

Opening Report

1 组 Topic: Information Flow & Covert Channel

1. Understanding about topic

After the Great Flood, with shared language, human beings worked together to build a tower that leads to heaven. In order to stop the plan, God force humans to speak distinct languages, so that human beings can't communicate with each other. The plan failed, and humans are scattered all over the world.

— "Old Testament-Genesis"

Since the opening of the universe and the birth of mankind, the spread of information plays an extremely important role in the development of civilization and the course of history. Basing on global history, the world pattern of modern world was determined when the technology of finding directions at sea and steel production flows from the East to Europe. On the rise and fall of a surname, Cai Lun reformed papermaking, which reduced the cost of information dissemination and broke the monopoly of the dynasty on knowledge, leading to the collapsing of the strong Han Empire. At the root of all these, they are due to the flow of information.

For thousands of years, mankind has never stopped exploring the flow of information. With the invention of computers and the Internet, the speed of information collection, processing and transmission has grown exponentially, and the way information is transmitted has become more diverse. In addition to the channels that are designed to convey information, people use other methods to convey information implicitly, which is called covert channel.

Explain these two nouns with modern computer science, information flow means the transmission of information from one place to another in both absolute and probabilistic ways. There are two principles. Confidentiality refers to what subjects can see what objects AND Flow controls what subjects actually see. We can guarantee it through two ways. One is complier-based and the other is execution-based. For example, we can use declaration to specify what security classes it belongs to. But it may be too strict to deal with numerous data in our daily life and cause some implicit flows. Fortunately, Data mark machine and run-time checking can be a miracle in these problems.

While Covert Channels is a path of communication that was not designed to be used for communication. It's really hard to observe. Let alone the elimination. Lots of ways can cause leak of data such as Data hiding in TCP/IP, Lan environment, OSI model and so on. Two relatively old techniques remain the standards for locating potential covert channels. One works by analyzing the resources of a system and other works at the source-code level.

During this lesson, our teacher gave us an example about the information flow which shows what malicious information flow could do, in this example, it could be used to transform

information from higher security level to lower security level by periodically using system resource to do some calculation, so it actually could bypass some of the database security measures. In this example, attacker actually could find some covert channels, which means the path of communication that was not designed to be used for communication. There are two kinds of covert channel, one is the storage covert channel and the other is the timing covert channel, here the attacker actually used a timing covert channel which modulate its own system resource and affect response time. From this aspect, we could know that some information flow could cause the leak of information, so we need to find measures to identify such things and stop them. We also know that totally stop the covert channel isn't always realistic, because this may also affect the efficiency of the system used by normal users, but we could slower the covert channel and lower the efficiency of leaking. It couldn't prevent the leak from happening but this could keep the secret for some time, therefore could solve the problem about saving some information which is time-critical.

As a result, the topic can convert into two parts:

1. How can programs or compilers limit illegal information flows, in order to guarantee the security and validity of programs.
2. How can we identify covert channels and prevent our data from leak.

Here we are to discuss about the latest progress in information flow and introduce different approach to mitigate the bad effects of Covert Channels. These subjects have already been presented during the class but we will go quite deeper. We will answer the questions in the end of PPT with our own interpretation towards information security.

2. Tasks flow

- i. Preliminary inquiry and understanding of information flow and covert channel
- ii. Search for related papers and layer their content and expand
- iii. Submit preliminary draft before the speech
- iv. Discuss the content and form of the speech
- v. Make a PPT for the presentation and simulate rehearsal
- vi. Discuss the parts of the report that need to be improved
- vii. Improve the preliminary draft and complete the final paper

3. Work distribution

work	manager
Making the PPT	王钟毓
Giving the speech	孔成俊
Overall planning and Inspect the report	彭子帆
Writing the report	陈宇威
	惠铭康
	韩卓均
	王鹏
	李宇璇

4. Schedules

task flow	date
Understand the topic	3.24
Review the paper	3.24—讲前 5 天
submit the draft	讲前两天
make the ppt	讲前一天
give a speech	暂未定
perfect the report	4.16