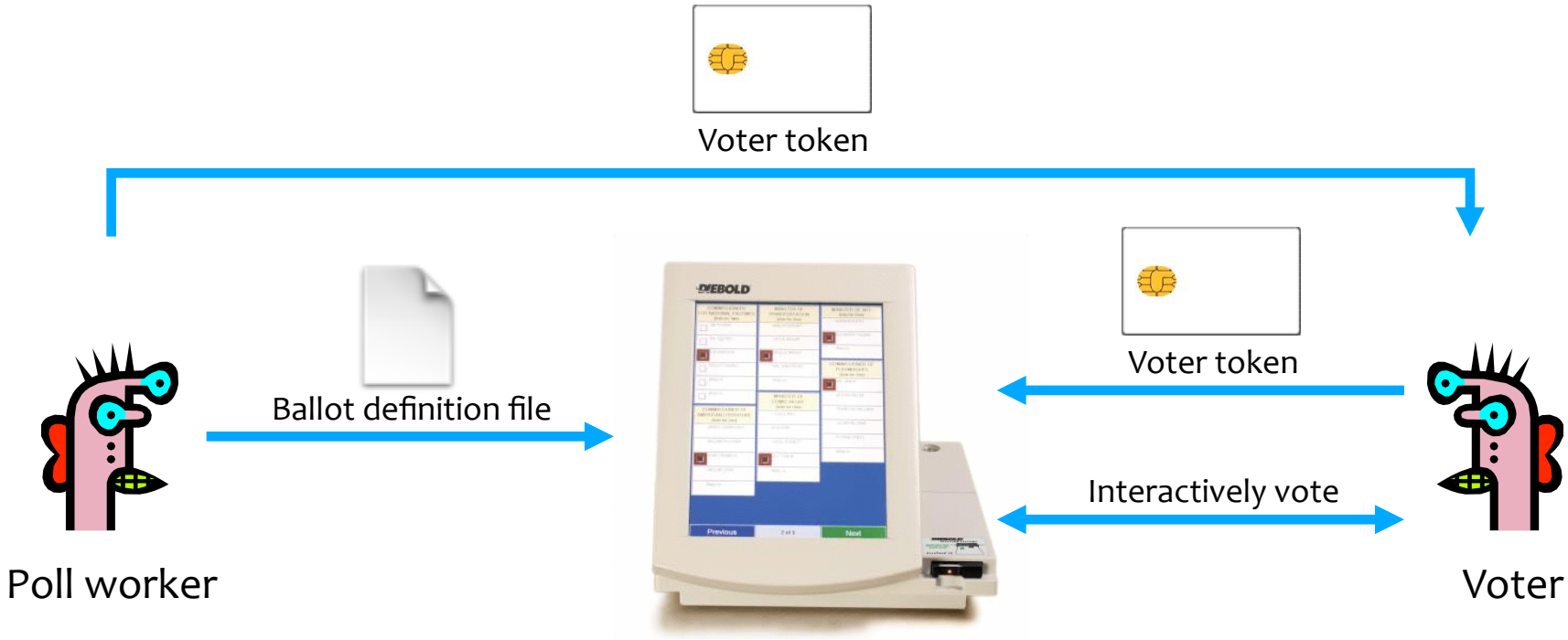


Pre-Election



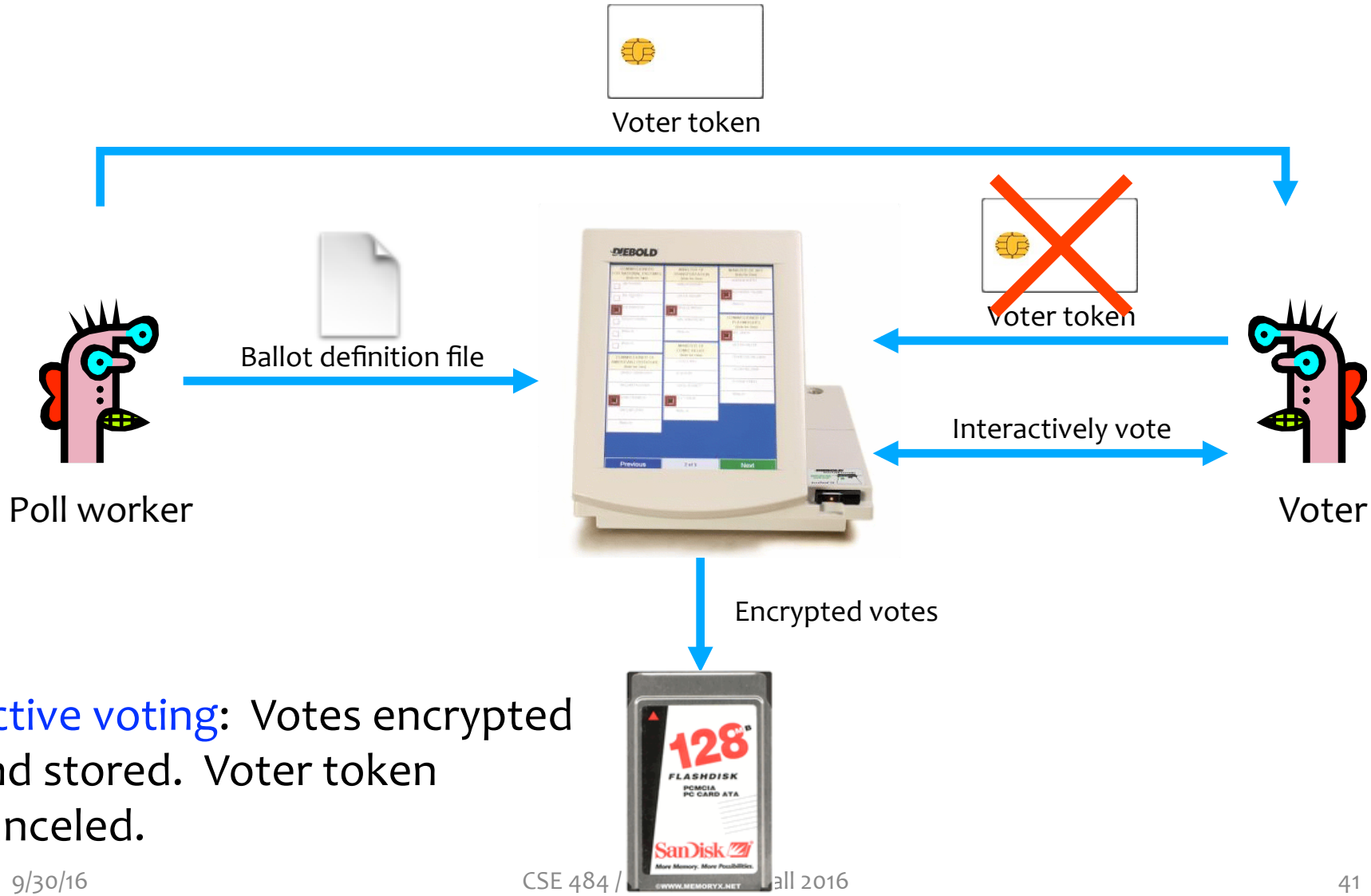
Pre-election: Poll workers load "ballot definition files" on voting machine.

