An Efficient Approach to Resolve Covert Channels

Muawia A. Elsadig[1] and Yahia A. Fadlalla[2]
(Corresponding author: Muawia A. Elsadig)
College of Computer Science and Technology, Sudan University of Science and Technology[1]
Khartoum, Sudan
Lead Consultant/Researcher, InfoSec Consulting, Hamilton, Ontario, Canada[2]
(Email: muawiasadig66@gmail.com)
(Received May 8, 2017; revised and accepted Oct. 21, 2017)

Abstract

The competitive edge of many companies and public trust in government institutions can often depend on the security of the information held in their systems. Breaches of that security, whether deliberate or accidental, can be profoundly damaging. Therefore, security is a highly topical issue for both designers and users of computer systems. A system is said to be secure if it supports the policy of a security model in a demonstrable way. Two users, or processes operating on their behalf, are communicating indirectly or covertly in such a system if they are communicating through means that violate the interpretation of the supported security model. Research to eliminate or resolve covert communication channels is limited compared to the real, rapid, and often dangerous threats these channels continuously pose. That is due; at large; to their ingenious, inventive, and numerous scenarios. In order for any two users to establish a covert channel, they both must know one another's identity. This paper proposes a design that is based on the fact that it is impossible inside a system for any process to recognize any user, for whom other processes are invoked, in order to covertly communicate with him or her - identities of all users are hidden. Our design is sought to eliminate covert channels that are known to a system and those that are unknown and waiting to be discovered and potentially utilized illicitly. The design is sought to eliminate covert channels indifferent to the scenario they employ.

Keywords: Covert Channels; Channel bandwidth; Cryptography; Multilevel Security; Network Protocols; Security Model; Security Policy

1 Introduction

It is well known that a large number of databases contain data that needs to be categorized into different security levels to securely manage the access to this data. In addition, the database user must obtain security clearance that allows them to access a particular data level [16]. In other words, any system must ensure that the users obtain the data which they are authorized for [35]. Therefore, civilian and military government agencies are used to building up their relational database systems based on the hierarchical classification levels such as Top Secret, Secret, Confidential and Unclassified.

The Mandatory Access Control (MAC) is a common security access control model that requires users and resources to be classified and assigned security labels [14], In other words, objects and subject are labelled with different security levels [13]. MAC is an approach to restrict unauthorized users from accessing objects that hold sensitive information. It is a B1 level requirement of the Orange Book [9], and interested readers can see more about the Orange Book in [23]. When a system ororganizes its data into different classification levels and mandates with its access control utilizing the MAC model, then the system will be defined as a Multilevel Secure System (MLS). The MLS is an implementation of MAC. It is mainly developed for databases and computers that belong to highly sensitive government organizations such as the U.S. Department of Defense [10]. In Multilevel Secure Database Management Systems, users are cleared at different clearance levels (*i.e.* Top-secret, Secret, Confidential and Unclassified. While data is given different sensitivity levels (i.e. Top-secret, Secret, Confidential and Unclassified) [38]. A covert channel scenario exists if labelled data is being transferred to an unauthorized user without violating Mandatory Access Controls. The unauthorized user in this case is a user that hasn't the appropriate clearance to access this labelled data. Commonly, a covert channel is a method of exploiting a communication channel by a process in order to pass information without violating the system security policy. It is noteworthy to mention that any proposal to solve a covert channel problem should take into account the system usability and usefulness. In other words, a useful covert

channel solution is a solution that doesn't diminish the usability and performance of the overt channel - a legitimate channel that is supposed to allow labelled data to be accessed by a legitimate user. This paper introduces a design that is supposed to fully eliminate any potential covert channel scenario that is intended to leak labelled information to unauthorized parties.

The rest of this paper is organized as follows: The next section gives a general overview of covert channel concepts and their development. Section 3 illustrates the typical covert channel model, which reflects the general concept of the covert channel scenario through addressing so called prisoners problem. Section 4 sheds some light onto some common fundamental concepts to give a concrete idea that facilitates a full understanding of our proposed design which is presented in Section 5. Then Section 6 outlines the evaluation criteria of the proposed design. The paper is concluded in Section 7 and subsequently the future work is presented in Section 8.

