Foundations of Computer Security

Lecture 15: Covert Channels III

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

Covert Channels: Who Cares

Definition: A *covert channel* is a path for the illegal flow of information between subjects within a system, utilizing system resources that were not designed to be used for inter-subject communication.

It might seem that such channels would be so slow that you wouldn't really care.

That's not true. Covert channels on real processors operate at thousands of bits per second, with no appreciable impact on system processing.

Covert Channels

The important characteristics of a covert channel are:

Existence:	is a channel present or not?
Bandwidth:	how much information can be transmitted per second?
Noiseless/noisy:	can the information be transmitted without loss or distortion?

It is usually infeasible for realistic systems to eliminate every potential covert channel.

Dealing with Covert Channels

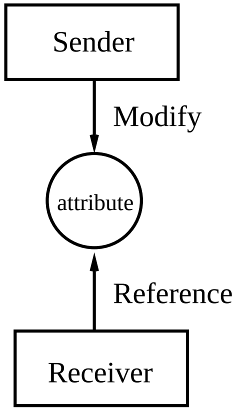
Once a potential covert channel is identified, several responses are possible.

- We can eliminate it by modifying the system implementation.
- We can reduce the bandwidth by introducing noise into the channel.
- We can monitor it for patterns of usage that indicate someone is trying to exploit it. This is *intrusion detection*.

Using a Covert Storage Channel

For a sender and receiver to use a covert *storage* channel, what must be true?

1. Both sender and receiver must have access to some attribute of a shared object.
2. The sender must be able to modify the attribute.
3. The receiver must be able to reference (view) that attribute.
4. A mechanism for initiating both processes, and sequencing their accesses to the shared resource, must exist.



Using a Covert Timing Channel

For a sender and receiver to use a covert *timing* channel, the following must be true:

1. Both sender and receiver must have access to some attribute of a shared object.
2. Both sender and receiver have access to a time reference (real-time clock, timer, ordering of events).
3. The sender must be able to control the timing of the detection of a change in the attribute of the receiver.
4. A mechanism for initiating both processes, and sequencing their accesses to the shared resource, must exist.

Lessons

- Important characteristics of any covert channel are: existence, bandwidth, and noisy/noiseless.
- Dealing with a covert channel may include: eliminating it, restricting the bandwidth, or monitoring it.
- Certain conditions must hold for a covert channel to exist.

Next lecture: Detecting Covert Channels