CSE 484 / CSE M 584: Computer Security and Privacy

Autumn 2018

Tadayoshi (Yoshi) Kohno
yoshi@cs.washington.edu

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

Announcements / Answers

- If you're on the class mailing list, you should have received an email (about office hours this week).
- Ethics form: Due next Wednesday (10/3).
- Homework #1: Due next Friday (10/5) – start forming groups, feel free to use forum.

Announcements / Answers

- No quiz section on Thanksgiving Day
- No lecture on the Wednesday before Thanksgiving day: Video assignment instead

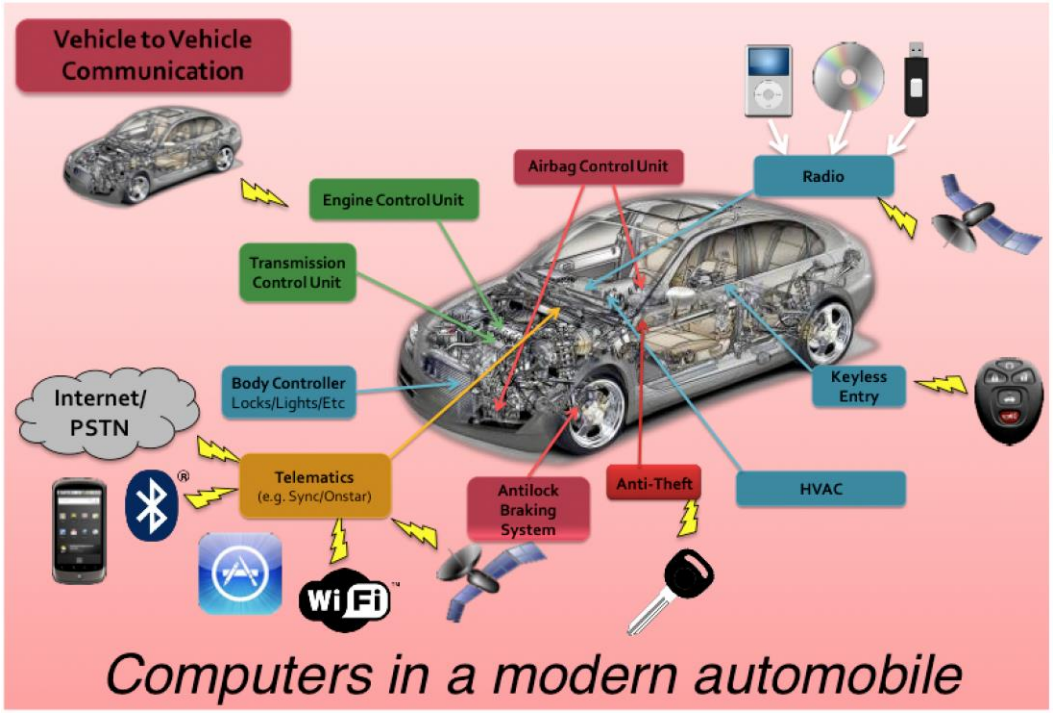
Last Time + Quiz Section

- Importance of the security mindset
  - Challenging design assumptions
  - Thinking like an attacker
- There's no such thing as perfect security
  - But, attackers have limited resources
  - **Make them pay unacceptable costs to succeed!**
- Defining security per context: identify assets, adversaries, motivations, threats, vulnerabilities, risk, possible defenses

Example: Modern Automobiles

Modern automobiles contain dozens of computers.

Those computers control nearly everything in the car, including locks, lights, brakes, the engine, the airbags, etc.



Who might want to attack? Why, and how?

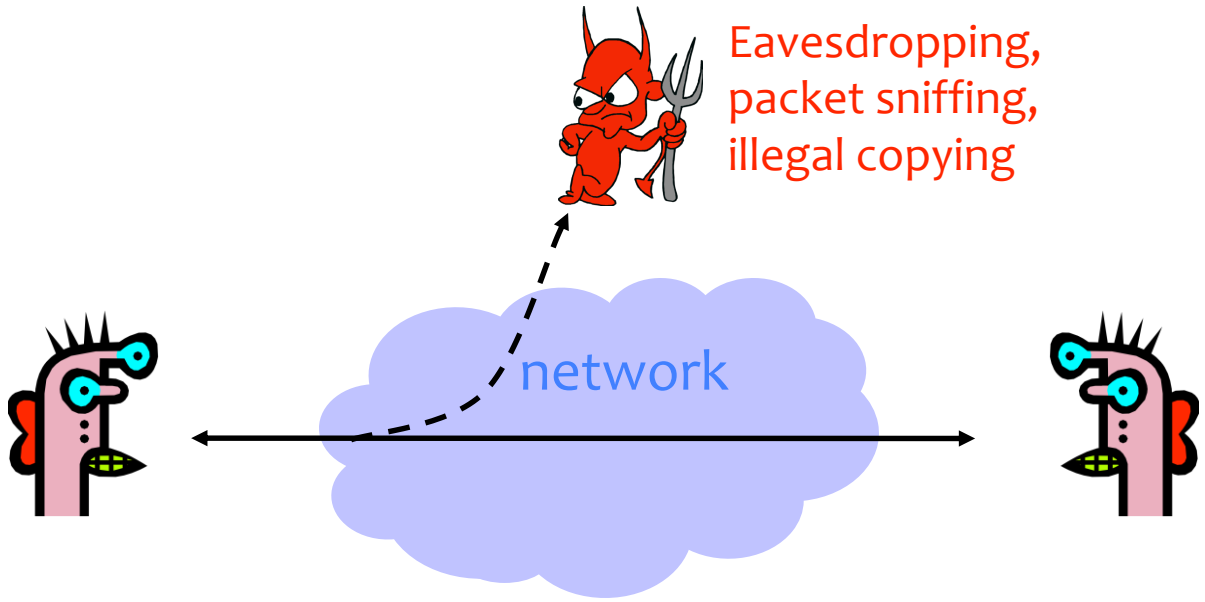
Practicing Security Mindset

- See worksheet, Q3

SECURITY GOALS ("CIA") (QUIZ SECTION AND TODAY)