2 Covert Channel Development

A covert channel allows people to exchange hidden information in an undetectable way - in a way that doesn't diminish legitimate communication procedures, which complicates the detection of such kinds of threats. In addition, a covert channel can also be exploited to pass malicious activities such as Trojans and viruses *etc.* so traditional firewall systems couldn't recognize them.

It is illogical to attain full elimination of covert channels; however, it is possible to reduce them through an efficient and careful system design. Initially, the covert channel was introduced in stand-alone systems and was later extended to exploit computer network environments. Accordingly, there are two scenarios in which covert channels exist: network-based system covert channels and stand-alone system covert channels. In stand-alone covert channels, two processes of different security levels communicate with each other covertly to leak hidden information, (*i.e.* a high security level process leaks secret data to another process with low security level). In, contrast, a network covert channel exploits network protocol to carry covert messages [4].

Recently, different techniques have been developed that increasingly magnify covert channel threats. These rapidly developed techniques present security experts with a real challenge to fight against this ongoing threat. Interested readers are referred to [6], for in depth information on the rapid development of covert channels, in which a lack of covert channel countermeasures is clearly noticed. In the same context, Elsadig *et al.* introduced a valuable concept, the network covert channel triangle (DSM - Development, Switching and Microprotocol), which involves three elements that have the most direct impact in developing network covert channel technology. The DSM triangle reflects the importance of network covert channels and the security challenge that is posed [6]. Another good contribution in network steganography is done by Wendzel *et al.* [40]. They introduced a unified description that assist in categorizing network hiding methods. This valuable effort provides a unified taxonomy of hiding techniques, enables the comparison between them and offers an evaluation framework to assess hiding methods novelty.

It is noteworthy to mention that covert channels are not always used to threaten information security. Some practical uses for covert channels were presented, [11, 12, 34, 36] such as use of covert channels by network administrators to distribute secret information among the network users, use of covert channels to secure authentication processes, *etc.* As an example of using covert channels legitimately, Singh *et al.* proposed an approach that uses covert communication to enhance Vehicular Adhoc Networks (VANETs) security [34]. VANETs have become a hot area of research as they pose many security challenges [8]. Moreover, any suggested security solution for VANETs has to ensure an acceptable overhead that doesn't affect their protocols performance [7]. Singh's model exploits a storage covert channel approach to convey secure data while the transmission of unimportant data can be done through the system overt channel. However, this trend, the trend of using covert channels for useful purposes, doesn't change the fact that covert channels are ongoing, devolved and a dangerous threat, as covert channel techniques are developed according to the rapid development of computer system and network protocols.

3 Typical Covert Channel Model

This section introduces the typical concept of covert channels, which is illustrated through the common scenario that is known as the prisoners problem [33].

Alice and Bob are prisoners who wish to communicate to each other, keeping in mind the end goal is to arrange their escape. The possible communication channel that can be used to speak to each other is under monitoring by so called Wendy (Warden). Wendy is dedicated to watch the communication between them. When Wendy catches any suspicious information, Alice and Bob will be moved into solitary confinement and that results in killing any hope for them to exchange any piece of information. Therefore, in order to avoid this situation, Alice and Bob should find a secret channel to exchange their messages in a manner such that Wendy cannot be able to detect them. In this case, this channel is known as a covert channel which allows two communication parties to exchange their secret information covertly without being detected by a monitoring system.

When Alice and Bob are establishing their communication via networked computers, then the scenario is representing another type of covert channel which is know as a network covert channel [5].

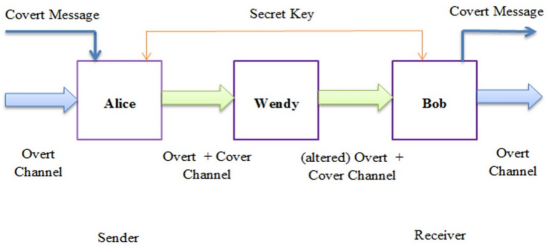

Figure 1: Typical covert channel model

4 Fundamental Concepts

This section has introduced fundamental security concepts that are required to understand our proposed design which is illustrated in Section 5. These concepts encompass Authentication, Multilevel Security and Cryptosystems. In addition, this section sheds some light on a storage covert channel that threatens multilevel security systems.

