Policies, mechanisms, and assurance

Specification and implementation

For any system:

- Specification: *What is it supposed to do?*
- Implementation: *How does it do it?*
- Correctness: *Does it really work?*

In security:

- Specification: *Policy*
- Implementation: *Mechanism*
- Correctness: *Assurance*

Caveats

But:

- Some mechanisms are presented as policies.
- Mechanisms sometimes come before policies.
- Assurance can guide policies and mechanisms.
- Assurance is sometimes replaced with "security by obscurity".
- Attacks can exploit gaps at any level.

Security properties

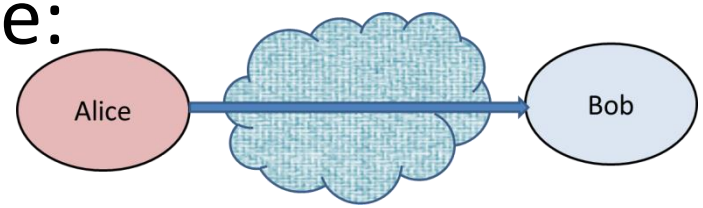
The main security properties are:

- ***Integrity properties***
  (no improper modification of information)
- ***Secrecy properties***
  (no improper disclosure of information)
- ***Availability properties***
  (no improper denial of service)

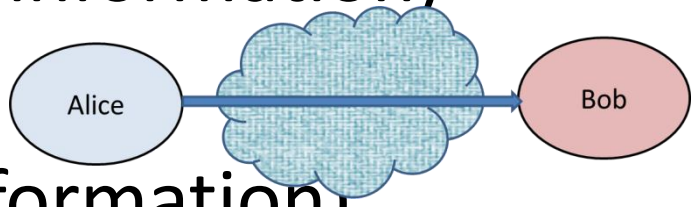
Security properties

The main security properties are:

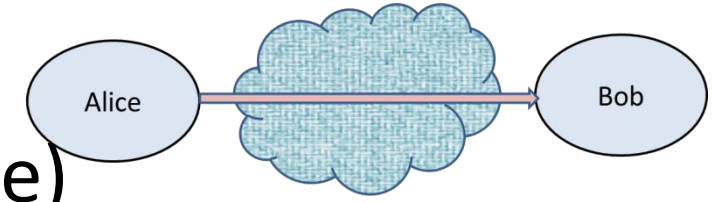
- ***Integrity properties***
  (no improper modification of information)



- ***Secrecy properties***
  (no improper disclosure of information)



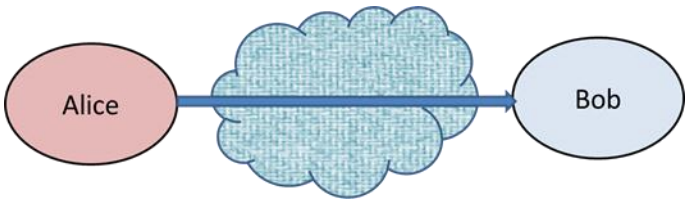
- ***Availability properties***
  (no improper denial of service)



Variations on integrity

Authenticity is often the same as integrity,

- with a difference only in emphasis,
- or with a requirement of freshness.



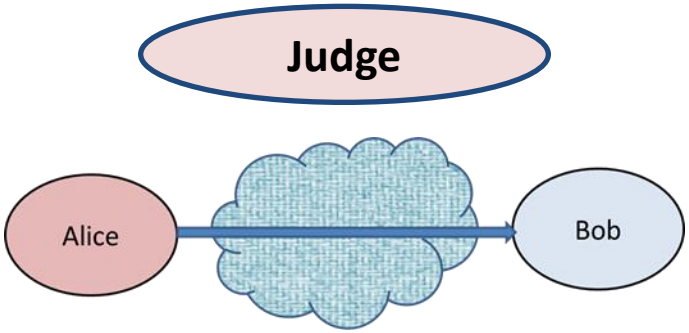
Variations on integrity

Authenticity is often the same as integrity,

- with a difference only in emphasis,
- or with a requirement of freshness.

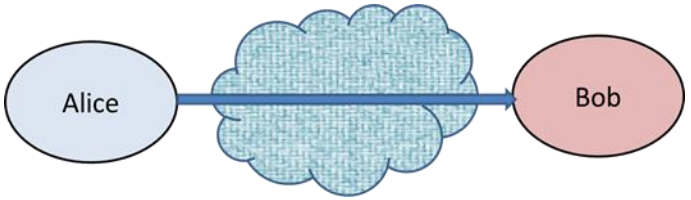
Other concepts are closely related to integrity:

- ***non-repudiation***,
- ***accountability***.



