Read more about covert channels

Covert channel is a path of communication not designed to be used for communication.

Feels like steganographic technique of sending information.

Covert channels are communication methods used to transfer information in a way that is not intended or designed for communication by the system. In computer security, covert channels are typically used to breach security systems by bypassing security mechanisms, such as firewalls or network monitoring systems, which are designed to prevent unauthorized access or data leaks.

1. **Storage Channels**: These involve the indirect communication of information by modifying a storage location. For instance, one process may write data to a file or a specific memory location, which another process then reads. The reading process interprets the data in a manner that was agreed upon beforehand.
2. **Timing Channels**: These channels leverage the timing of events to communicate information. For example, one process may influence the timing of another process's actions (like the time it takes to complete a task) to send signals. The receiving process then observes these timing variations to decode the message.

Covert channels can be quite sophisticated and are often hard to detect because they utilize normal system functions in unintended ways.

They are a significant concern in systems where security is paramount, such as in government or military applications. Detecting and mitigating covert channels often requires careful system analysis and monitoring.

Secret information of a company.

Covert channels piggyback. Ride on someone else’s work.

Confinement problem – problem of preventing server from leaking information user of service considers confidential.

How to communicate between 2 laptops. They have underlying hardware in common.

A process that cannot be observed and cannot communicate with other processes cannot leak information. This is total isolation.

Firewalls –

DMZ