Active Voting



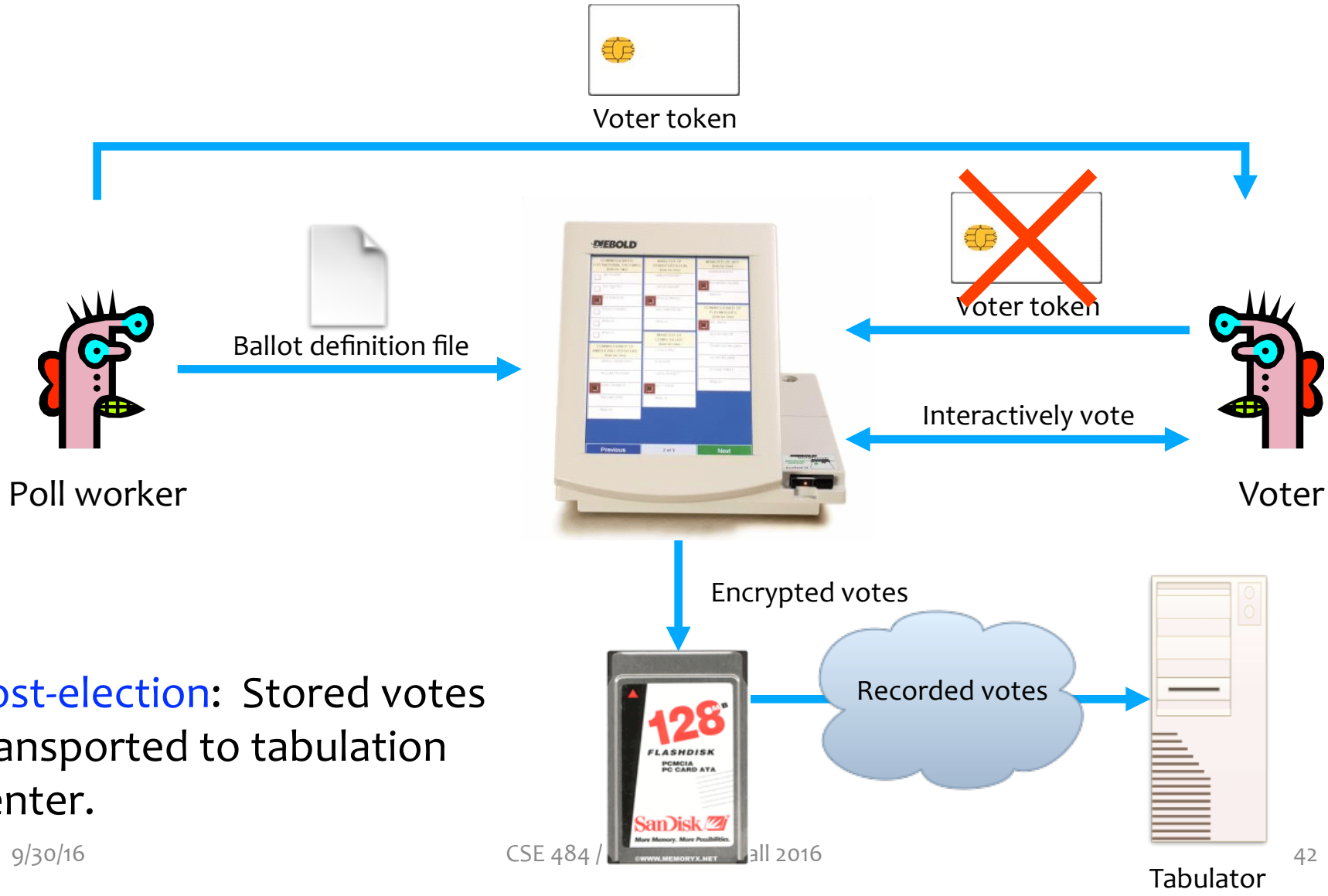
Active voting: Voters obtain single-use tokens from poll workers. Voters use tokens to activate machines and vote.