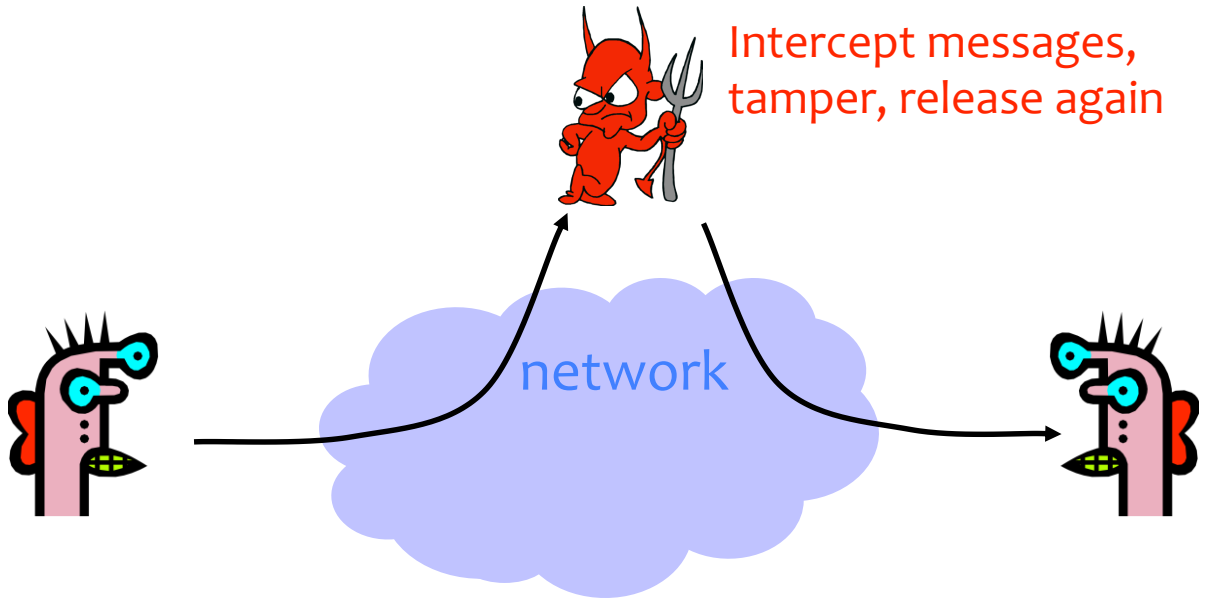
Confidentiality (Privacy)

- Confidentiality is concealment of information.



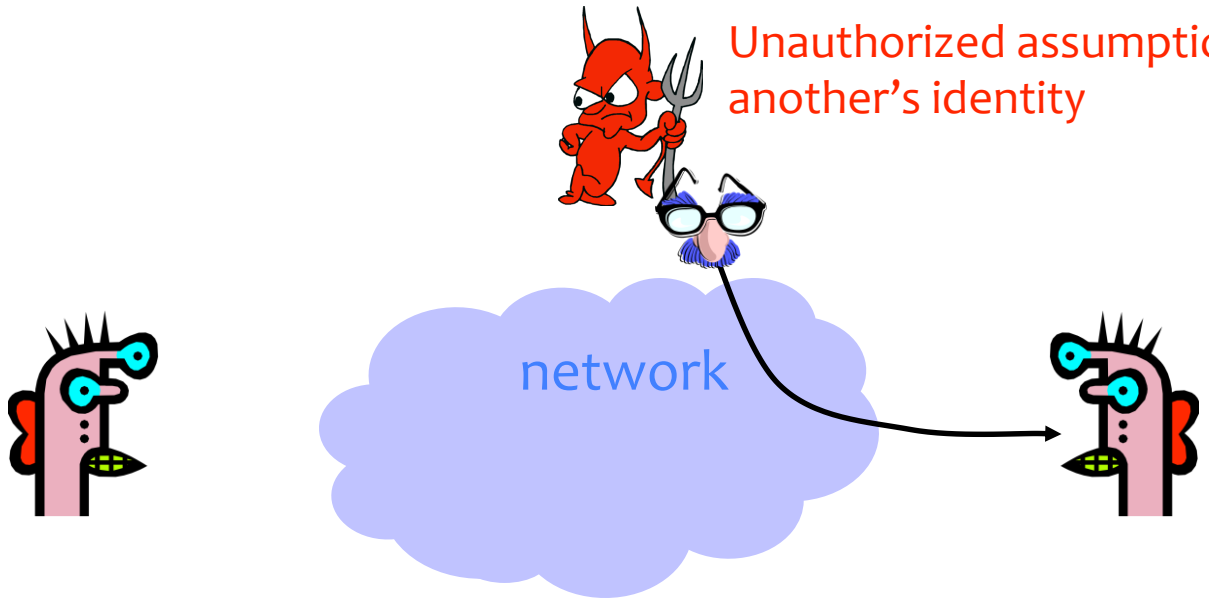
Integrity

- Integrity is prevention of unauthorized changes.



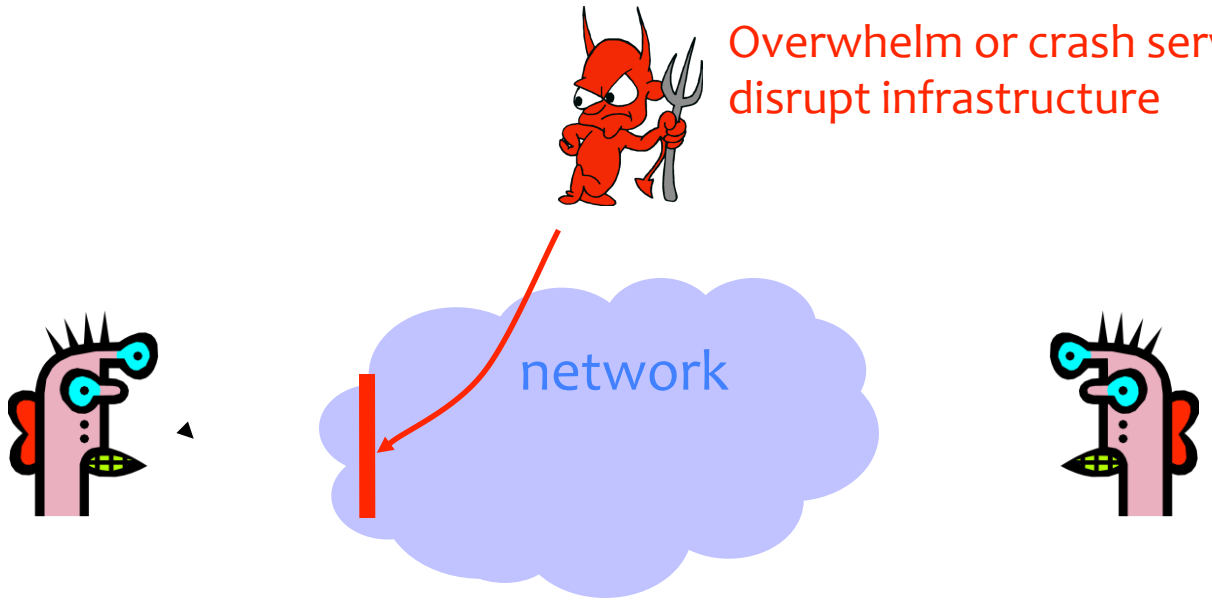
Authenticity

- Authenticity is knowing who you're talking to.