4.1 Authentication

Authentication, authorization and accounting (AAA) is a framework to apply policies, control and manage access to resources and examine the usage of these resources [42]. Authentication is a process of verifying the identity of a subject so as to ensure no subject can gain access to an information resource (object) unless their identity is verified. The next step after verification is Authorization which determines what a subject accesses after authentication. Authorization is classed into two types, Course Authorization and Fine Authorization. As an example, having access to a payroll system is a Course Authorization while determining which function is allowed to be accessed after getting into a payroll system is a Fine Authorization.

Accountability is concerned with recording what a subject does, when it does it and where it does it.

These combined processes (authentication, authorization and accounting) are considered vital for effective network management and security. Moreover, authentication is considered the foundation of all security systems [28].

An effective and successful authentication procedure is heavily based on the efficiency of the verification procedure that is being used. The trusted computing base (TCB) is the mechanism that is used to perform the authentication procedures as a part of its whole security mission. It maintains enforcement of the security policy of a given system. The careful design and implementation of a TCB for any system is paramount to its overall security. System users are considered outside the system boundaries, so the TCB doesn't deal directly with the system users. The TCB is dealing with the processes inside the system that act on behalf of the real system users. Normally, inside a system boundary, the system creates processes to represent users, so the processes request and consume the system resources on behalf of the associated users.

In our proposed design, the Extended TCB Theater (ETCB) that is illustrated in Section 5, a user is assumed to have neither stolen nor forged the identity of a legitimate user that is given to provide authorized access to the TCB system.

Commonly, there are three types of authentication mechanisms: password-based [1, 15, 20, 25, 27, 39], token-based and biometrics-based [17, 21, 22, 43]. Password-based is the most popular one and it uses something a user knows (*i.e.* password, personal identity number (PIN) *etc.*). While token-based uses something a user possesses (*i.e.* smart cards, physical keys *etc.*). The last type is biometrics-based which is known as something a user is and does (*i.e.* fingerprint matching, iris scanning, voice recognition *etc.*) [28].

Pham *et al.* discussed the shortcomings of the aforementioned authentication mechanisms and recommended the new mechanism that has emerged recently, which is known as electroencephalography (EEG) [28]. EEG is a type of biometrics and combines the advantages of password-based and biometrics-based authentication mechanisms without their shortcomings. Accordingly, Pham *et al.* proposed an authentication system based on EEG signals to be used in multilevel security systems.

4.2 Multilevel Security

The development of database systems and their utilization by various people with various interests makes it crucial to design completely secured database systems [31].

Commonly, any secure Database Management System (DBMS) uses some rules to control access to its data. The setting of these rules is defined as the system security policy, in which any company enforces its security policy to allow only authorized users to access what they are authorized for. The access process encompasses subject and object. The subject is an active process request to access an object, while the object is a passive entity such as information resources. The rules that control the access process can be abstracted by what is called an access control matrix. Each element of this matrix represents an authorized mode of access as illustrated in Figure 2.

Each subject is assigned a clearance, and each object a classification [18]. Clearances and classifications are formed into so called access classes. Each access class involves two parameters (a hierarchical and a group of nonhierarchical categories). Top secret and Secret are examples of hierarchical components while Navy, Military is an example of a group of nonhierarchical categories [9].

MAC, which is mainly based on the Bell-LaPadula model [10, 26] allows a labelled object to be transferred to a subject if and only if the object access class is dominated by that of the subject. The TCB mechanism is closely similar to MAC concepts. It is the set of security components in which to enforce a system security policy.

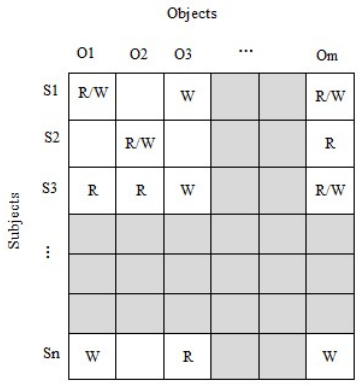

Figure 2: An example of TCB model

It assigns labels to objects, users and processes. The TCB should be carefully designed and protected to enforce access controls effectively.

