Levi Seibert

00086809

lseiber1@my.athens.edu

ITE 523 – Dr. Yahia Fadlalla

Covert Channels

In the field of data communications, there are two main types of communication channels: overt channels and covert channels (a channel is a means of sending data). Overt channels are communications that are obvious and work as expected. Covert channels are the opposite, they are communications that occur behind the scenes (not in a good way) and are obscured from common view. The goal of covert channels is to allow communications to occur undetected in order to allow for malicious access.

The main application of covert channels is their use in avoiding access controls for databases, specifically those with hierarchical security rankings, in which different parts of the database are available to a user depending on the credentials of the user. Many of these databases are used to store confidential information for national security/military purposes, and obviously not just anyone should have access to this information. Instead, there must be an authentication procedure in place in order to associate the right object with the right subjects. The database is protected by the Database Management System controls (DBMS) that assign objects (database entities) to each subject (process accessing the database). The DBMS are defined using an access control matrix that contains labels for each subject/object combination in order to determine the clearances granted to each authenticated user [1].

Covert channels are communications that transfer data in such a way that they violate the security policy of a system by sending data in a way that is not expected, but without being detected. There are two main types of covert channels: storage channels and timing channels. A storage channel is a channel that sends unauthorized data via an object that can be written to (legally according to the security policies in place) and read by a different process, also in a legal manner, using a shared storage location [1, 2]. Because these data transfers occur outside the normal expected channels, there are often no security policies in place to prevent them. Timing channels differ in that they do not explicitly write data to a process but rather signal processes in such a way that their response times (or similar observable data) convey a message that can be determined by another process [1]. Covert channels can also be considered as falling into two camps: stand-alone, local systems (where separate processes on a single system communicate at different security levels) and the more common option, network-based systems [2].

Covert channels are a difficult problem to deal with and have major associated dangers. One of the most common threats with covert channels is the capability of "leaking" information to unauthenticated or lower-authenticated users. For example, assume there is a protected database that stores data for subjects with clearance classifications of UNCLASSIFIED, CONFIDENTIAL, SECRET, and TOP SECRET. An unauthenticated user shouldn't have access to any of the information in the database and actual users should only be allowed to view data corresponding to their classification or lower (with TOP SECRET obviously being the highest clearance). If a SECRET user wanted to leak SECRET information to a UNCLASSIFIED user, then they could use a covert channel, either via timing signals or through storage channels, to provide the information to the lower-ranking user without being caught. To make matters a bit more complex, many DBMSs have need-to-know categories in addition to their security classifications, thus making the access control matrix and, as a consequence, the differences between different classifications of users, more intricate. A database of this type is referred to as a Multi-Level Secure system or MLS. With an MLS, there are even more avenues for leaks, as there will be additional discrepancies between users and their authentication levels, and therefore, a need for stronger security [1].

Although most examples of covert channels involve security clearances and military information, covert channels are not solely a security/military issue. Rather, they can be used to obscure communications on many different types of channels. It really comes down to any situation when a user shares information, access, or privileges with another user who is not allowed to have the same rights. An unauthenticated user may be able to steal (borrow, share, etc.) music from a streaming service via an authenticated user, for example.

As described in [2], covert channels are a major issue, especially in today's technological world. The increase in cloud computing, virtualization, and Internet of Things devices is causing major intensifications of the covert channel issue. On top of the hardware/device threats, there is also a problem with protocols and micro-protocols (some of which can switch in form during a communication) being used in significant ways to make identification of covert channels even more difficult [2]. As [1] points out, covert channels are inevitable; there is no way that they can all be removed. Instead, the goal of designers and cybersecurity subject matter experts should be reducing the amount of possibilities for covert channels and finding ways to identify them before they do their damage.

Covert channels are very hard to recognize as they are designed to be undistinguishable by a normal human user (after all, they are supposed to be covert). The key word in the previous sentence is “human”. Humans are not very good at identifying differences in patterns and behaviors, but machines are. The solution to covert channels will likely lie in the hands (or circuits) of computers. There have been some studies performed that indicate that Machine Learning can identify abnormalities in network traffic better than humans and thus are able to discover covert communications [2]. As the artificial intelligence world continues to grow, it can only be expected that the capabilities of these systems will also increase and “robots” will be the solution to preventing unauthorized accesses.

On the other hand, there is a potential that artificial intelligence could be used negatively in the case of covert channels. Once again, computers have a knack for outperforming humans in certain aspects. There is a potential that ML algorithms could be used to create a covert channel that is multidimensional and undetectable by most humans, and even defensive AI systems. Hopefully this will not be the case, but it does bring up the potential of having AI robots become leakers of confidential information, a concept that is not commonly considered but would have major repercussions. If an artificial intelligence system finds something of interest in a data channel and there is a large enough “reward” available for the information, would the system know to keep the data private? This leads to an even deeper question regarding whether or not computer devices can make “moral” choices, or will they always select a pathway that leads to the greatest gains for themselves? This is a concept that needs to be further investigated and could be the foundation for many research studies in the future.

Covert channels can almost be thought of as a man-in-the-middle attack, where the attacker is in alliance with one of the communicating ends, usually the client in a client-server setup. This doesn’t quite hold true; however, because the client is actually working maliciously, and therefore the attacker does not work alone. Instead, covert channel attacks should be thought of more as a team-worked attack, with at least one participant being an insider to the data (so that the data itself can be legally accessed and not raise any alarms). Identification of guilty parties is more difficult than in normal cyberattacks, as multiple entities have to be found and proven to be working together.

References

[1] Y. A. Fadlalla, “A Cryptographic Approach to Resolving the Storage Covert Channel Problem,” *APICS*, 2003.

[2] M. A. Elsadig and Y. A. Fadlalla, “Network protocol covert channels: Countermeasures techniques,” *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, 2017.