Availability

- Availability is ability to use information or resources.



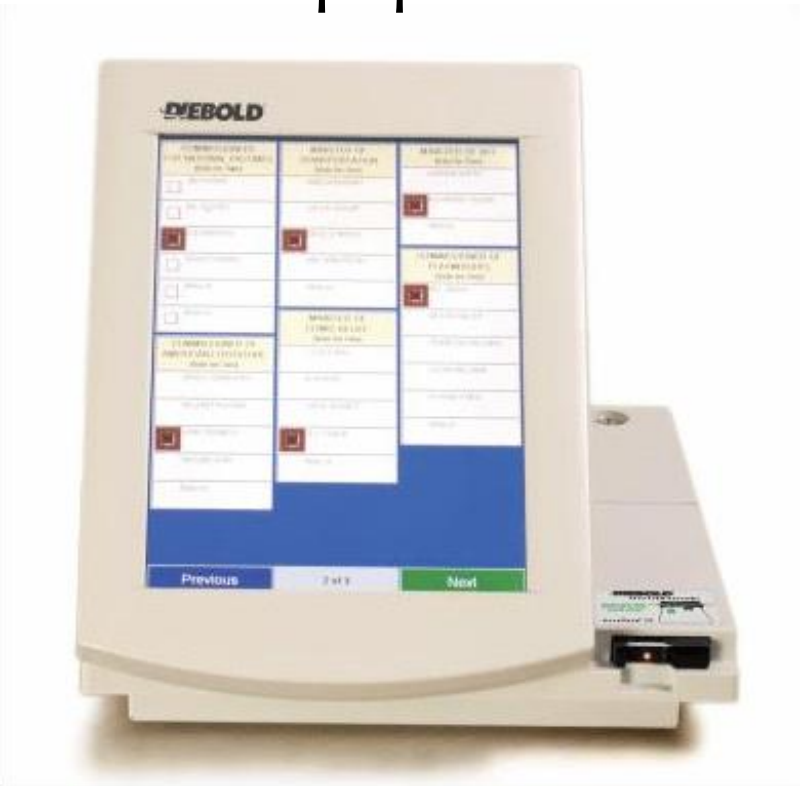
THREAT MODELING

Threat Modeling (Security Reviews)

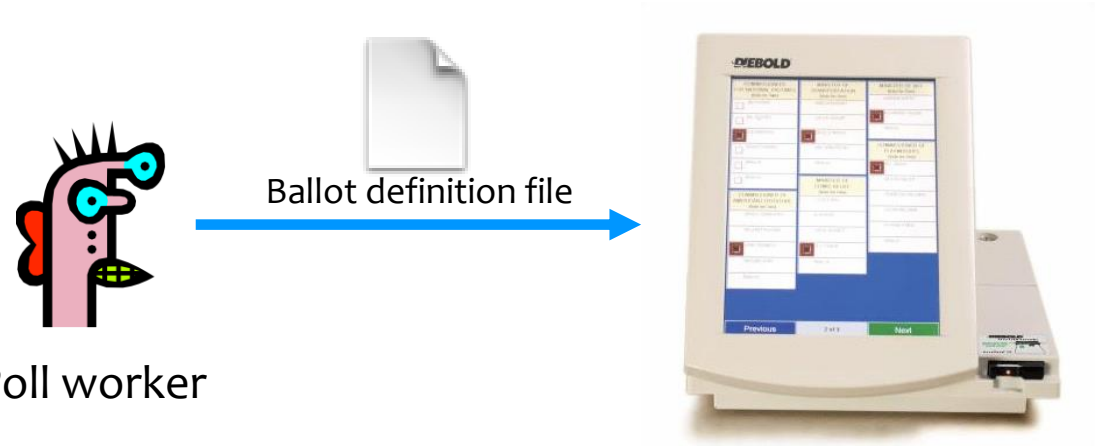
- Assets: What are we trying to protect? How valuable are those assets?
- Adversaries: Who might try to attack, and why?
- Vulnerabilities: How might the system be weak?
- Threats: What actions might an adversary take to exploit vulnerabilities?
- Risk: How important are assets? How likely is exploit?
- Possible Defenses