Variations on secrecy

- Similarly, ***confidentiality*** is basically secrecy.
- So is ***privacy***, often, in the context of personal information. (More on this later.)
- ***Anonymity*** is basically an instance of secrecy.
- ***Pseudonymity*** is anonymity plus linkability.
- ***Plausible deniability*** is the contrary of non-repudiation and might be viewed as a weak form of secrecy.



Security policies

Security properties are combined into security policies. For example, a bank may want:

- authenticity of clients at ATMs, on the Web,
- non-repudiation of transactions,
- integrity of the books,
- integrity of the messaging systems,
- secrecy for client data and for internal data,
- availability of the alarm system.

Security policies (cont.)

Policies are not always articulated precisely.
E.g.:

- for privacy of personal data,
- against email flooding and spam,
- against denial-of-service attacks.

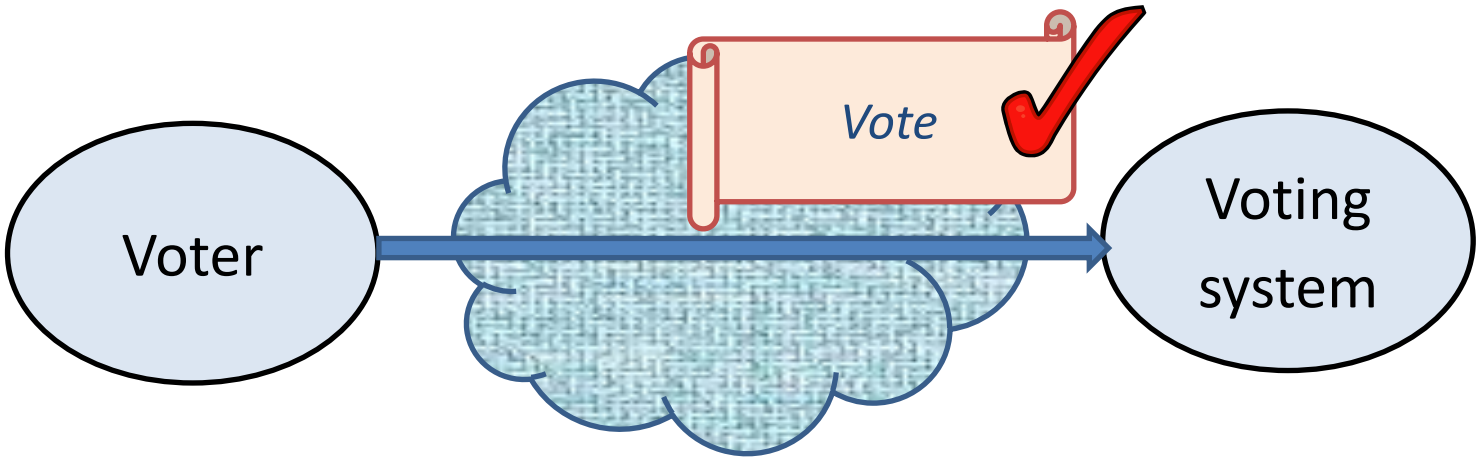
Security policies (cont.)

