Nanyang Technological University

AY2021-2022 Semester 2

CE/CZ4067 SOFTWARE SECURITY

Tutorial 1: Side Channels and Covert Channels

1. In computer security, side-channel attacks are common threats to computer systems.

   (a) Explain what a side-channel attack is.

   (b) Which security goal is compromised by a side-channel attack?

   (c) List at least three examples of side-channel attacks.

2. Covert channel is a related concept. It is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.

   (a) What is the key difference between side channels and covert channels?

   (b) Give an example of a covert channel.

3. A CPU cache is a hardware cache used by the central processing unit (CPU) of a computer to reduce the average cost (time or energy) to access data from the main memory [2].

   (a) Recap what a CPU cache is and how it works.

   (b) Investigate cache-based side-channel attacks on the Internet and explain how they work in your own words. You may refer to these examples [3, 1].

References

[1] Jicheng Shi, Xiang Song, Haibo Chen, and Binyu Zang. Limiting cache-based side-channel in multi-tenant cloud using dynamic page coloring. In *2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pages 194–199. IEEE, 2011.

[2] Gabriel Torres. How the cache memory works, September 2007.

[3] Zhenghong Wang and Ruby B Lee. New cache designs for thwarting software cache-based side channel attacks. In *Proceedings of the 34th annual international symposium on Computer architecture*, pages 494–505, 2007.