Quantitative Information Flow and Side Channels

Instructor: Tevfik Bultan

Lecture 1
What is a side channel?
What is a side channel?

TIME
Monday, Aug. 13, 1990
And Bomb The Anchovies
By Paul Gray

Delivery people at various Domino’s pizza outlets in and around Washington claim that they have learned to anticipate big news baking at the White House or the Pentagon by the upsurge in takeout orders. Phones usually start ringing some 72 hours before an official announcement. "We know," says one pizza runner. "Absolutely. Pentagon orders doubled up the night before the Panama attack; same thing happened before the Grenada invasion." Last Wednesday, he adds, "we got a lot of orders, starting around midnight. We figured something was up." This time the big news arrived quickly: Iraq’s surprise invasion of Kuwait.
What is a side channel?

Delivery people at various Domino’s pizza outlets in and around Washington claim that they have learned to anticipate big news baking at the White House or the Pentagon by the upsurge in takeout orders. Phones usually start ringing some 72 hours before an official announcement. "We know," says one pizza runner. "Absolutely. Pentagon orders doubled up the night before the Panama attack; same thing happened before the Grenada invasion." Last Wednesday, he adds, "we got a lot of orders, starting around midnight. We figured something was up." This time the big news arrived quickly: Iraq's surprise invasion of Kuwait.
What is a side channel?

Delivery people at various Domino's pizza outlets in and around Washington claim that they have learned to anticipate big news baking at the White House or the Pentagon by the upsurge in takeout orders. Phones usually start ringing some 72 hours before an official announcement. "We know," says one pizza runner. "Absolutely. Pentagon orders doubled up the night before the Panama attack. Same thing happened before the Grenada invasion." Last Wednesday, he adds, "we got a lot of orders, starting around midnight. We figured something was up." This time the big news arrived quickly: Iraq's surprise invasion of Kuwait.
What is a side channel?
What is a side channel?

- **Confidentiality**: A program that manipulates secret information should not reveal that information.
- **Confidentiality can be hard to achieve**
  - Especially if an attacker is able to observe different aspects of program behavior such as execution time and memory usage.
- **Side-channel attacks** recover secret information from programs
  - by observing non-functional characteristics of program executions
    - such as execution time, memory usage, memory accesses, or packets transmitted over a network.
Information leakage

if (password==guess) grant_access(); else print_error();

- This code leaks information about the secret password
- It leaks the information through the main channel (the output) of the program
Information leakage

In many cases some leakage is unavoidable:

- Any password checker leaks some information about the password
- Consider an electronic voting application, the result of the vote is public and it does leak information about the votes, but still individual votes should be private.
Information leakage

- One common way to model information leakage in programs is to separate the inputs and outputs of the program to different security levels.

  High: highly classified (secret)
  Low: not highly classified (public)

- Then confidentiality means that information about High values should not be leaked to Low values.
Non-interference

- Having no information leakage is characterized as non-interference, which means that:

  High values have no influence on Low values
Non-interference

- Let us assume that:
  - a program is a function from High and Low input values to High and Low output values where
  - $f_L$ denotes the function that maps High and Low input values to the Low output value
  - $H$ and $L$ denote the domains of High and Low values

Then, we can state non-interference property (for deterministic programs) as:

$$\forall h_1 \in H, h_2 \in H, l \in L : f_L(h_1, l) = f_L(h_2, l)$$
Information leakage

- Non-interference for main channel can be checked using dependency analysis techniques:
  - Determine data and control dependencies among High and Low values and make sure that Low values do not depend on High values)
  - Determining non-interference for side-channels could be more difficult to figure out
Information leakage

- As we discussed, for many practical cases (such as password checking or electronic voting) non-interference is simply not possible and some information leakage from High values to Low values is unavoidable.
Information leakage

- If leakage is unavoidable, then the question becomes:
  - “How much information is leaked?”
- For example, how much information about password can be obtained by the attacker who can enter different password guesses to the program
- If the amount leaked is very small, the program might be considered secure even though there is some information leakage
Quantitative information flow

- The goal of quantitative information flow techniques is to quantify the amount of information leaked from a given program.

- Quantitative information flow techniques can also be used to detect the amount of information leaked from side channels.