Active Voting



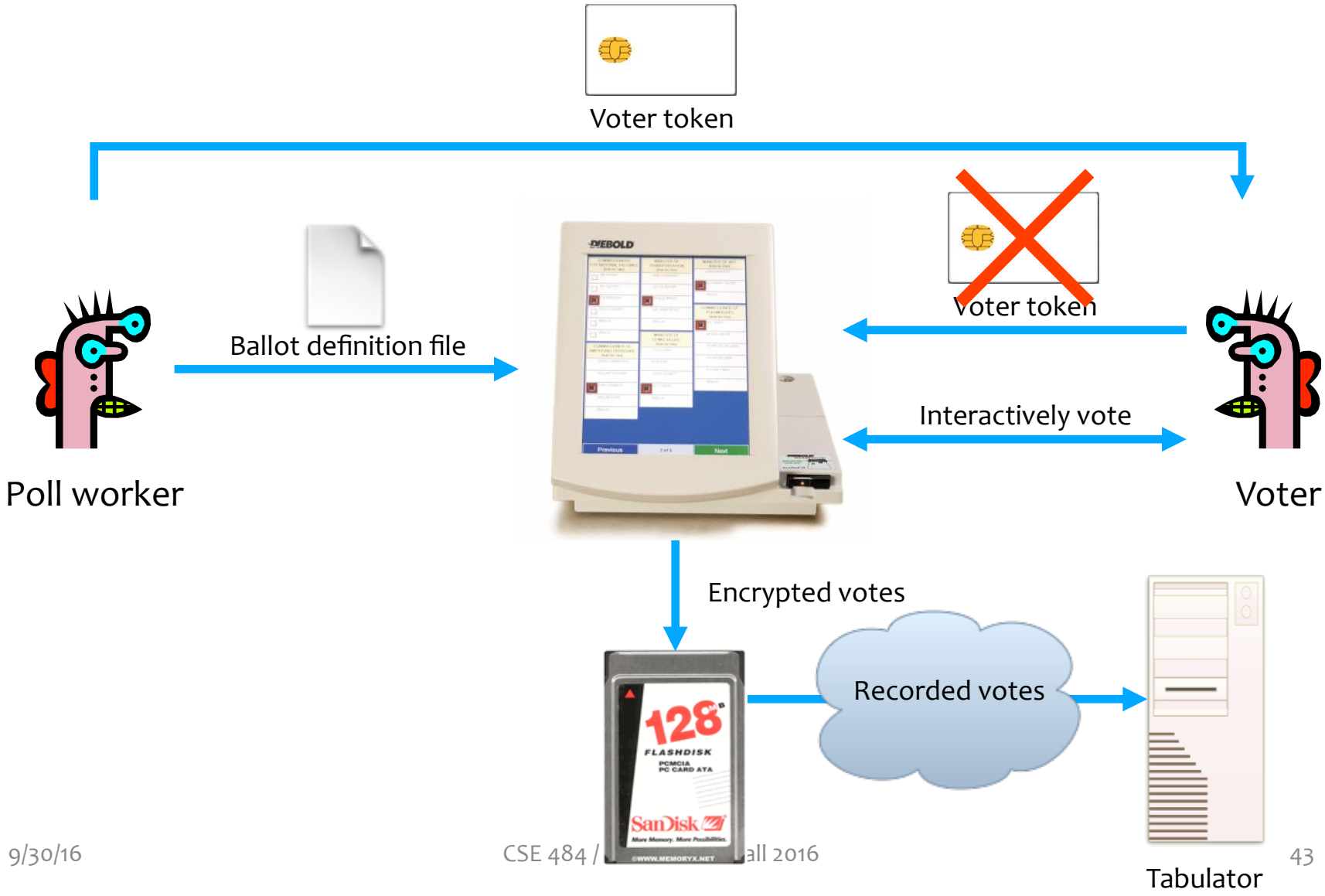
Active voting: Votes encrypted and stored. Voter token canceled.

Post-Election



Post-election: Stored votes transported to tabulation center.

Answer Q3


Voter token
Ballot definition file
Voter token
Interactively vote
Poll worker
Voter
Encrypted votes
Recorded votes
Tabulator

Security and E-Voting (Simplified)

- Functionality goals:
  - Easy to use, reduce mistakes/confusion
- Security goals:
  - Adversary should not be able to tamper with the election outcome
    - By changing votes (**integrity**)
    - By voting on behalf of someone (**authenticity**)
    - By denying voters the right to vote (**availability**)
  - Adversary should not be able to figure out how voters vote **(confidentiality)**

Potential Adversaries

- Voters
- Election officials
- Employees of voting machine manufacturer
  - Software/hardware engineers
  - Maintenance people
- Other engineers
  - Makers of hardware
  - Makers of underlying software or add-on components
  - Makers of compiler
- …
- Or any combination of the above

