CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous Class

- What is security?
  - Terminologies
    - Assets, vulnerabilities, threats, attacks and controls
  - Goal of Adversary
  - Goal of Owner\ Administrator
- Security Services

This Class

- Security Tolls
- Program security
  - Flaws,

    faults, and failures
  - Unintentional security flaws
    - Buffer overflows

Problems

- Problems with Threat model
  - Consider a system uses DES 56-bit key at present
    - Computational assumption changes over time
  - Human factor not accounted
  - User gets email asking to send credential,
  - Assumption
    - CA are assumed trusted. In 2011 issued fake certs
- Problems with the policy
  - Yahoo mail has user name password and security Qs
- Problems with the mechanism
  - No of password attempts in login system
  - Small IV in WEP

Countermeasures

means used to deal with security attacks

- prevent
- detect
- recover

may introduce new vulnerabilities

Residual vulnerabilities may remain

goal is to minimize residual level of risk to the assets

Threat Modelling

- 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

Threat Modelling (Security Reviews)

- Assets: What are we trying to protect? How valuable are those assets?
- Risk: How important are assets? How likely is exploit?
- 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?
- Possible Defenses

Threat Consequences (3Ds)

Disclosure is a threat to confidentiality

- **Exposure**: This can be deliberate or be the result of a human, hardware, or software error
- **Interception**: unauthorized access to data
- **Inference**: e.g., traffic analysis or use of limited access to get detailed information
- **Intrusion**: unauthorized access to sensitive data

Threat Consequences

Deception is a threat to either system or data *integrity*

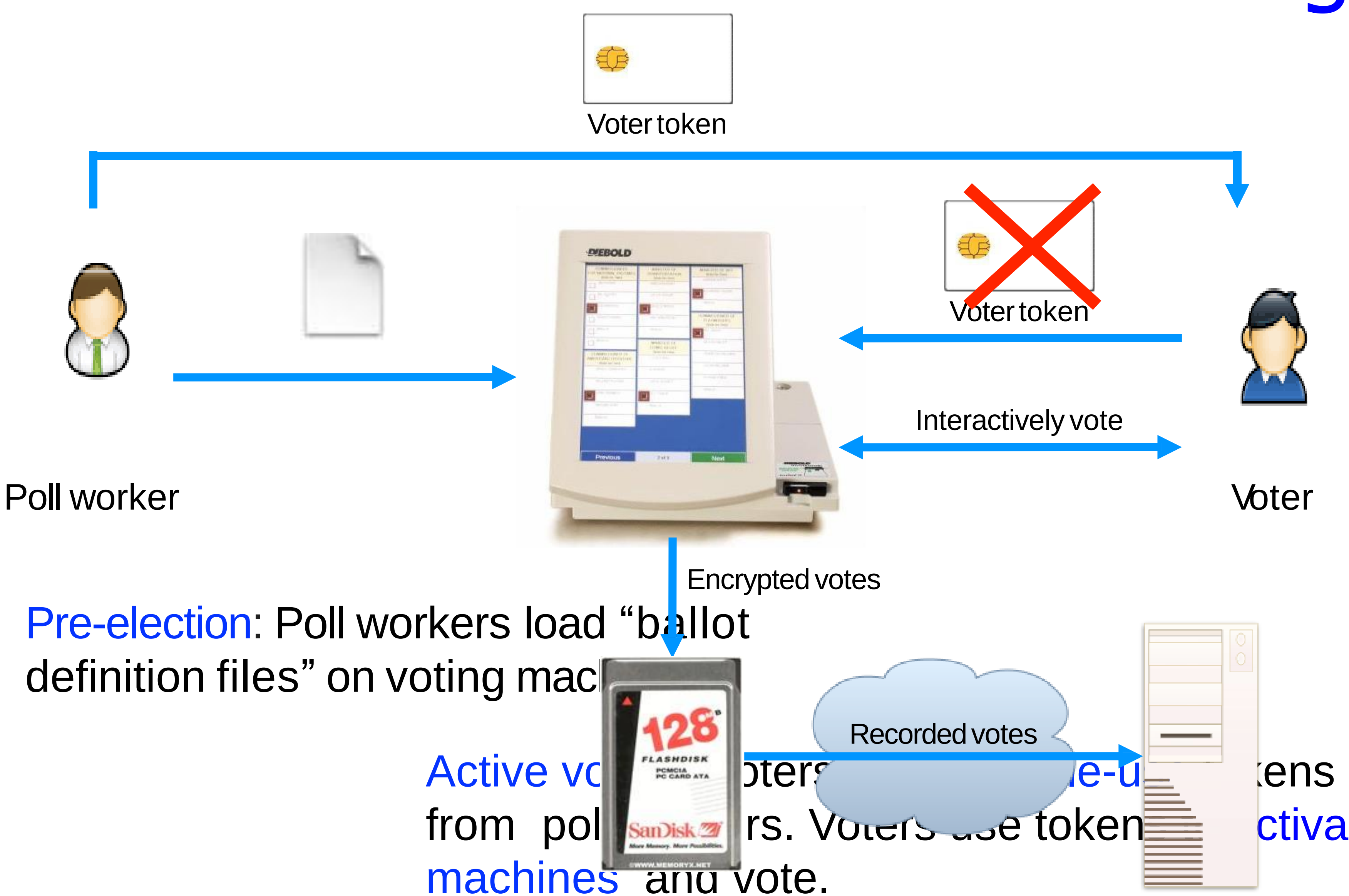
- ***Falsification***: altering or replacing of valid data or the introduction of false data
- ***Repudiation***: denial of sending, receiving or possessing the data.
- ***Misuse***: security functions can be disabled or thwarted
- ***Masquerade***: an attempt by an unauthorized user to gain access to a system by posing as an authorized user

