UNIDIRECTIONAL DATA TRANSFER: A SECURE SYSTEM TO PUSH THE DATA FROM A HIGH SECURITY NETWORK TO A LOWER ONE OVER AN ACTUAL AIR-GAP

Atila Bostan, Department of Computer Engineering, Atılım University, Ankara, Turkey
Email: *atila.bostan* @atilim.edu.tr
Gökhan Şengül, Department of Computer Engineering, Atılım University, Ankara, Turkey
Email: *gokhan.sengul@* atilim.edu.tr
Murat Karakaya, Department of Computer Engineering, Atılım University, Ankara, Turkey
Email: *murat.karakaya@* atilim.edu.tr

ABSTRACT

The term "air-gap" is typically used to refer physical and logical separation of two computer networks. This type of a separation is generally preferred when the security levels of the networks are not identical. Although the security requirements entail parting the data networks, there is a growing need for fast and automatic transfer of data especially from high-security networks to low-security ones. To protect security sensitive system from the risks originating from low-security network, unidirectional connections that permit the data transfer only from high to low-security network, namely information-diodes, are in use. Nonetheless, each diode solution has its drawbacks either in performance or security viewpoints. In this study, we present a unidirectional data transfer system in which the primary focus is data and signal security in technical design and with a plausible and adaptable data transfer performance. Such that the networks do not touch each other either in physically or logically and the transfer is guaranteed to be unidirectional. Apart from avoiding the malicious transmissions from low to high-security network, we claim that the proposed data diode design is safe from emanation leakage with respect to the contemporary sniffing and spoofing techniques.

Keywords –data security, data diode, information diode, air gap, signal security, multi-level security networks.

1. INTRODUCTION

Central to the proliferation of automatic information-processing is the ease and speed of information and data sharing achieved by this technology [1]. In contemporary information processing systems it is hard to find one which does not share any information (import or export) with some others [2]. Hence an information system is generally supposed to be exporting or importing information in a given configuration. When a system is connected to other one or a network of systems then several security considerations rise. Thus secure ways of information sharing and access should be developed. Nevertheless, security is generally deemed to be a hurdle against information and data dissemination or access [3]. In the current state of the information technologies there are considerable number of security tools and configurations which aims to secure information access and usage [4,5,6]. However, common understanding is that when a systems shares the information with some others the security risks come out as well.

Aside from the other security considerations in information sharing, in this study the focus is on the security mechanisms in transferring the data from one system to another. Although the definition of subject matter sounds like the data transfer is one-way, readily available data communication technologies, by default, necessitate two-way communication infrastructure [7,8]. Since in most of the communication protocols acknowledgements, which informs the successful delivery of the transmissions, play an important role. While there are several transport layer services and applications that transmit or receive only [9, 10], they generally run on a duplex communication infrastructure. Furthermore, unless the transfer of signal is assured to be one-way on physical layer, merely transmitting the data from one system to another on transport or application layer does not guarantee that the system is safe from security risks which stem from the other peers or from the network connected. Malicious incidences were generally detected to be covertly exploiting the available channels in the infrastructure used [11, 12, 13]. Hence, in order to be safe from clandestine attacks it is better to nullify the infrastructure that they can utilize.

On the other hand signal emanation security is another dimension when two systems with different security levels run within close perimeters. There are technical and physical measures developed to prevent spying on leaking emanations. The most commonly accepted and referred set of standards in this area is named TEMPEST. TEMPEST's name is believed to have been a code name used during development by the U. S. government in the late

1960s, but at a somewhat later stage, it became an acronym for Telecommunications Electronics Material Protected from Emanating Spurious Transmissions [14]. In essence, TEMPEST defines the minimum set of technological and physical measures to be followed in order to be safe from leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations [15].

In this study, we present our design of an information diode that allows only one way of a data transfer and can be configured to comply with TEMPEST standards as well. In the following section we present the design and configuration of proposed system. In the conclusion section the advantages and future work were reported.

2. SYSTEM DESIGN

The system has three core components, these components are; high-end-unit, transfer-unit and low-end-unit. Conceptual relations between these three components are depicted in Figure 1, below.

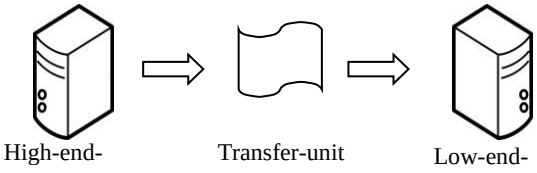

Figure 1. The components of the system.

High-end-unit is a computer which is connected to the high security part of the network and operating under the high-security configurations. Additionally, this unit is connected to the transfer unit over an input/output interface other than the one used to connect the security-high network infrastructure. In essence, the addressing, forwarding and communication protocol should better be different than that of the ones used in high-security network. So that the data traffic on security-high network may not be easily forwarded to the transfer-unit without using proper conversion mechanisms and having physical connection.

Transfer-unit a customized hardware and software component which guaranties the information flow is one way. This unit consists of two physical hardware parts with the actual air gap in between. While one of the hardware components is connected to high-end-unit, the other one is connected to the low-end-unit. Details of the transfer unit and the connection over physical air gap are explained in section 2.2.