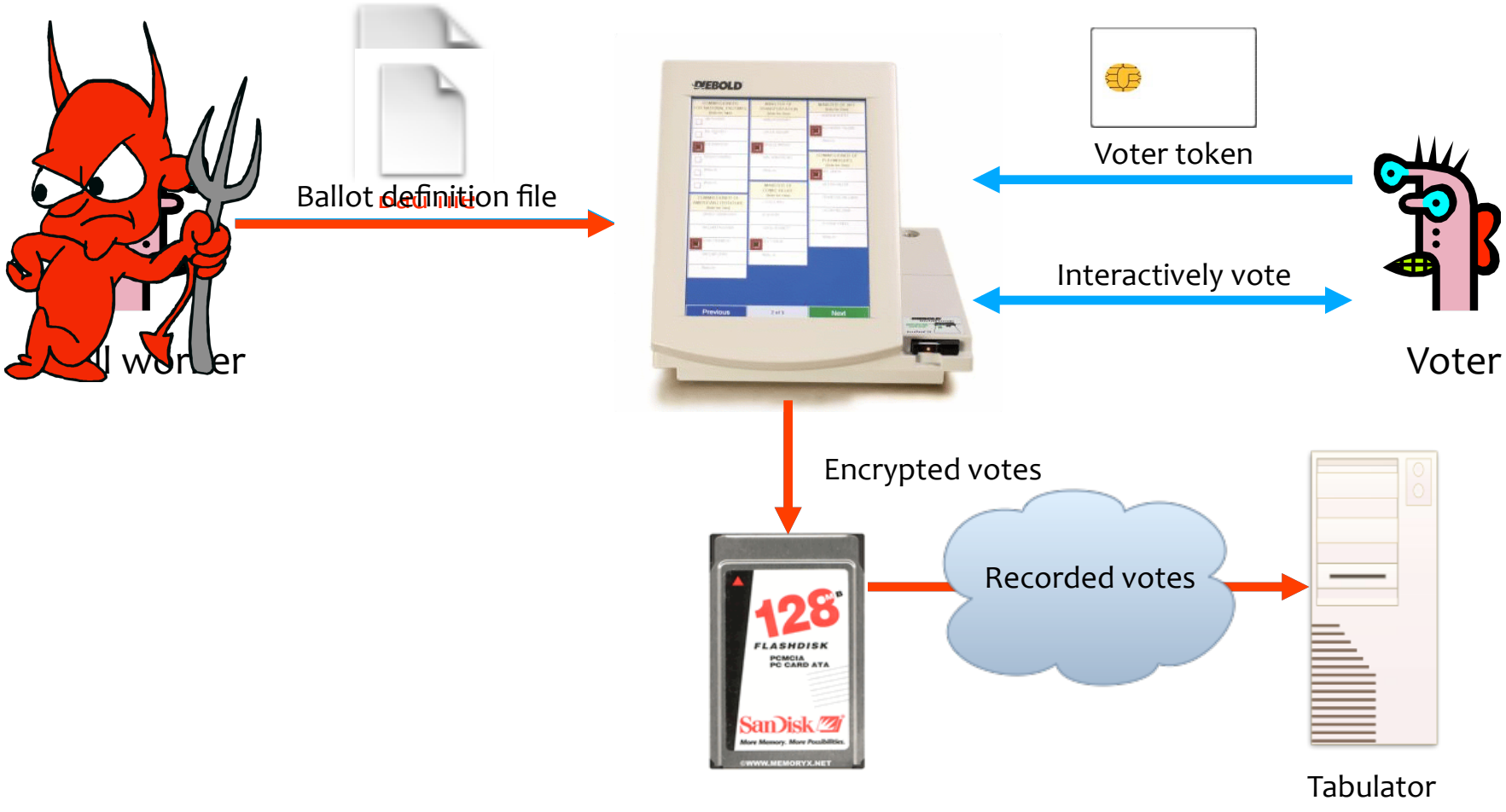
What Software is Running?

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 he or she 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.