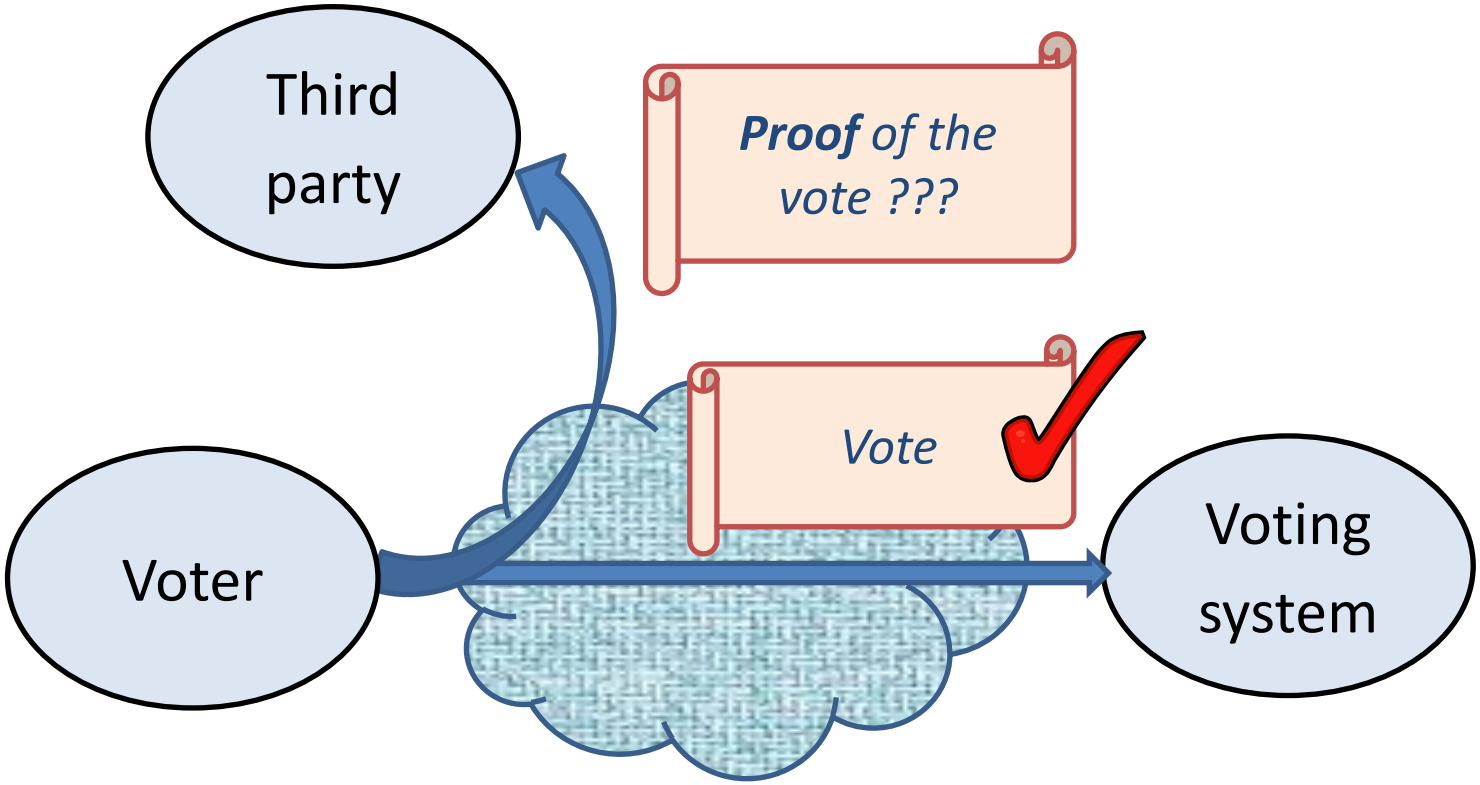
Policies are not always articulated precisely.
E.g.:

- for privacy of personal data,
- against email flooding and spam,
- against denial-of-service attacks.

Policies may include less standard properties.
E.g.:

- exclusivity of duties,
- dual control for sensitive transactions.


Voter
Vote
Voting system


Third party
Proof of the vote ???
Vote
Voter
Voting system

Security policies (cont.)

Security properties are often in conflict

- because of the conflicting goals of each party (e.g., integrity vs. secrecy),
- because each party has its own goals (e.g., anonymity vs. non-repudiation).

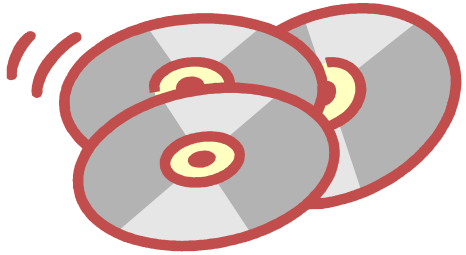
The Boston Globe

Security firm: Sony CDs secretly install spyware

Company denies it, saying program aims to foil music piracy

By Hiawatha Bray

Globe Staff / November 8, 2005



Defining security

There is no unique definition of security

- Different security policies are appropriate for different users, organizations, and systems.
- Security is largely subjective (or conventional). Whether an attack is serious or not, and whether it is an attack at all, depends on what we expect from the system.

Il suffit de penser que l'acquisition d'un bien ou la fuite d'un mal est possible, pour être incité à la désirer. Mais quand on considère, outre cela, s'il y a beaucoup ou peu d'apparence qu'on obtienne ce qu'on désire, ce qui nous représente qu'il y en a beaucoup, excite en nous l'espérance, et ce qui nous représente qu'il y en a peu, excite la crainte, dont la jalousie est une espèce. Lorsque l'espérance est extrême, elle change de nature et se nomme sécurité ou assurance.

Descartes

Roughly:

It suffices to think that the acquisition of a good or the escape from an evil is possible in order to be incited to desire it. But when one considers, in addition, whether there is much or little appearance that one will obtain it, what represents to us that there is much excites in us hope, and what represents to us that there is little excites in us fear, of which jealousy is a kind. When hope is extreme, it changes nature and is called security or assurance.

Descartes

Security is a joy born of the idea of a future or past thing, concerning which the cause of doubting has been removed.

Spinoza

Any information that you put into a computer is public information.

