Foundations of Computer Security

Lecture 17: Non-Interference

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

Communication

Recall that earlier we said:

> *If S_L ever sees varying results depending on varying actions by S_H, that can be used to send a bit of information from S_H to S_L.*

That applies whether the action by S_H is to write into a file or to modulate some system attribute.

If security demands that S_H must never communicate with S_L, there shouldn't be *anything* that S_H can do that has effects visible to S_L.

This observation is the basis of a very general security policy called *Non-Interference*.

Non-Interference

Non-Interference is the best known instance of a class of policies called *information flow* policies.

Rather than constraining subject actions, we specify which subjects are allowed to "interfere with" which other subjects.

You can think of "interfere with" as meaning "do something that has an effect visible to."

Specifying Non-Interference

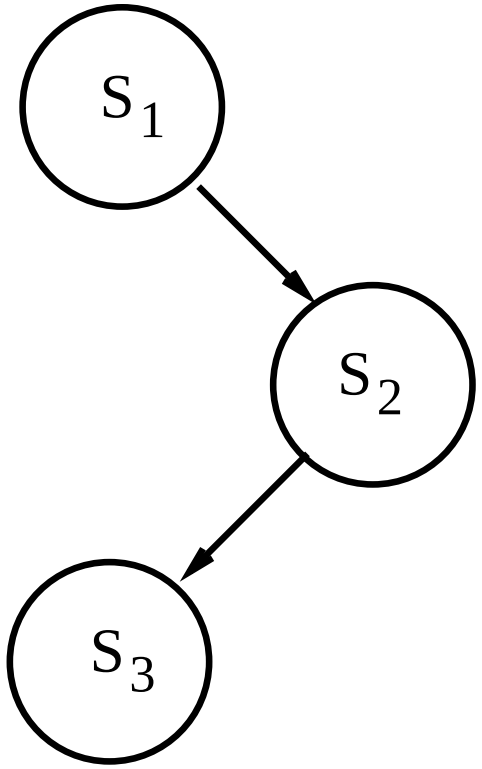
The system *policy* is a reflexive binary relation ($a \mapsto b$) over the subjects of the system that says which subjects are permitted to "interfere with" which other subjects.

For example, given subjects S_1, S_2 and S_3, a potential non-interference policy is:

$$S_1 \mapsto S_2, S_2 \mapsto S_3,$$

graphed to the right.

Since $\mapsto$ is reflexive, we don't bother to specify the additional clauses: $S_1 \mapsto S_1$, $S_2 \mapsto S_2$, and $S_3 \mapsto S_3$.



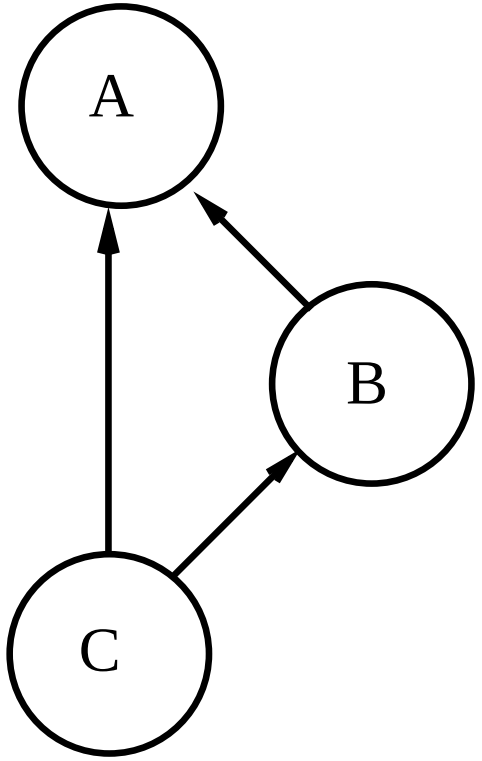
MLS to Non-Interference

It is possible to take *any* MLS policy and turn it into a Non-Interference policy.

A BLP system with subjects:

- A at **(Secret: {Crypto, Nuclear})**,
- B at **(Secret: {Crypto})**, and
- C at **(Unclassified: { })**.

yields the NI policy on the right.



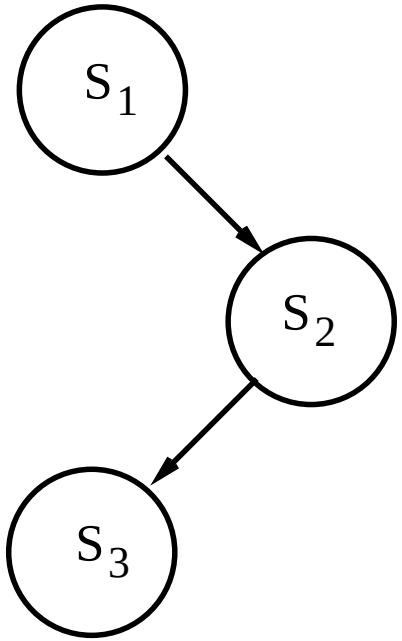
In general, $S_i \mapsto S_j$ if the level of S_j dominates the level of S_i. Think about why that's so.

MLS and Non-Interference

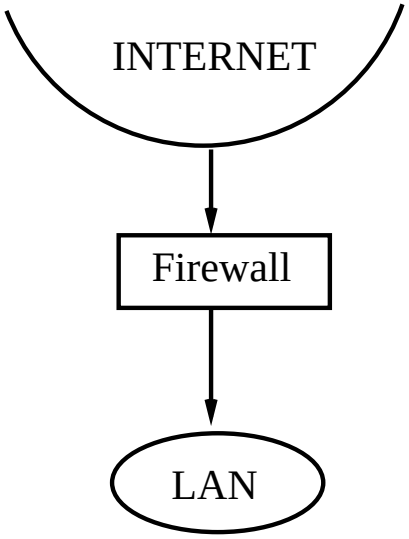
It is *not* true that any Non-interference policy can be reformulated into an MLS policy.

For example, the NI policy on the right is not transitive, since there is no arrow from S_1 to S_3. All MLS policies are transitive by definition.

Would anyone ever want a non-transitive policy?



Non-Transitive Policies



Consider, a firewall system that mediates all traffic from the Internet into your LAN.

The appropriate policy is:

$$\text{INTERNET} \mapsto \text{Firewall}$$
$$\text{Firewall} \mapsto \text{LAN}$$

We explicitly don't want a channel from the Internet directly into the LAN. But there's no way in MLS to specify this policy.

Lessons

- Non-interference is an *information flow* policy, meaning that it specifies the security of the system by stating which flows are allowed.
- The policy is specified by a reflexive relation over the subjects of the system stating which can "interfere" with which others.
- NI is very general. Any MLS policy can be rewritten as an NI policy, but not vice versa.

Next lecture: Non-Interference II