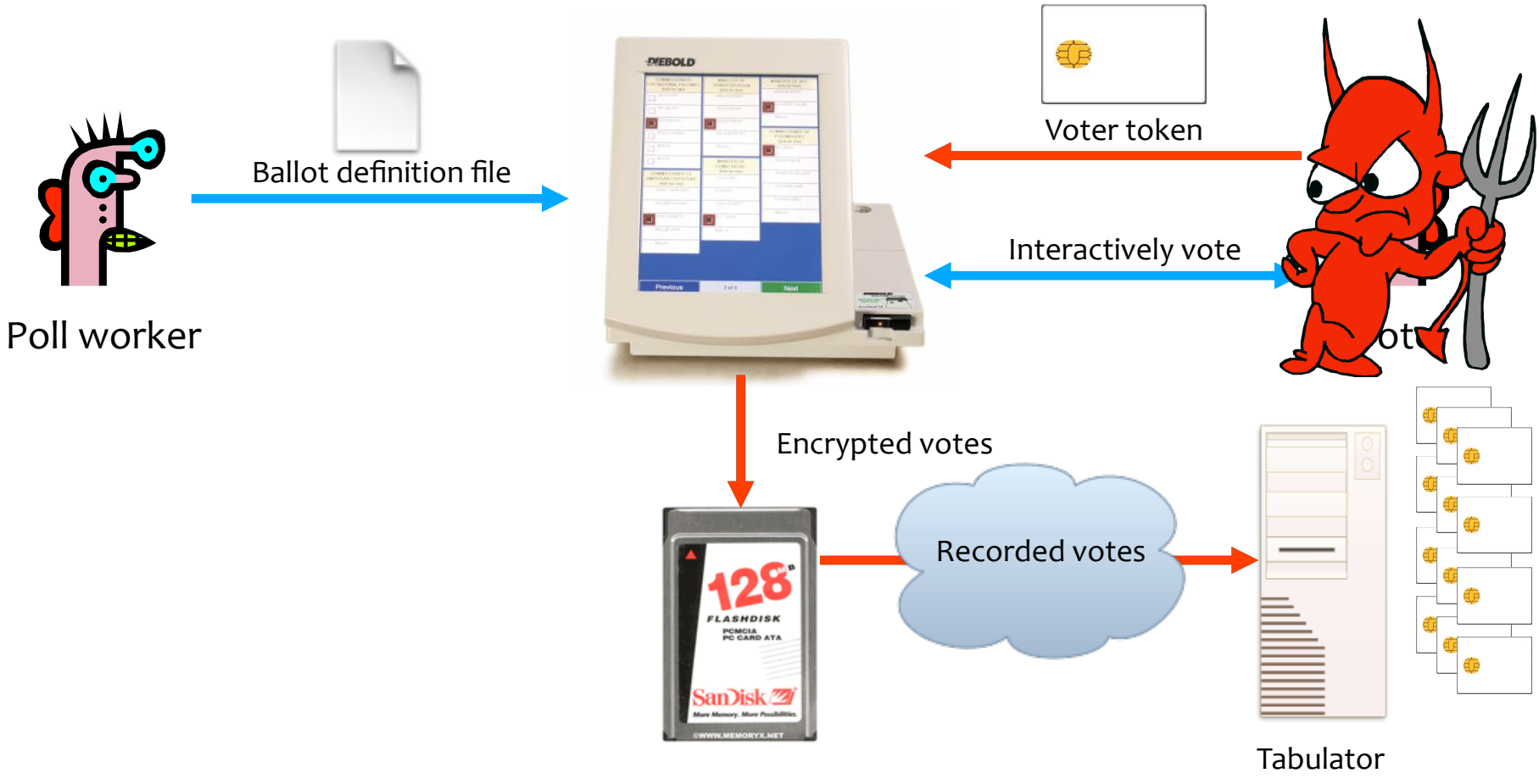
Problem: Ballot definition files are not authenticated.