Threat Consequences

Disruption is a threat to *availability* or *system integrity*

- ***Incapacitation***: a result of physical destruction of or damage to system hardware
- ***Obstruction***: e.g. overload the system or interfere with communications
- ***Misappropriation***: e.g., theft of service, distributed denial of service attack
- ***Corruption***: system resources or services function in an unintended manner; unauthorized modification

Threat Modeling of Electronic Voting



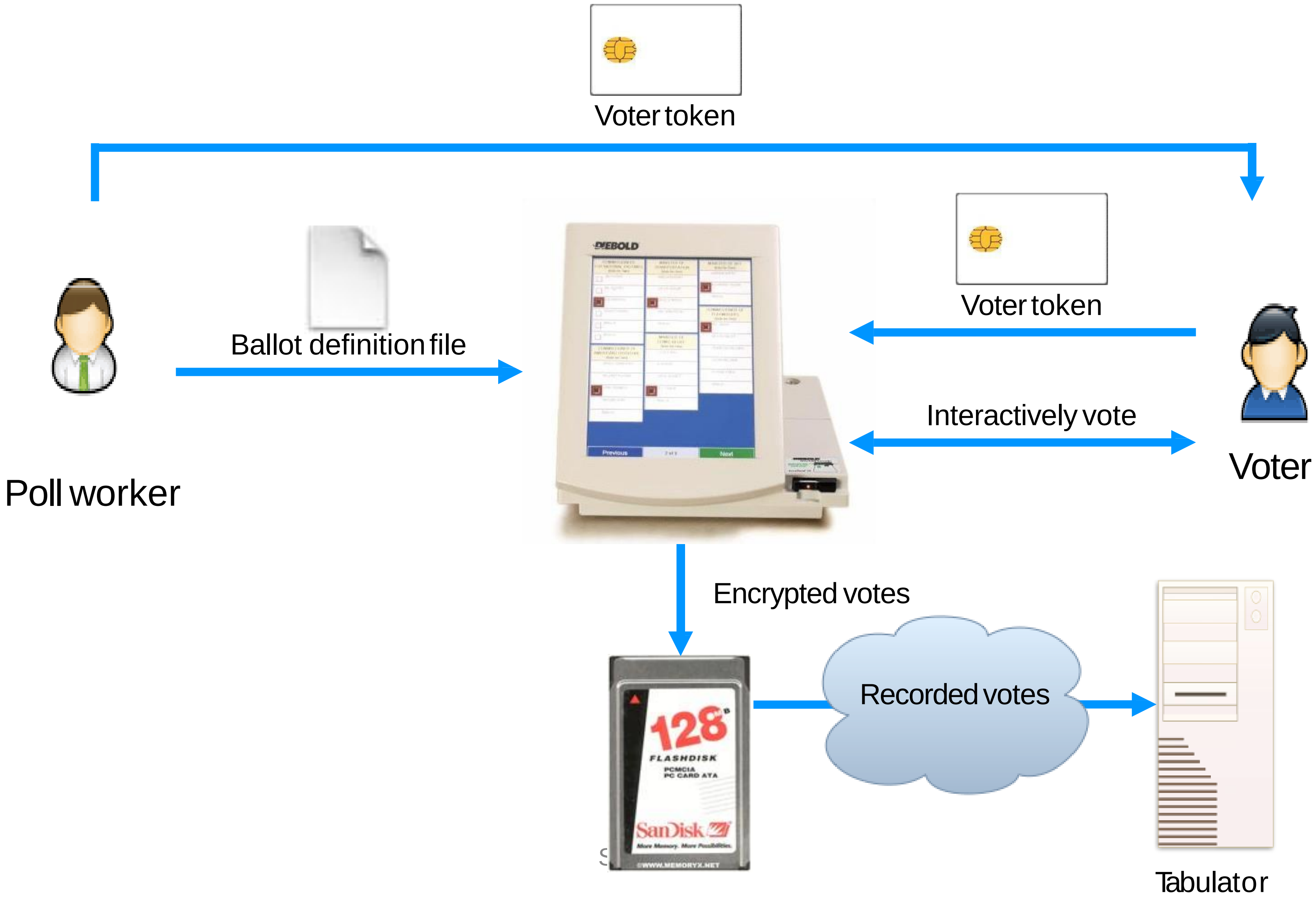
Pre-election: Poll workers load “ballot definition files” on voting mac

