Foundations of Computer Security

Lecture 4: Aspects of Security

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

Aspects of Security

Often, computer security is defined to encompass:

Confidentiality: (also called secrecy/privacy) who can *read* information?

Integrity: who can *write*, modify or generate information?

Availability: are resources available when needed?

Some experts (e.g., NSA) add to this list:

Authentication: how do we establish identity?

Non-repudiation: can I deny my actions?

What About ...?

Many other topics relate to computer security:

- cryptography,
- digital signatures,
- access control,
- firewalls,
- passwords,
- certificates,
- many others.

These are *mechanisms* for protecting one or more of the major aspects such as confidentiality or integrity.

Which Is Most Important

Question: Of confidentiality, integrity, and availability, which is the most important?

Answer: It all depends on the context.

- For a DoD system protecting the national war plan, *confidentiality* may be paramount.
- For a bank protecting financial data, *integrity* may count most.
- For an online retailer, *availability* may be a matter of survival.

What is Confidentiality About?

How do I protect my information from unauthorized disclosure?

Historically, this was the first computer security concern, and remains extremely important in military and commercial settings.

- Is all of my data equally sensitive? If not, how do I group and categorize data?
- How do I characterize who is authorized to see what?
- How are the permissions administered and checked? According to what rules?
- Can authorizations change over time?

What is Integrity About?

How do I protect my information from unauthorized modification?

Integrity is a fuzzier notion than confidentiality and more context dependent. But for many commercial applications it is *more important* than confidentiality.

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

What is Availability About?

How do I ensure that my information/system resources are available when I need them?

Threats to availability are often called *denial of service* (DoS) attacks.

- Are resources provided in a timely fashion?
- Are resources allocated fairly by the system?
- Is the system so difficult/tedius to use as to be useless?
- If faults occur, can the system compensate/recover?
- How is concurrency controlled by the system?

Many virus and worm attacks are DoS attacks. The MyDoom worm cost businesses an estimated $38.5 billion, according to some estimates.

Lessons

- Much of computer security is about protecting confidentiality, integrity and availability.
- Authentication and non-repudiation may also be important in many contexts.
- Which of these is most important is highly dependent on the context.
- Many other topics in security involve *mechanisms* for protecting one of the "big three" (or five).

Next lecture: Policies and Metapolicies