

Information Flow security

February 20, 2014

1 A lattice model of secure information flow

Motivation Traditional way of dealing with information flow security is based on simple “no read up, no write down” policy, a.k.a. BellLaPadula model. Here the structure is simple. Denning noticed that the structure is a lattice and generalize the information flow to be able to apply on many different situations.

Difference between Information Flow and Access Control Access Control policy is to make sure that directly access to certain object is controlled, without caring about the potential information flow between different objects. Information flow policy focus on how sensitive information can be passed between entities. For example, access control policy can have such a rule:

A has access to B and B has access to C while A do not have to C.

However, Information flow policy will say it is not valid because of the transitivity.

explicit flow, implicit flow and covert flow Let consider this example: `If (x) then y=z;`. Here `y=z` has an explicit information flow from `z` to `y` by the assignment. However, there is an implicit flow from `x` to `y`, because the value of `x` can determine the value of `y`. Program transformation is robust to explicit flow while not implicit flow.

Difference between implicit flow and covert flow: If we view programs as black box taking input and producing output, for a program without implicit/explicit flow, alternating High input will not change the output. If other changes can be observed because of the change of input, e.g. time to finish, power consumption, etc, they are called covert flow.

More discussions

1. Lattice model make sense in reality because of transitivity reflective, anti-symmetry properties.
2. `q = *p` has two information flows.

3. Information flow can appear without assignment. e.g., `if (h > 5) l = 1`

2 Language-based information flow security

Noninterference Attacker cannot observe the difference of confidential output between different input. This is a finer grind definition of information flow security and is the real rule to ensure.

Discuss on equational security property Program C is secure iff for any input state, the following two cannot be distinguished:

1. set h to arbitrary value; run C; set h to arbitrary value.
2. run C; set h to arbitrary value.

We will talk more on termination based leakage and noninterference next lecture.