Example: Electronic Voting

- Popular replacement to traditional paper ballots

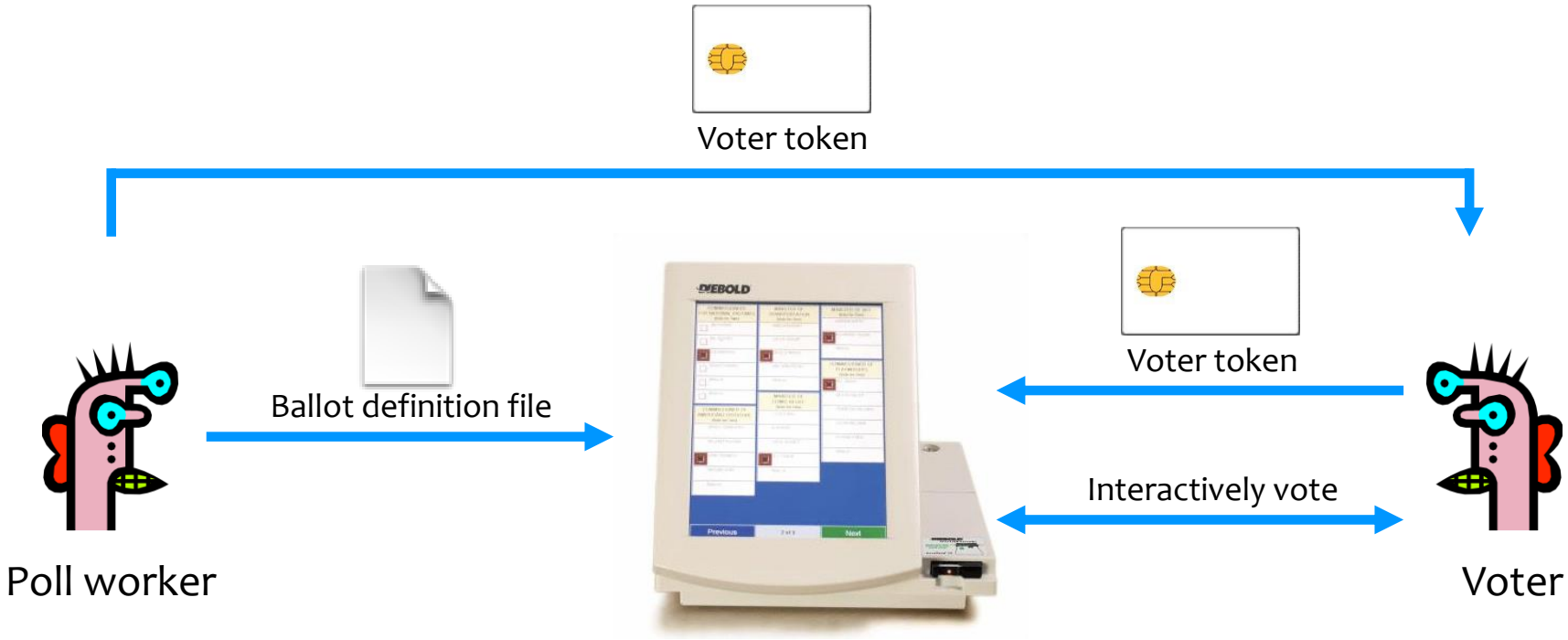


Pre-Election



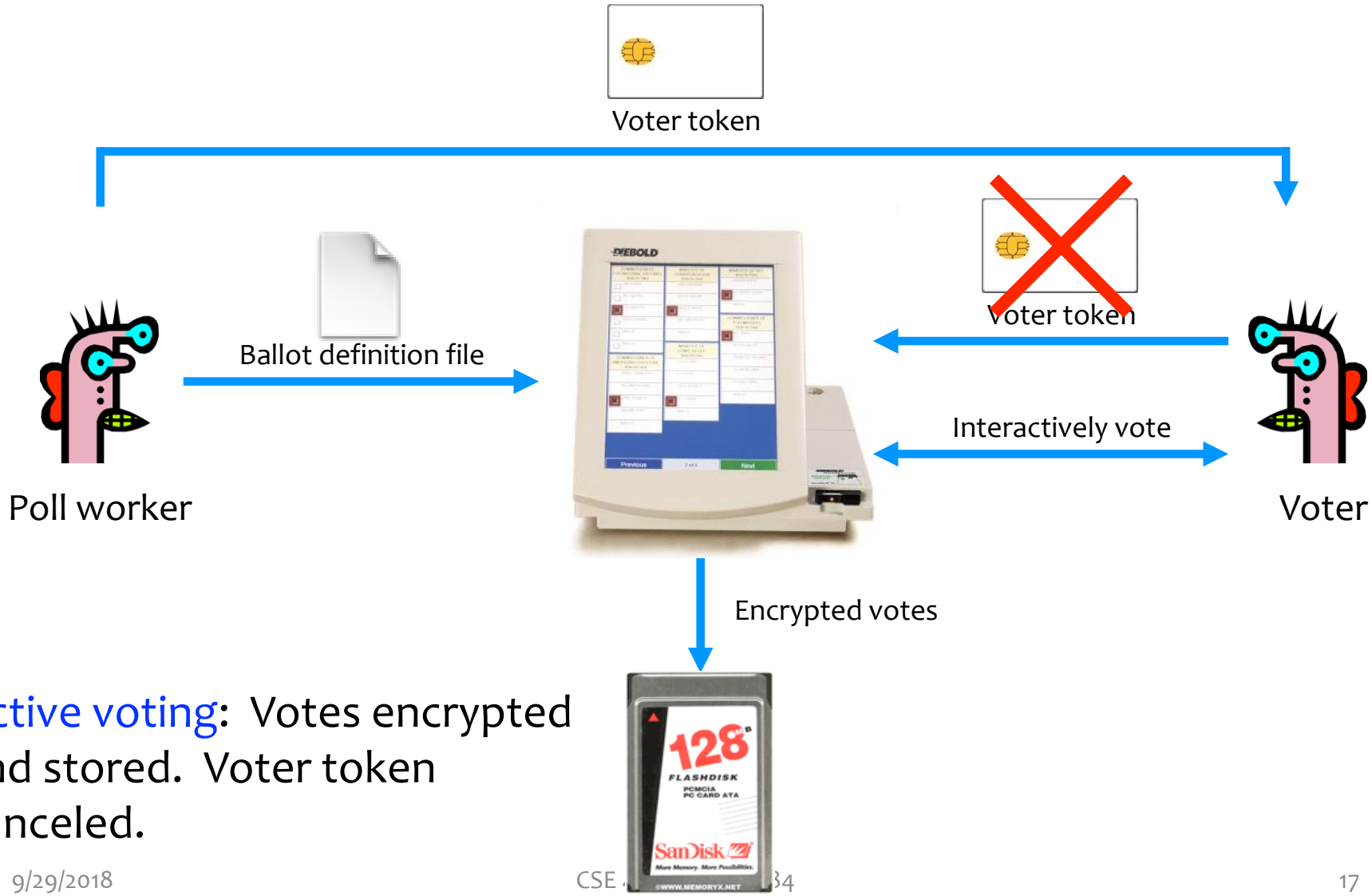
Pre-election: Poll workers load "ballot definition files" on voting machine.

