Foundations of Computer Security

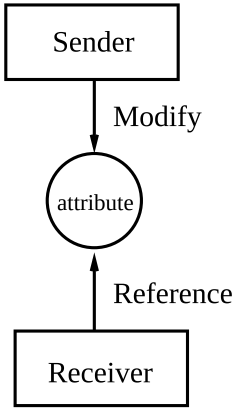
Lecture 16: Detecting Covert Channels

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

Finding Covert Storage Channels

Recall that several conditions must hold for there to be a covert *storage* channel:

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.


Sender
Modify
attribute
Reference
Receiver

Detecting Covert Channels

Richard Kemmerer (UC Santa Barbara) introduced the Shared Resource Matrix Methodology (SRMM). The idea is to build a table describing system commands and their potential effects on shared attributes of objects.

	READ	**WRITE**	**DESTROY**	**CREATE**
file existence	R		M	M
file size	R	M	M	M
file level	R		M	M

An R means the operation References (provides information about) the attribute *under some circumstances*. An M means the operation Modifies the attribute *under some circumstances*.

Note that this works for storage channels, not for timing channels.

A Subtlety of SRMM

Suppose you have the following operation:

CREATE (S, O): if no object with name O exists anywhere on the system, create a new object O at level L_S; otherwise, do nothing.

For the attribute *file existence*, should you have an R or not for this operation or not? Consider this: after this operation, you *know* that the file exists. *Why?*

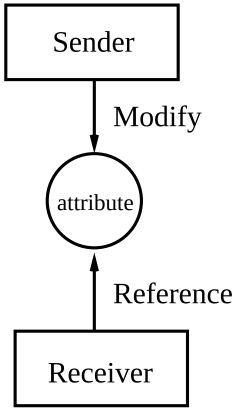
That's not enough. It's not important that you *know* something about the attribute; what's important is that the operation *tells* you something about the attribute.

Working with the SRMM

If you see an R and M in the same row, that indicates a *potential* channel. Why?

SRMM doesn't identify covert channels, but suggests where to look for them.

Any shared resource matrix is *for a specific system*. Other systems may have different semantics for the operations.



Sender

Modify

attribute

Reference

Receiver

Covert Channels and System Analysis

How might you use this methodology?

1. Use an access control policy like Bell and LaPadula to control standard information flows.
2. Use a separate technique like Kemmerer's SRMM to identify covert channels.
3. Deal with covert channels by closing them, restricting them, or monitoring them.

Lessons

- Kemmerer's Shared Resource Matrix Methodology provides a systematic way to investigate potential covert channels.
- However, using it effectively requires a lot of knowledge about the semantics and implementation of system operations.
- Covert channel analysis can be used to close some of the security holes of an access control policy like BLP.

Next lecture: Non-Interference