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



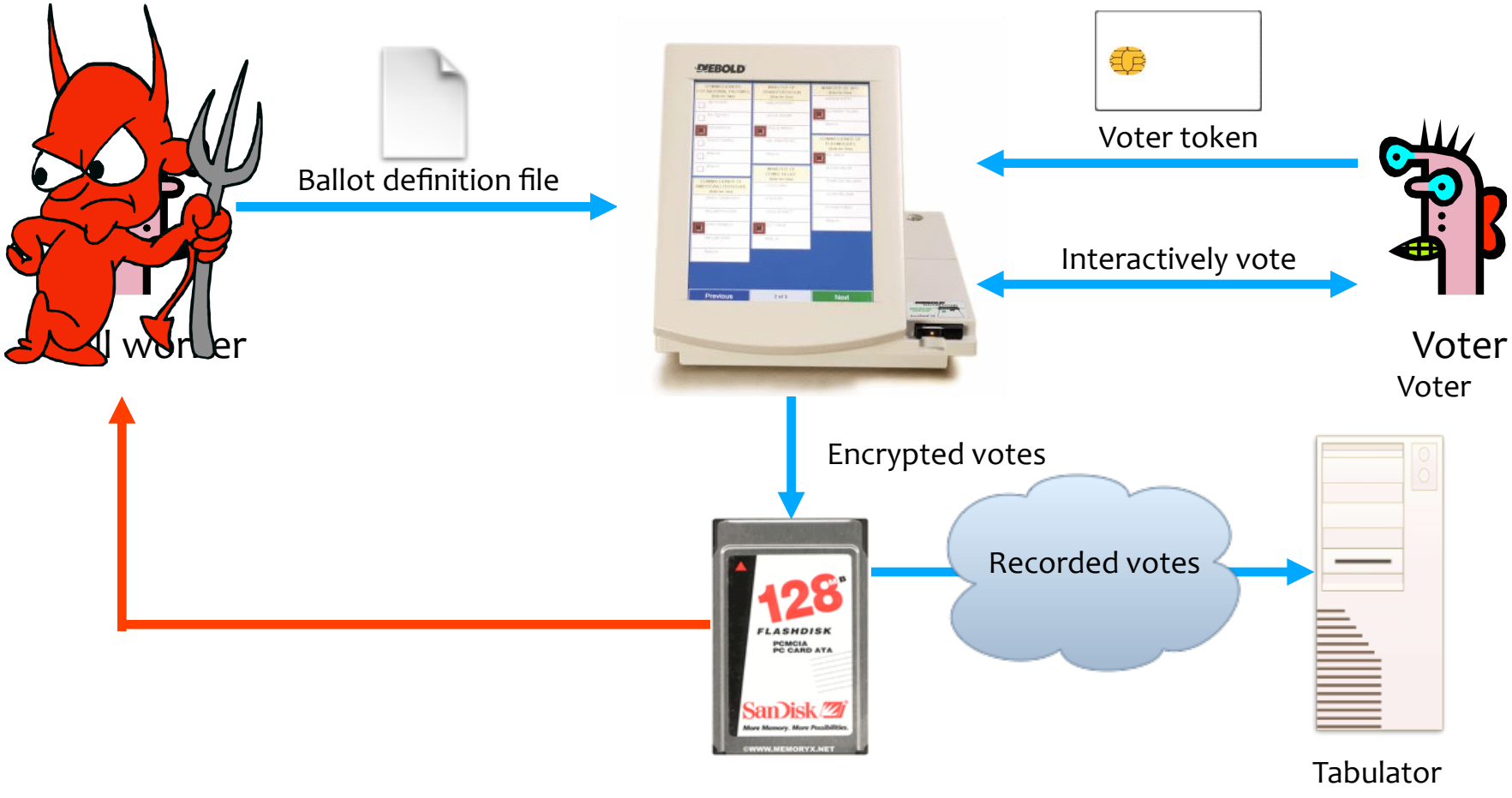
Problem: Smartcards can perform cryptographic operations. But there is no authentication from voter token to terminal.

Example attack: A regular voter could make his or her 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 the the tabulator.

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