Fadlalla asserted that covert channels still exist in many systems despite the fact that many effective criteria were presented to disallow any attempt at covert communication between two processes. These criteria include CTCPEC, TCSEC and the Bell-LaPadula model *etc.* [9].

As mentioned, in Multilevel Secure Database Management Systems, users are cleared at different clearance levels (*i.e.* Top-secret, Secret, Confidential and Unclassified. Data is given different sensitivity levels (*i.e.* Top-secret, Secret, Confidential and Unclassified) [38]. To illustrate the concept of a security level classifications approach an example is given below.

Example 1. *Imagine a database system with five user classifications as follows: Top Secret, Secret, Confidential and Unclassified. According to these classifications, the database would be classified into the same security level classifications as shown in Figure 3.*

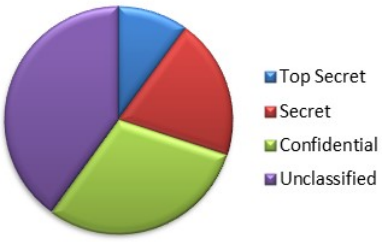

Figure 3: Database security level classification

A user can access the database according to two parameters (their security level and database security level). These classifications are hierarchical in nature. In other words, an unclassified user can only see the unclassified database while the Top-Secret user can see all other database security levels (Top Secret, Secret, Confidential and Unclassified). Confidential can see Confidential and Unclassified security levels and so on as illustrated in Figure 4.

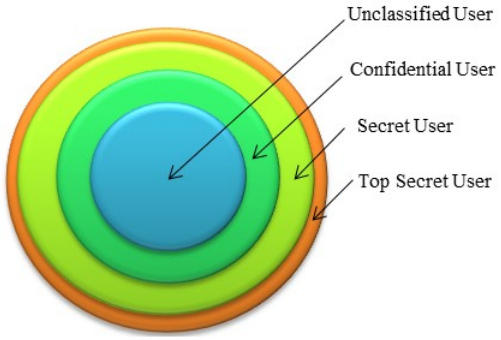

Figure 4: User clearance levels

Generally, it is commonly known that any system enforces the two rules: (1) simple security property and (2) star property providing multilevel security [30, 37]. Multilevel Security is expected to help in the decision to access a domain with security classifications, a domain where its information has security levels (*i.e.* Confidential, Secret *etc.*) [29]. Based on some specific requirements and definitions, the National Security Agency (NSA) has defined various levels of security for computer and network systems. These definitions were stated on the evaluation criteria: Trusted Computer System Evaluation Criteria (TCSEC) and Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria. Accordingly, six hierarchical ratings levels are defined: A1, B3, B2, B1, C2 and C1. A1 is the most secure level while C1 is the least secure. The requirements for MLS are presented in Division B, which includes three sub-levels (B3, B2 and B1). Generally, we summarize that MLS refers to a system in which at least two classification levels of information or more are processed at the same time, and not all users are cleared for all levels of information [41].

4.3 Covert Channel

When dealing with a data object, as one subject writes to and another reads from, in this case the data object is considered an overt channel because this entity (data object) is mainly intended to hold data (*i.e.* files, buffers *etc.*). When subjects exchange information through a non-data object entity, then a covert channel exists. That means covert channels use a non-data object (an object that isn't used to hold data) to send data from one subject to another. There are two types of covert channel, storage and timing covert channels [3]. In a storage channel, the unauthorized information is being exchanged through a non-data object (*i.e.* one high process writes information to a non-data object, and then a low process reads that information). This scenario is legally accepted because the two processes can write to or read from a non-data object. However, from a different perspective, the sce-

nario is violating the system security policy because the information is exchanged between a high process and low process, which is prohibited. Therefore, it is noteworthy to say that detection of covert channels is highly difficult since the covert channel doesn't diminish the system legal operations. Timing covert channels occur by means of one process that can modulate signals or secret messages to another process that is not authorized to gain such information. After modulation of the secret message by the sender process, then the intended process (receiver) observes and decodes the secret message [4].

