Foundations of Computer Security

Lecture 19: What is Integrity?

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Meaning of Computer Security

Recall that computer security is described as encompassing at least:

Confidentiality: who can *read* information;

Integrity: who can *write* or modify information;

Availability: what mechanisms ensure that resourses are available when needed.

Confidentiality models, like BLP, are useful but obviously limited.

How might we extend our models to handle integrity concerns?

Integrity

Integrity is a fuzzier notion than confidentiality and more context dependent.

- Who is authorized to supply or modify data?
- How do you separate and protect assets?
- How do you detect and/or correct erroneous or unauthorized changes to data?
- Can authorizations change over time?

Unlike confidentiality, *a program can damage integrity without interaction with the external world, simply by computing data incorrectly.*

Integrity Thought Experiment

Suppose you're checking out at the grocery store and on the adjacent newsrack you notice the headline: "Hillary Clinton to have Alien's Baby." *Do you believe it?*

Your reaction might be different depending on whether the publication is:

1. *The New York Times*: Wow! Could there be something to this?
2. *The Wall Street Journal:* The vast right wing conspiracy is after poor Hillary again!
3. *The National Enquirer:* They clearly just made it up.

What's different in the three cases? It's your assessment of the *integrity* of the source.

Integrity Labels

As we did with confidentility, we might assign *integrity labels*:

- An *object's* label characterizes the degree of "trustworthiness" of the information contained in that object.

  Gossip overheard on the subway should have lower credibility than a report from a panel of experts.

- A *subject's* label measures the confidence one places in its ability to produce / handle information.

  A certified application may have more integrity than freeware downloaded from the Internet.

Some Integrity Principles

Intuitively, integrity relates to *how much you trust an entity to produce, protect, or modify data.*

Integrity has aspects and principles of operation not as relevant to military security:

Separation of Duty: several *different* subjects must be involved to complete a critical function.

Separation of Function: a single subject cannot complete complementary roles within a critical process.

Auditing: recoverability and accountability require maintaining an audit trail.

Often commercial security controls are discretionary, procedural, and decentralized, rather than mandatory and centralized.

Commercial Concerns

Integrity concerns are frequently more important than confidentiality concerns in commercial settings.

For example, Steve Lipner (Microsoft) describes integrity concerns you might find in a commercial data processing environment:

1. Users will not write their own programs, but use existing production software.
2. Programmers develop and test applications on a nonproduction system, possibly using contrived data.
3. Moving applications from development to production requires a special process.
4. This process must be controlled and audited.
5. Managers and auditors must have access to system state and system logs.

Lessons

- Integrity relates to how much we trust an entity to produce, protect, or modify data.
- Unlike confidentiality, violations of integrity don't require external action.
- In some applications, particularly in the commercial world, integrity is more important than confidentiality.

Next lecture: Modeling Integrity