Active Voting



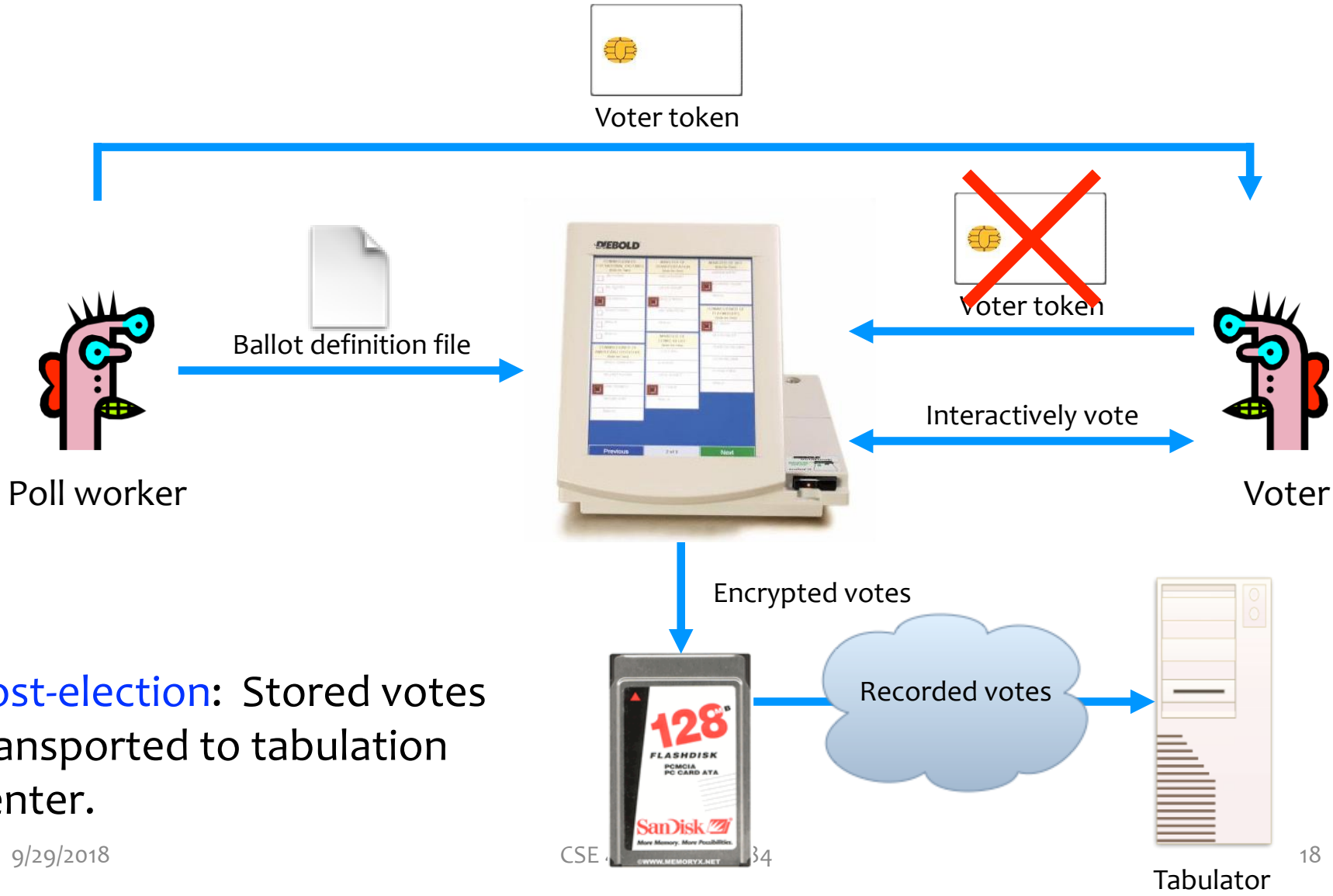
Active voting: Voters obtain single-use tokens from poll workers. Voters use tokens to activate machines and vote.