Low-end-unit is a computer which is connected to low-security network and running under compatible configurations with this network. Low-end-unit has a connection with the transfer unit over an input/output interface other than the one used to connect to the low-security network. So that the data traffic on low-security network may not be easily forwarded to the transfer-unit without using proper conversion mechanisms and having physical connection

Moreover, on each component there are special service software running. Detailed designs and configurations of the three components are described in the following sections.

2.1 High-End-Unit

This component is responsible to identify, filter and direct the data that will be transferred to low-security network. Depending on the preferred services, it plays a communication-gateway role for the other hosts on high-security network. Other hosts should address the data that is to be transferred to low-security network to high-end-unit on high-security network. The high-end-unit should be functioning as an application-proxy for the preferred applications running on the high-security network.

High-end-unit should be capable to identify and filter data that is received and further to be relayed to transfer-unit. In order to successfully deliver the data to the transfer-unit, it must have well-suited transport services as well. Conceptual design of the modules and data flow in high-end-unit are shown in Figure 2.

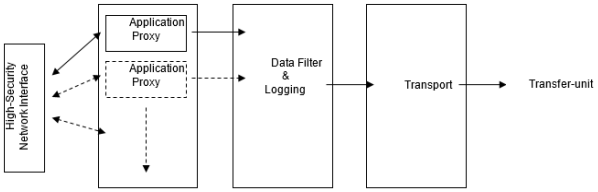

Figure 2. High-end-unit conceptual design

Application proxies should be capable to convey the received message (not data) to the data filter in a custom format that has the destination address and the communication content together. Afterwards, data filtering and logging module scan the message and record for achieving purposes. Finally, the message should be processed by a custom transport service which is running a special communication protocol with the transfer-unit.

2.2 Transfer-Unit

Transfer-unit consists of two hardware components. The one which has a cable connection with high-end-unit is named as transmission-part. The other one which has a cable connection with low-end-unit is named as receiver-part. Transmission-part has transport module which is facing towards the high-end-unit and an optical transmitter. On the other hand, the receiver-part has optical sensor and transport module which is facing

towards low-end-unit. Schematic diagram of transfer unit is shown in figure 3.

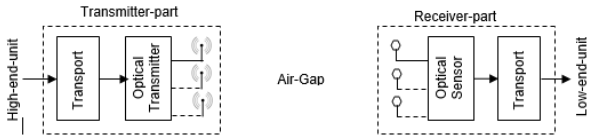

Figure 3. Transfer-Unit conceptual design.

The transport module in the transmitter-part is responsible to communicate with the high-end-unit by using special communication protocol. Whereas the transport module in receiver-part is responsible to communicate with low-end-unit by using the customized protocol as well. Optical transmitter and sensor units should have at least a pair of optical transmitter and sensor devices, but may have several pairs in parallel. Important point in this design is that the transmitter-part can only transmit, while the receiver-part can only receive signals, as they do not have the other physical devices. Therefore, this design guaranties one way information (signal) flow on physical layer.

With the purpose of having faster transfer speed, the number optical transmitter and sensor device pairs may be increased. Otherwise, single pair transfer speed will be limited with a one-bit serial transfer.

The air-gap between transmitter-part and receiver-part should be clear and free from any optical interference and blockage. Moreover, the distance between these two components should be big enough to comply with the TEMPEST criteria as well. It would be a plausible installation if the transfer-unit is installed in a controlled room or box. To prevent any signal leakage, it is advised to power these two parts with different power sources. In case it is required to prevent optical dissemination, nonconductive pipe-like material may also be used between optical transmitter and sensor pairs.

It is obvious that that there will be no acknowledgement/negative-acknowledgement from receiver-part to transmitter-part which can inform the transmission is successful or nor. This problem should be mitigated by eliminating the sources of optical noise in the transfer-unit.

The other palpable communication problem between the transmitter and receiver parts is the synchronization of the pairs. Depending on the sensor capabilities, the solution can be either utilizing a preamble or discriminating between no-signal and at least two different intensity levels of optical signal. In later case, a simple solution may be inserting a no-signal between bit transmissions. Since 0 and 1 are identified with different optical intensities.

Another extension to the transfer-unit can be the inclusion of signal feedback from receiver-part to transmitter-part. In order to prevent any misuse of the channel from low side to high side, feedback mechanism should be implemented on electronic circuit level. By this way, the communication speed would get higher with the achieved acknowledgement signal and ease of synchronization. Typical design of proposed feedback mechanism is shown in Figure 4.

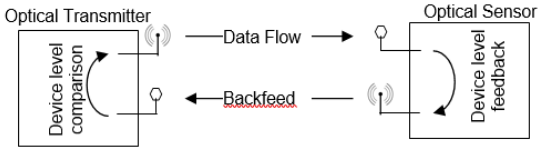

Figure 4. Feedback mechanism.

