Mario J. Lorenzo
mario@mjlorenzo.com

February 2020

Covert Channels as Leakage Points in Information Systems

The ability to secure an organization's IT systems and network resources is integral to safeguarding the organizations sensitive information. Securing an organization requires a comprehensive approach that secures all layers including physical location, hardware, software, networking, and personnel. The Rand report identifies the areas of vulnerabilities throughout these layers of a computing environment as leakage points (Ware, 1970). The report discusses the various threat vectors that system designers should consider when designing resource-sharing systems.

One such leakage point involves the use of covert channels used to transmit information using unconventional methods through optical, thermal, or acoustic mediums (Zander, Armitage, & Branch, 2007; Lampson, 1973). This technique involves the use of devices such as LEDs, speakers, displays, or CPUs to modulate a signal that is received by another device that may be disconnected (i.e. isolated) from the network. Secure computing networks, such as the Joint Worldwide Intelligence Communications System (JWICS), used by military and government agencies to share sensitive information are typically isolated from other networks such as the internet (Guru, Zadov, Daidakulov, & Elovici, 2018). Some very secure systems are physically isolated from all other systems, referred to as air-gapped, because there is no network connection connecting them to another computing device. For intruders to exfiltrate information from these air-gapped systems they must use covert channels such as hard-drive LED (Guri et al, 2016), LED displays with steganography (e.g. hidden within an image) (Guri et al, 2016), or Smartphone display brightness and volume (Chandra, Lin, Kundu, & Khan, 2014).

All these covert channels have numerous limitations such as low data rates, or requiring close-proximity, or establishing line-of-sight between the transmitter and the receiver device. Schmidt, Hanspach, & Keller (2015) present a case study on the theorical and practicality of leveraging covert channels for data exfiltration. Their work demonstrates the reasonably high data rates that can be attained by covert channels.

Another variation of the optical covert channel investigated by Guri et al (2018) involves the use of a network routers LED to transmit information to a nearby camera or even a drone hovering outside an office building. Their work demonstrated high transfer rates by leveraging multiple LEDs on the router to increase the throughput (bandwidth) of data transfer reaching speeds up to 960 bit/sec when using 8 LEDs concurrently. Guri et al (2018) also demonstrated the ability to conceal the activity by blinking the LED at 5,800 blinks per second making it unperceivable to the human eye and reducing the chances of detection by IT staff.

Of course, these techniques require some malicious programs to run within the target device and therefore require other leakage points in order to establish control of the optical device. Ware (1970) in the Rand report describes this as Leakage Point Ecology where other vulnerabilities in software, hardware, or the organizations personnel are used to deploy the malicious program. Guri et al (2018) describe several case studies where the use of cleaning staff (described as “The Evil Maid”) are used to install a program that can then propagate itself throughout the secure network until a target device is identified. This attack also requires the use of an optical sensor such as a smart phone camera or body cam to receive the information.

Another point of vulnerability involves a supply-chain infection where a network router is infected with the malicious program prior to it being acquired by the organization. Guri et al (2017) cite several related examples including the infection of USB thumb drives at an electronic store near NATO headquarters in Kabul, Afghanistan. The sophisticated attack was able to breach the military JWICS network after a NATO employee inserted the compromised USB drive into a secure system. Other examples include known vulnerability to certain Cisco routers or potential backdoors in Huawei networking equipment (Guri et al, 2017). One news article alleged that the National Security Agency was tampering with U.S. made routers (Greenwald, 2014). Such tampering can lead to vulnerabilities that can then be used at a later point to penetrate a secure network and deploy malicious code that use a covert channel to exfiltrate data out of an air-gapped computer system.

Guri et al (2017) mentions the case of the infamous “Stuxnet” attack where malware was widely dispersed throughout a region where Iranian scientist lived in order to infect a device such as a laptop or USB device that would later be connected to the secure uranium enrichment facility. This malicious program then propagated itself until it reached its intended target and adversely impacted equipment and sensors used to enrich uranium. A similar attack vector can be devised to instead exfiltrate data for government or corporate espionage.

Covert channels remain a relevant point of vulnerability in modern computing environments and a viable field of research. The field of research can include the exploration of new mediums, increased data rates through improved sensors, QoS improvements through error detection and error correction algorithms, as well as countermeasures for detecting and preventing covert channels. The recent emergence of drones has revived the focus on optical covert channels due to the ability for a drone to breach a physical perimeter to collect information from cover transmitters.

A proposed plan of research may include the use of a multi-sensor device that can be used as a countermeasure to detect and interrupt these covert channels. Such a device would feature acoustic, optical, and thermal sensors and may be installed in rooms where sensitive computer equipment exists. This hypothetical device could leverage modern pattern recognition algorithms including Deep Learning techniques to monitor and detect a possible covert transmission and then interrupt that transmission by flooding the medium with noise. This research could devise controlled experiments using baseline implementations for an optical channel such as LED-it-GO (Guri et al, 2017) or Acoustic channel (Guri et al, 2016) and demonstrate that the countermeasure device can detect the communication and interrupt the communication. Such an experiment would likely be narrowed down into several investigations each focusing on a single medium type and separately assessing the ability to detect and the ability to interrupt these covert transmissions.

References

Guri, M., Zadov, B., Daidakulov, A., & Elovici, Y. (2018, August). xLED: Covert data exfiltration from air-gapped networks via switch and router LEDs. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)* (pp. 1-12). IEEE.

Lopes, A. C., & Aranha, D. F. (2017, February). Platform-agnostic Low-intrusion Optical Data Exfiltration. In *ICISSP* (pp. 474-480).

Guri, M., Zadov, B., & Elovici, Y. (2017, July). LED-it-GO: Leaking (a lot of) data from air-gapped computers via the (small) hard drive LED. In *International conference on detection of intrusions and malware, and vulnerability assessment* (pp. 161-184). Springer, Cham.

Guri, M., Hasson, O., Kedma, G., & Elovici, Y. (2016, December). An optical covert-channel to leak data through an air-gap. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)* (pp. 642-649). IEEE.

Guri, M., Solewicz, Y., Daidakulov, A., & Elovici, Y. (2016). Diskfiltration: Data exfiltration from speakerless air-gapped computers via covert hard drive noise. *arXiv preprint arXiv:1608.03431*.

Guri, M., Hasson, O., Kedma, G., & Elovici, Y. (2016). Visisploit: An optical covert-channel. *arXiv preprint arXiv:1607.03946*.

Schmidt, W., Hanspach, M., & Keller, J. (2015). A case study on covert channel establishment via software caches in high-assurance computing systems. *arXiv preprint arXiv:1508.05228*.

Chandra, S., Lin, Z., Kundu, A., & Khan, L. (2014, September). Towards a systematic study of the covert channel attacks in smartphones. In *International Conference on Security and Privacy in Communication Networks* (pp. 427-435). Springer, Cham.

Greenwald, G. (2014). How the NSA tampers with US-made Internet routers. The Guardian, 12.

Zander, S., Armitage, G., & Branch, P. (2007). A survey of covert channels and countermeasures in computer network protocols. *IEEE Communications Surveys & Tutorials*, *9*(3), 44-57.

Lampson, B. W. (1973). A note on the confinement problem. *Communications of the ACM, 16*(10), 613-615.

Ware, W. H. (1970). *Security controls for computer systems* (Vol. 609). RAND CORP SANTA MONICA CA.