Active Voting



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

Post-Election

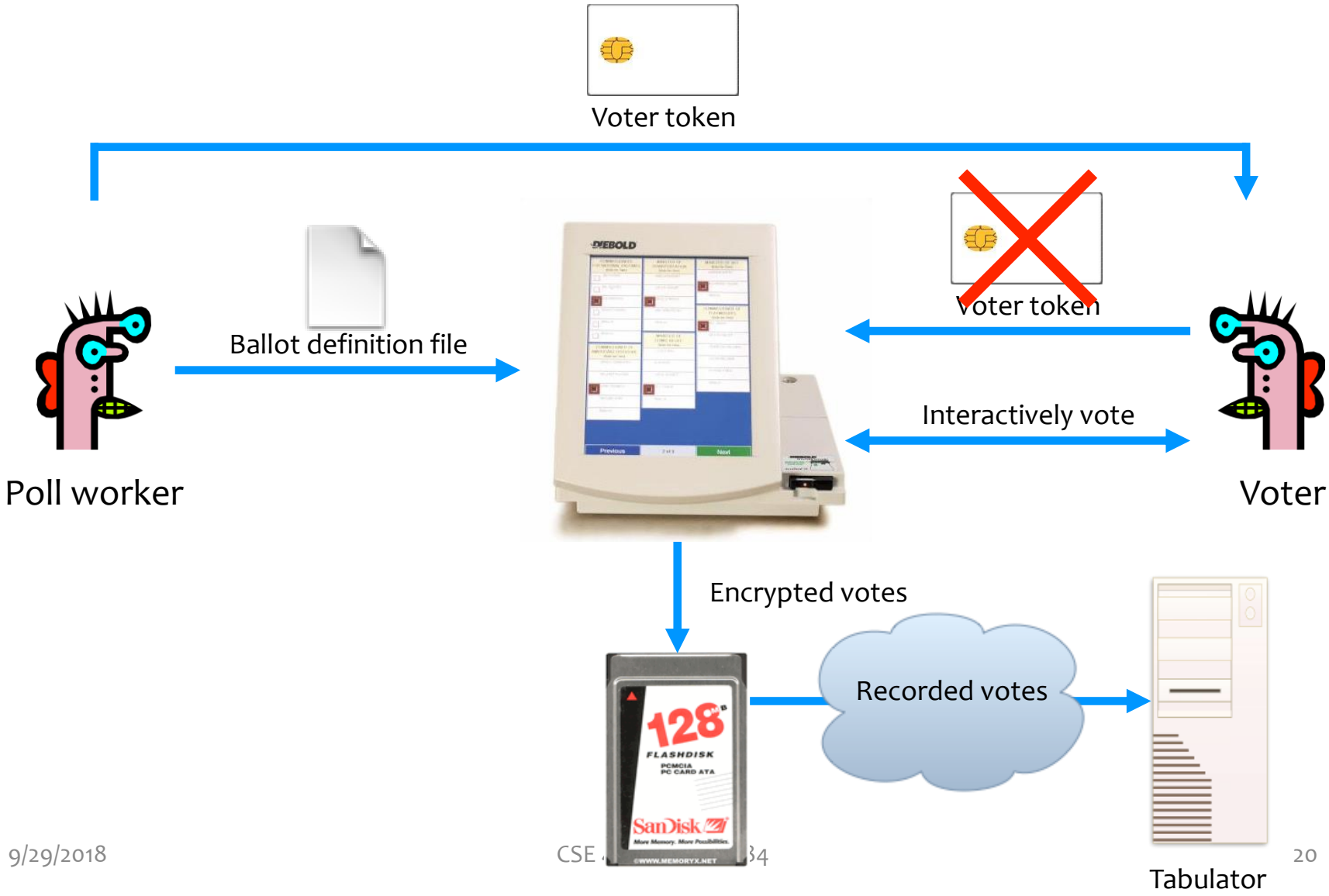


Post-election: Stored votes transported to tabulation center.

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**)

Can You Spot Any Potential Issues?



Q1 and Q2 on the Worksheet

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

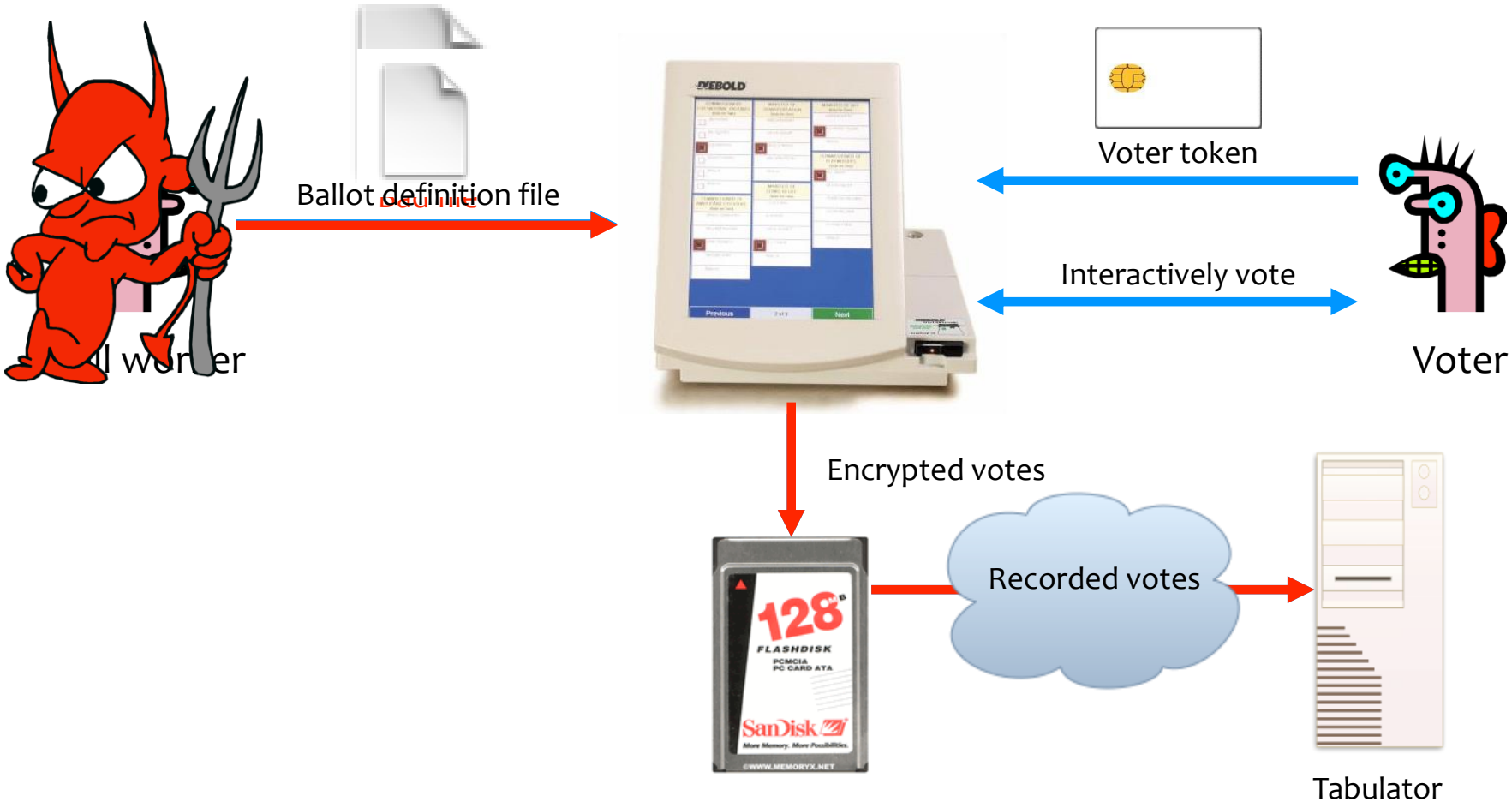
What Software is Running?

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.

