838G April - 8 - Chang Liu

Paper 1: Quantification

Andrew: (describe this paper)

Mike: can the graph has loop?

Kris: no

The graph represents the execution rather than the code.

Mike: Why annotation?

JP: for precision

Andrew: Line 7 should be a for loop rather than a while loop.

Mike: What are the capacity?

x=*p

Aseem made some comments I didn't follow.

Why min-cut?

Because any cut provides an upper bound to the number of possible outputs. The min-cut gives the tightest bound.

if (guess=pwd) then ok
else reject

This is 1-bit information capacity leakage. But from the entropy point of view, it is different. If the result is ok (worst case), then all information is leaked!

Why is this still useful?

In the example, the method works because there is few implicit flows.

Ignoring the distribution is a bad idea.

Chang: This capacity notion is both an overestimate and an underestimate. One possible reason for such a notion is for efficiency.

Mike: but efficiency is only a concern when we need to compute it. If it is not the thing we need to compute, then efficiency is meaningless.

Paper 2: Measuring Channel Capacity

Mike: What is the difference?

Andrew: the attacker can influence on the program counter.

Mike: This paper doesn't assume to run the program only once. The attacker can run the programs multiple times over different inputs.

Xiao: The program must be a straight-line program.

Andrew: is there a connection between them? They are doing similar things.

Mike: why loop on secret input is ok? suppose the analysis choose certain secret inputs, is that an underestimate or an overestimate?

It's an underestimate.

Mike: why it ends up PLAS?