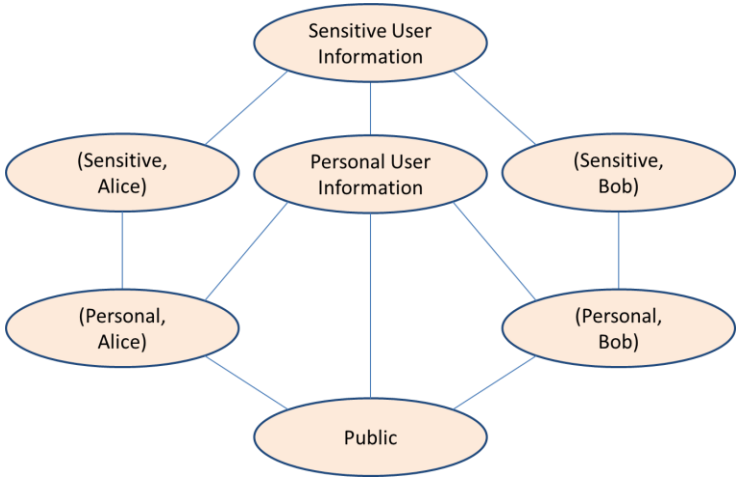
Thacker

Common themes

- Interaction with an uncertain environment. (Contrast with mutual exclusion.)
- Some security even against lucky, powerful, or persistent attackers.
  - Even if the attacker controls the network.
  - Even if a secret is compromised.
  - Even if an insider is dishonest.
- Doing without full functional correctness. E.g., message origin, not message correctness.

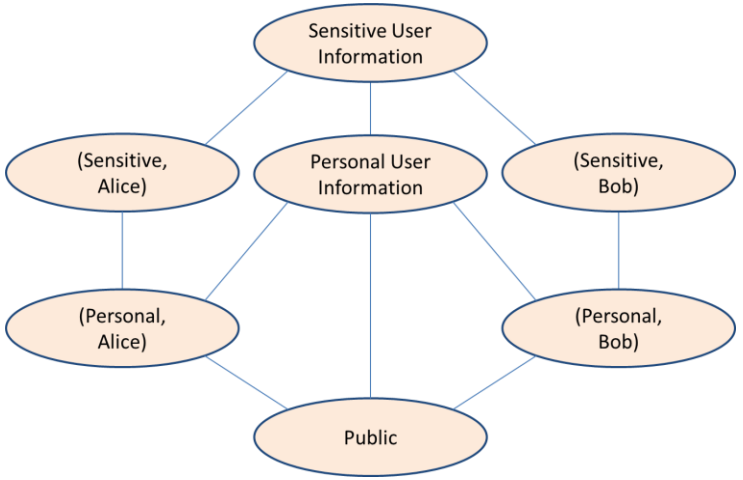
Information-flow security (preview)

- Classify data and principals into levels (e.g., public, secret, and top secret, or trusted and untrusted).
  - The levels need not be linearly ordered.
  - They should form a lattice.



Information-flow security (preview)

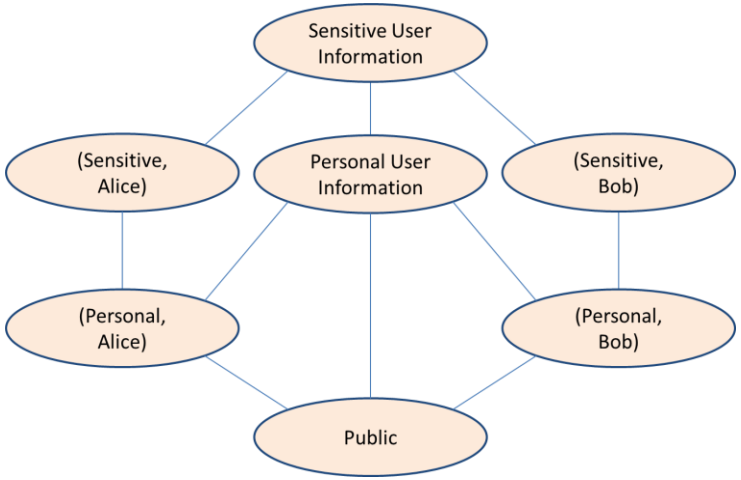
- Classify data and principals into levels (e.g., public, secret, and top secret, or trusted and untrusted).
  - The levels need not be linearly ordered.
  - They should form a lattice.



- Guarantee that a principal at level *k* sees data only for levels less than or equal to *k*.

Information-flow security (preview, cont.)

- Multiple mechanisms may be used:
  - Enforcement may rely on tagging data and principals with their levels, and on monitoring all communications, dynamically.
  - Enforcement may also include static analysis.



- Assurance may include formal verification.

  (We will return to assurance later in the course.)