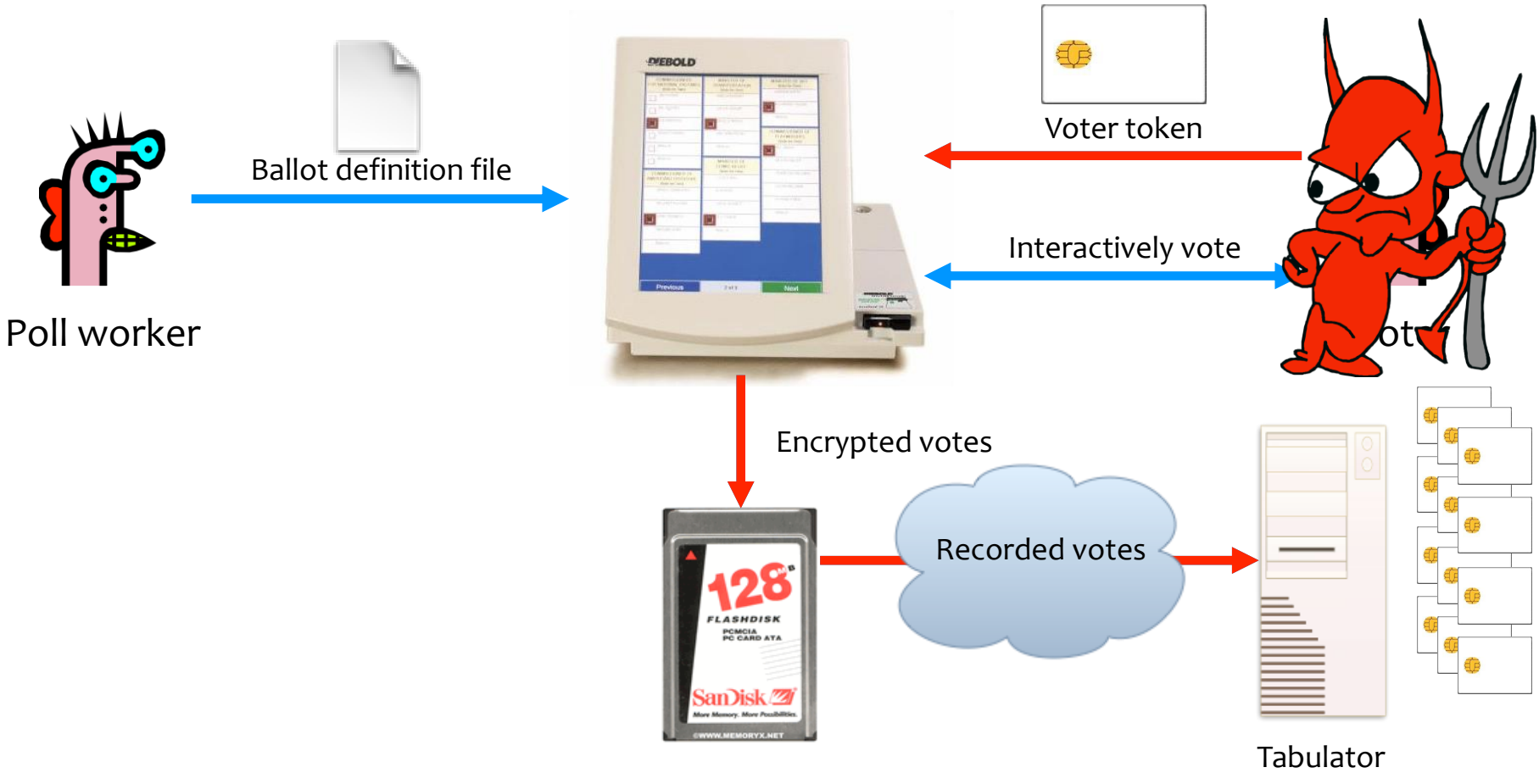
Problem: Ballot definition files are not authenticated.

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



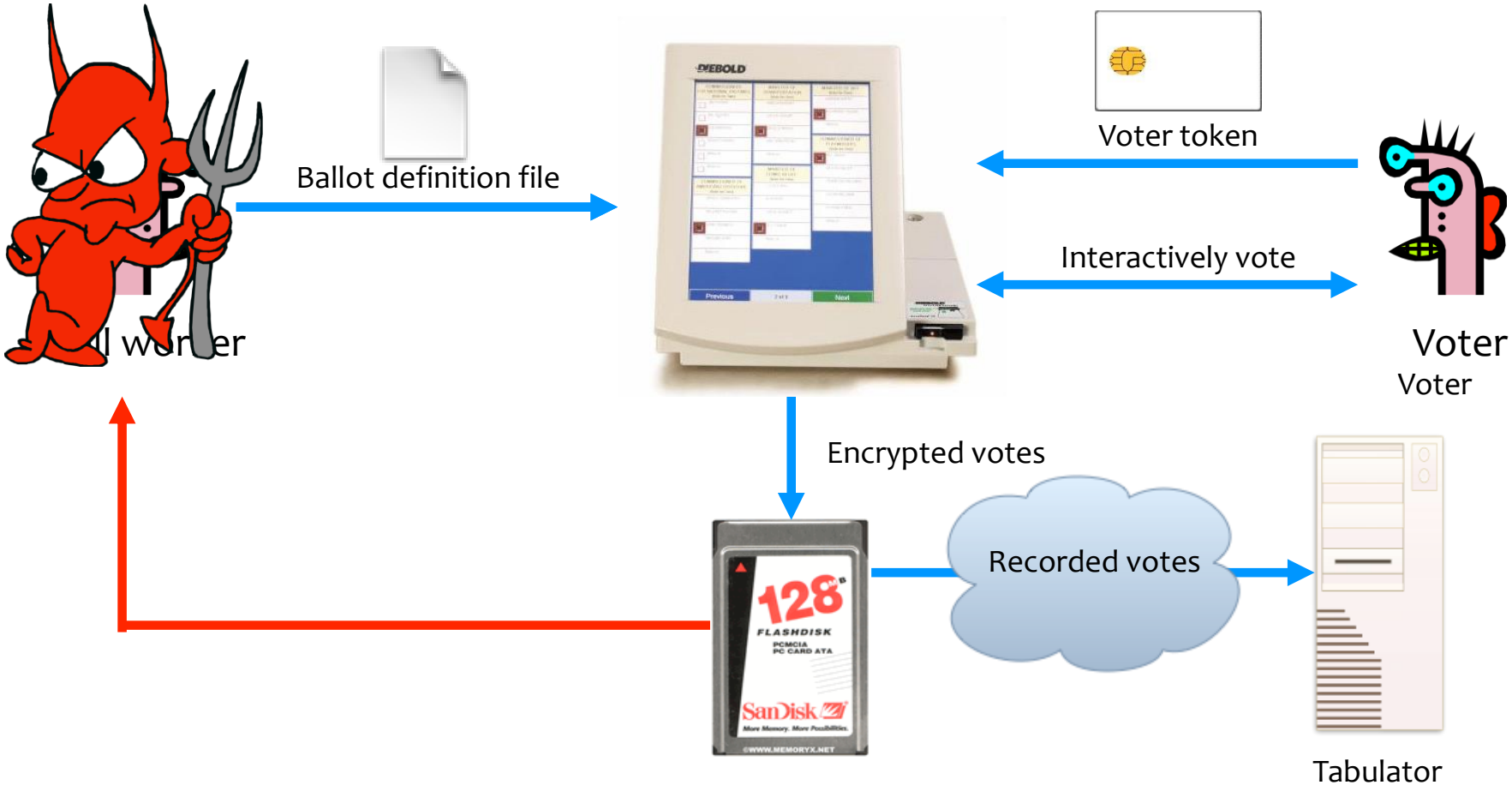
Problem: Smartcards can perform cryptographic operations. But there is no authentication from voter token to terminal.