Active vo oters e-u kens from pol rs. Voters use token ctivate machines and vote.

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

Post-election: Stored votes transported to tabulation center.

Any issues ?



Voter token

Poll worker

Ballot definition file

Voter token

Interactively vote

Voter

Encrypted votes

Recorded votes

Tabulator

Security goals

- Adversary should not be able to figure out how voters vote (confidentiality)

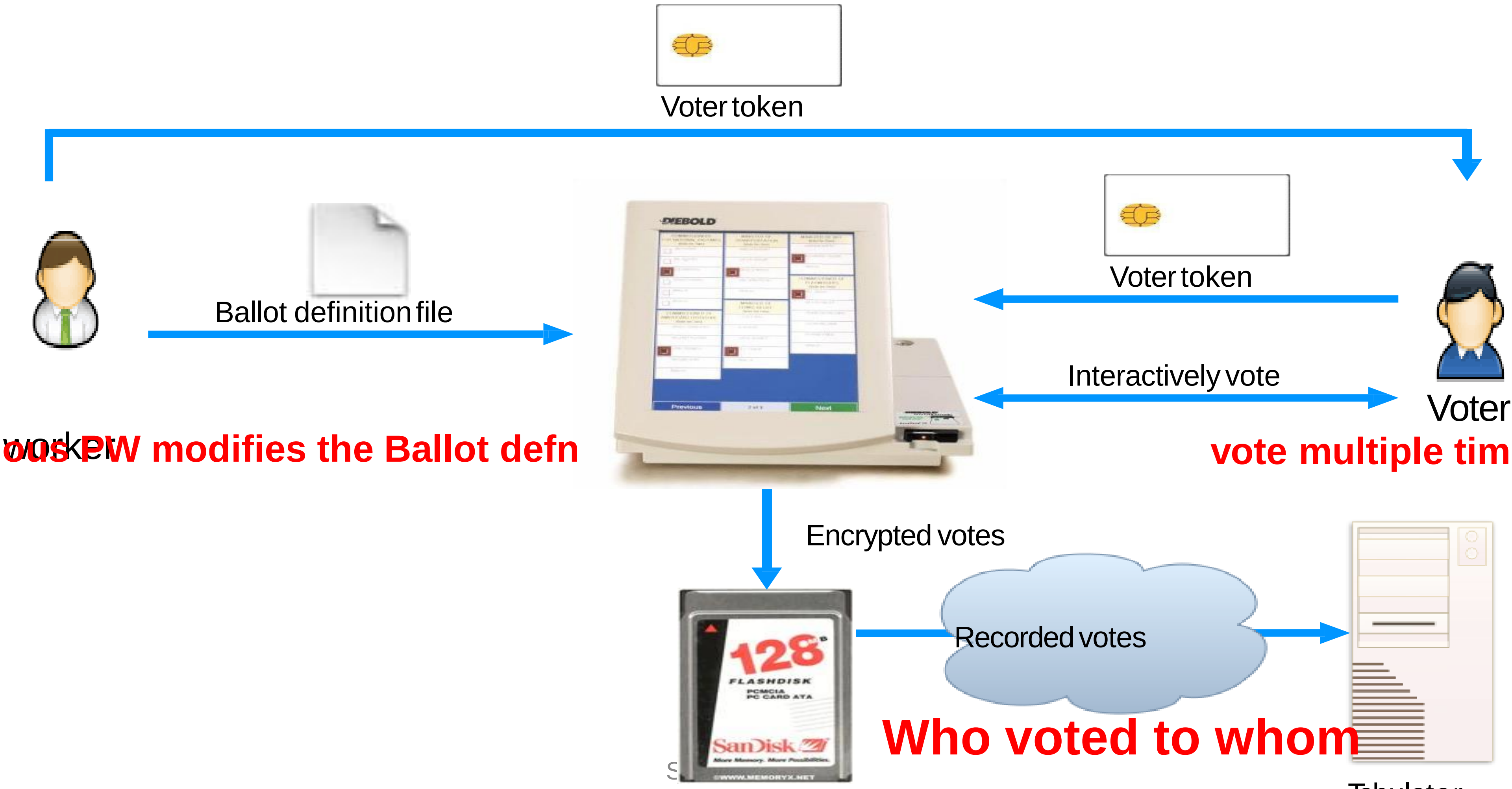
- Adversary should not be able to tamper with the election outcome
  - By changing votes (integrity)
  - By voting on behalf of someone (authenticity)
  - By denying voters the right to vote (availability)

Who can be adversary?

- Voters
- Election officials
- Employees of voting machine manufacturer
- Makers of underlying software or add-on components
- Makers of compiler
- …
- Or any combination of the above

Use case: Electronic Voting

What an Adversary could do?