2.3 Low-End-Unit

Low-end-unit is responsible to receive the messages from transfer-unit and send or service them in to the low-security network. Low-end-unit may function as application proxy as well. Keeping log on low-end-unit will help in debugging and error correction efforts. Conceptual design of the modules and data flow in low-end-unit are shown in Figure 5.

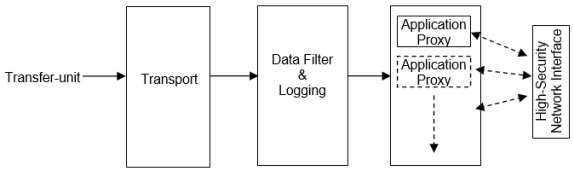

Figure 5. Low-end-unit conceptual design

Transport module communicates with the receiver-part of the transmitter-unit by using a customized communication protocol. Although data filter and logging module is optional, it is advised for error detection and communication tracing purposes. Whenever received messages transferred to the application proxies, it is their responsibility to send or disseminate the message into low-security network.

3. CONCLUSIONS

As computer systems and networks get connected to each other, information sharing becomes a substantial requirement. But this cooperation brings about the security risks as well, since not all the systems run on similar security settings. System administrators are reluctant to take on additional security risks that stem from information sharing. Undoubtedly, it is very common for a system which runs on a higher security setting oblige to transfer some information to a lower security system or network.

There are several studies in the literature which claim to reduce the security risks in information transfer between the networks with different

security levels. Considerable number of the studies rely on application level measures, where several of them are developed on operating systems level. In any case, most of the transfer mechanisms proposed so far keep utilizing a duplex communication infrastructure for the sake of communication speed and synchronization requirements. Therefore, these proposals mostly criticized for still having considerable security risks that originate from the other network.

Our proposal presented in this study has no physical connection between high-security and low-security networks. In other words, there is an actual air-gap between the networks. Hence the leaking emanations are prevented even on the power lines as well. Our design opt out the communication speed on account of guaranteeing the one-way data transfer. However, the design is more compatible with the TEMPEST requirements than the other alternatives. It would be a convenient way if the application proxies running on the high-end-unit inform the clients on that their messages will be relayed to the other network after a reasonable time delay. Similarly, the application proxies running on the low-end-unit inform the clients on that the message I subject to a significant time delay and the communication is one-way only. Development of the application proxies for both of the networks and specification of customized communication protocols to run in between transfer-unit and high-end, low-end units are recommended as future works.

4. REFERENCES

[1] Salehie Mazeiar and Ladan Tahvildari, "Autonomic computing: emerging trends and open problems." ACM SIGSOFT Software Engineering Notes. Vol. 30. No. 4. ACM, 2005

[2] Adams, Jonathan, and Tamar Loach. "Comment: A well-connected world." Nature 527.7577 (2015): S58-S59.

[3] Yan, Fan, Yang Jian-Wen, and Cheng Lin. "Computer Network Security and Technology Research." 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation. IEEE, 2015.

[4] Layton, Timothy P., “Information Security: Design, implementation, measurement, and compliance.”, CRC Press, 2016.

[5] Sim, Jae-Yoon, and Kyung-Ho Lee., "A Study on Information Access Control Policy Based on Risk Level of Security Incidents about IT Human Resources in Financial Institutions.", Journal of the Korea Institute of Information Security and Cryptology 25.2 (2015): 343-361.

[6] Peltier, Thomas R., “Information Security Policies, Procedures, and Standards: guidelines for effective information security management.”, CRC Press, 2016.

[7] Information Sciences Institute University of Southern California, “Internet Protocol Darpa Internet Program Protocol Specification”, Internet Engineering Task Force (IETF), 1981, [Online]
Available: https://tools.ietf.org/html/rfc791

[8] Kota, Sastri, et al. "Multimedia satellite networks and TCP/IP traffic transport." arXiv preprint arXiv:1603.08020 (2016).

[9] Paila T., Walsh R., Luby ., Roca V., Lehtonen R., “File Delivery over Unidirectional Transport”, Internet Engineering Task Force (IETF), 2012, [Online]
Available : https://tools.ietf.org/html/rfc6726

[10] Holbrook H., Cain B., Haberman B., “Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast”, Internet Engineering Task Force (IETF), 2006, [Online]
Available: https://tools.ietf.org/html/rfc4604

[11] Banerjee, Anindya, et al., "Method and apparatus for detecting malicious software activity based on an internet resource information database." U.S. Patent No. 8,978,139. 10 Mar. 2015.

[12] Tran, Manh Cong, and Yasuhiro Nakamura, "Suspicious Domain Filtering Based on Auto-ware Communication Features." ITC-CSCC: International Technical Conference on Circuits Systems, Computers and Communications. 2015.

[13] Greally, Andrew, and Christina Thorpe, "Investigating Near Field Communication as a Method of Malware Propagation." IT&T (2015): 19.

[14] Definition of TEMPEST, TechTarget [Online]. Available: http://searchsecurity.techtarget.com/definition/Tempest

[15] TEMPEST (Codename), Wikipedia [Online]. Available: https://en.wikipedia.org/wiki/Tempest_(codename)