Example attack: A regular voter could make his or her own voter token and vote multiple times.



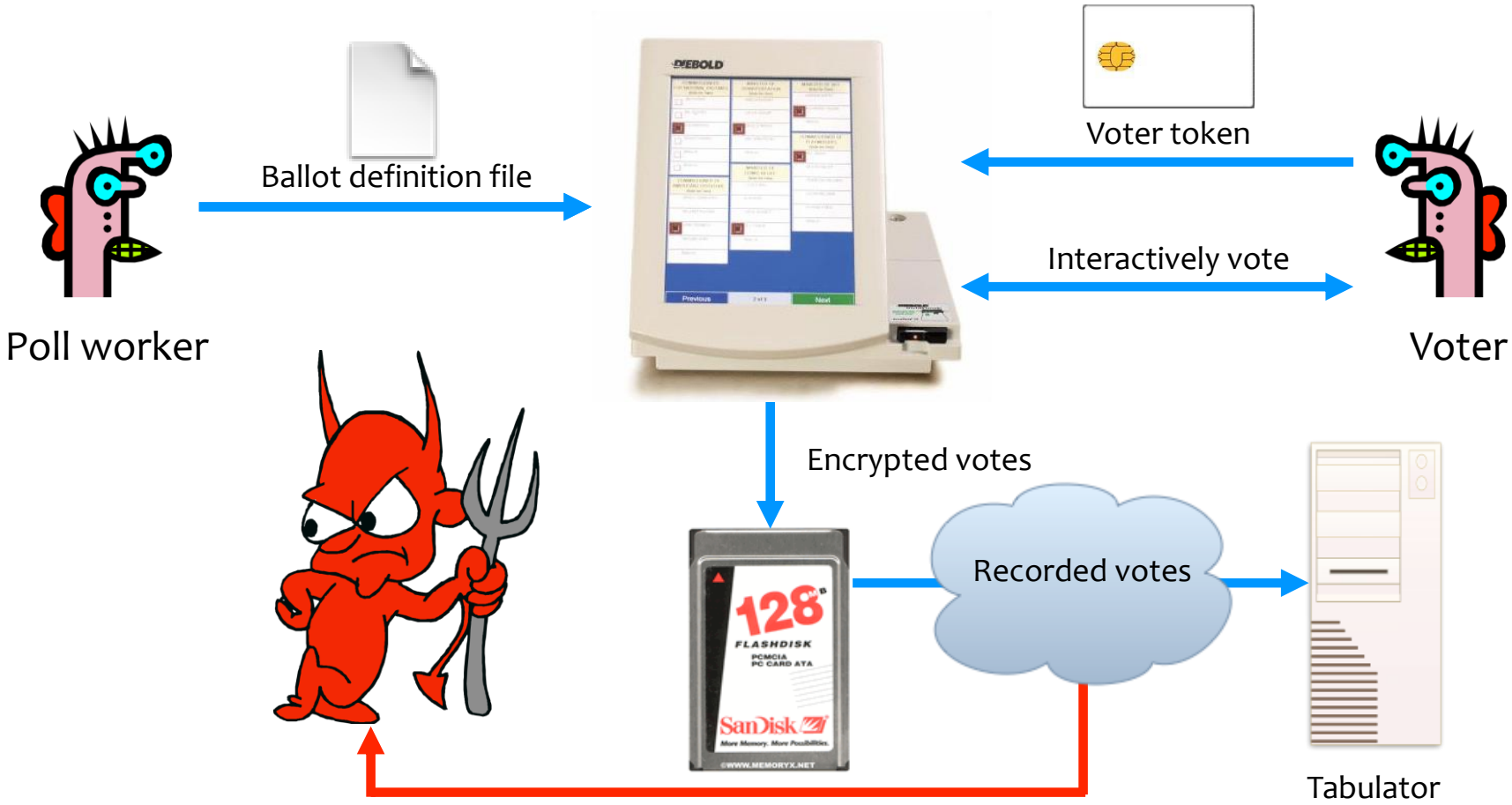
Problem: Encryption key ("F2654hD4") hard-coded into the software since (at least) 1998. Votes stored in the order cast.

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.



Tables Often Help!

Example Table 1

Attacker "Positions"	Machine Manufacturer	Poll Worker	Voter	Power Company Employee
Voter Privacy				
Vote Integrity				
Voting Machine Availability				
…				

- What can different parties do? Each cell would have an action or actions that these parties might try do
- Note that some parties could collaborate

Example Table 2

Attack Methods	Modify Software	Produce Fake Voter Tokens	Steal Flash Drive	Intercept Network Connections
Voter Privacy				
Vote Integrity				
Voting Machine Availability				
…				

- What different attack methods are there? (Columns)
- Who could mount these different attacks? What are the attack details (the cells)
- How easy is it to implement each of these attack methods?

Table from Paper

https://homes.cs.washington.edu/~yoshi/papers/eVoting/vote.pdf

	Voter (with forged smartcard)	Poll Worker (with access to storage media)	Poll Worker (with access to network traffic)	Internet Provider (with access to network traffic)	OS Developer	Voting Device Developer	Section
Vote multiple times using forged smartcard	•	•	•				3.2
Access administrative functions or close polling station	•	•			•	•	3.3
Modify system configuration		•			•	•	4.1
Modify ballot definition (e.g., party affiliation)		•	•	•	•	•	4.2
Cause votes to be miscounted by tampering with configuration		•	•	•	•	•	4.2
Impersonate legitimate voting machine to tallying authority		•	•	•	•	•	4.3
Create, delete, and modify votes		•	•	•	•	•	4.3, 4.5
Link voters with their votes		•	•	•	•	•	4.5
Tamper with audit logs		•			•	•	4.6
Delay the start of an election		•	•	•	•	•	4.7
Insert backdoors into code					•	•	5.3

Table 1: This table summarizes some of the more important attacks on the system.

TOWARDS DEFENSES

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

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

Whole System is Critical