Voter token

Ballot definition file

Poll worker

Malicious PW modifies the Ballot defn

Voter token

Interactively vote

Voter

vote multiple times

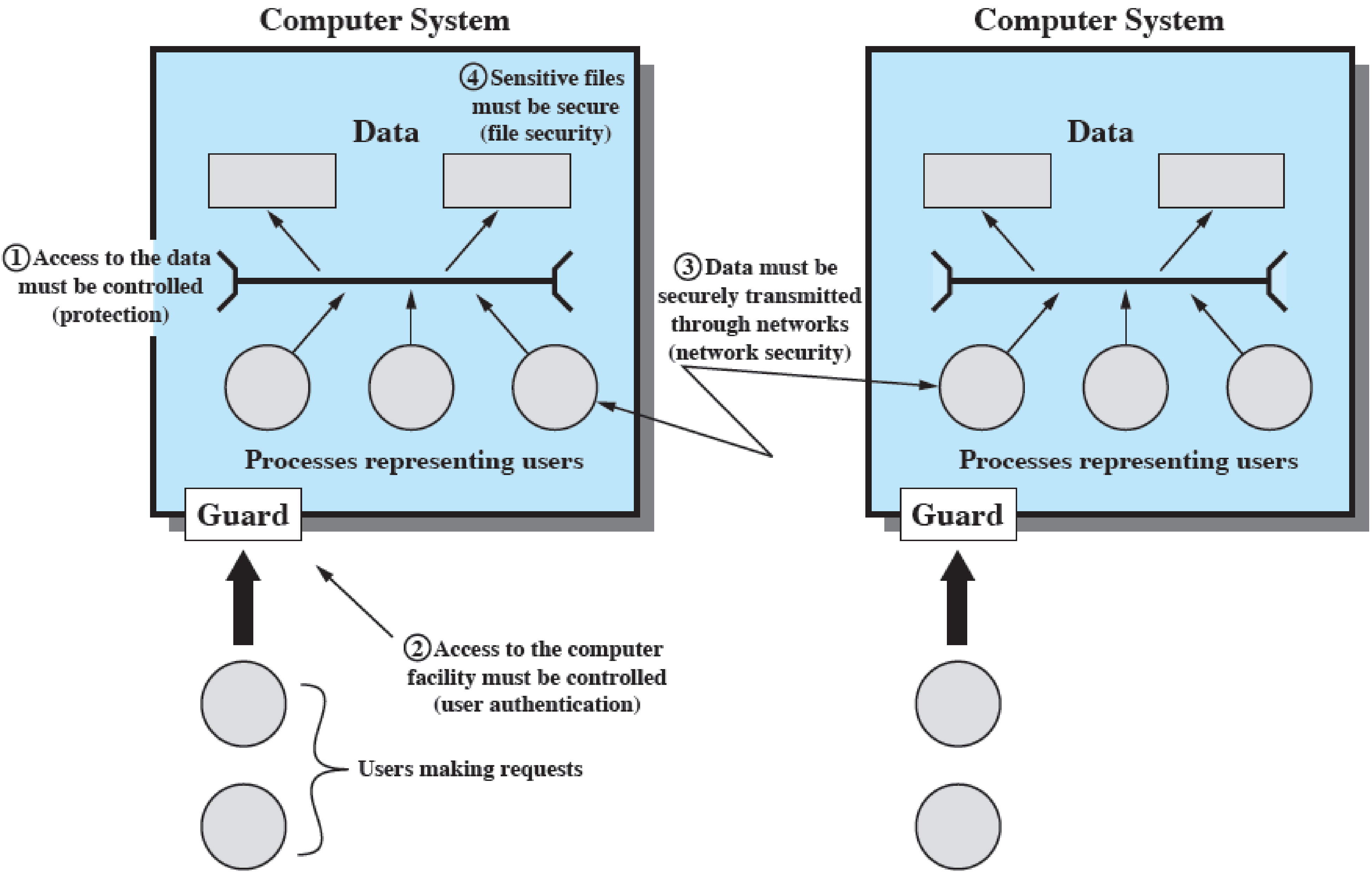
Encrypted votes

Recorded votes

Who voted to whom

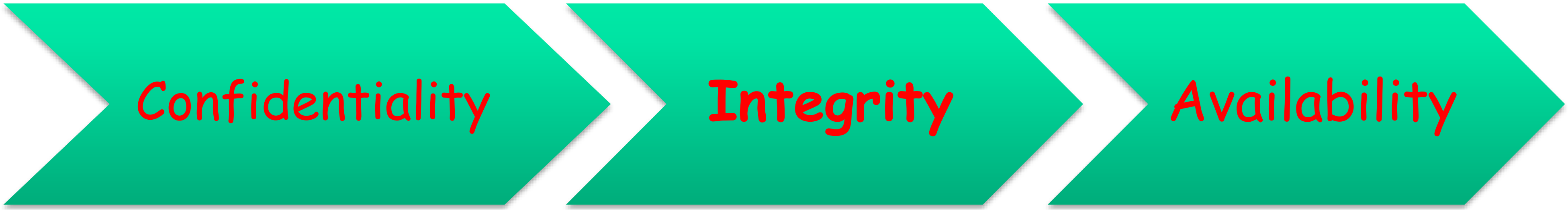
Tabulator

Scope of Computer Security


Computer System
Computer System
Data
Data
④Sensitive files must be secure (file security)
①Access to the data must be controlled (protection)
③Data must be securely transmitted through networks (network security)
Processes representing users
Processes representing users
Guard
Guard
②Access to the computer facility must be controlled (user authentication)
Users making requests

Security Goals

Basic Security Services
Key Security Concepts (FIPS PUB 199)



Confidentiality

- preserving authorized restrictions on information access and disclosure.

Integrity

- guarding against improper information modification or destruction,

Availability

- ensuring timely and reliable access to and use of information

Thanks