Commonly, most covert channel detection methods rely heavily on identifying illegal flow of information in source code or top-level specifications. As a matter of fact, some excluded resources in the interpretation phase of any security model represent fruitful areas for developing covert channels. These resources include design detail, implementation detail *etc.*

4.4 Cryptosystems

A cryptographic system has five components:

- A plaintext message.
- A ciphertext message.
- A key space.
- An enciphering transformation: the transformation of a plaintext into ciphertext.
- A deciphering transformation: the transformation of a ciphertext into plaintext.

Commonly, there are two rules that each cryptographic system should adhere to, these rules are:

1) The two main operations of any cryptographic system, enciphering and deciphering transformations, have to work for all keys of the key space.

2) Any cryptographic system must depend on maintaining the security of the keys not on the secrecy of the encryption/decryption algorithms.

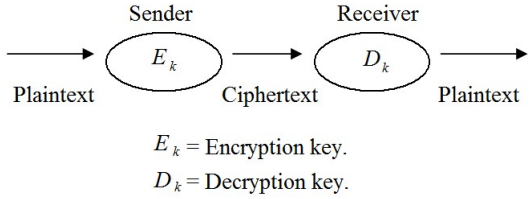

Figure 5: Diagram of a cryptographic system [9]

The Cryptosystems are categorized into two classes: symmetric cryptosystems and asymmetric cryptosystems. For symmetric cryptosystems, a same key is used for both operations, encryption and decryption, and this key should be kept secret. In asymmetric cryptosystems, the encryption key and the decryption key are different. So, the decryption key is kept secret while the encryption key is made public [9].

5 Extended TCB Theater

The extended TCB Theater is a security design that aims to eliminate any potential covert channel that is supposed to pass classified information to unauthorized users covertly. The design is an extended version of our design, TCB Theater presented in [9]. The enhanced version, called Extended TCB Theater (ETCBT) is a combination of two approaches, authentication and cryptography. This is to ensure that the identity of a user is kept secret from other users. So, covert processes - that work on behalf of users - would never know each other and this is expected to fully eliminate any potential covert channel that intends to leak confidential information to unauthorized parties. The ETCBT is controlling the request that is made by a subject to access an object; the subject would be any process that wishes to utilize object resources. As a matter of fact, some processes are legitimate processes that work on behalf of legitimate users, while some processes can be malicious (*i.e.* processes infected by Trojan horses or by any other means of malicious activity) that work on behalf of covert users -legitimate users that communicate with each other covertly. Therefore, this design is mainly built to break the connection between covert processes through hiding the true users' identities.

5.1 ETCBT Assumptions

There are three assumptions that our proposed system heavily relies on:

1) The design assumes that a user can't be seen on the ETCBT system after assigning a process to work on their behalf.

2) The design assumes that more than two processes are running at the same time. It is commonly expected that most times this assumption is valid, but in case this assumption is not valid, the ETCBT introduces a new approach to ensure the validity of this assumption. The ETCBT ensures the presence of this assumption by introducing a confusing process in the case that only two processes are running at a given time. If two covert processes try to infer that they are the only communicated processes at a given time, the confusing process defeats that.

3) The design assumes that a trusted, secure and direct communication path should be attained between a user and the ETCBT system. To ensure the two communication parties are authenticated by each other and their exchanged data is secured.

5.2 ETCBT Components and Description

The ETCBT system consists of four essential components listed below and illustrated in Figure 6.

1) Theater Office.
2) TCB.
3) Confusing Process Generator.
4) The user.

5.2.1 Theater Office

This unit is the same as the "Box Office" unit illustrated in the previous model [5]. A user is required to obtain "pass-information" to be able to access the TCB. This pass-information is provided by the Theater Office. When the Theater Office provides the user with the pass-information, it sends encrypted information about the user to the TCB at the same time. The detail of how this unit works is discussed in the next section.

5.2.2 TCB

This unit consists of four components: the Database Trusted Guard, the Reference Monitor, the Authenticator, and the Secure Data Block. The Secure Data Block has a direct communication channel with the Theater Office, whereas the rest of the components are logically connected to the Theater Office.

5.2.3 Confusing Process Generator

This unit works only under special conditions, when there are only two processes running at the same time. When this condition is met, the Reference Monitor sends a request to the Confusing Process Generator, and then the latter unit generates a confusing process. The Reference Monitor receives the confusing process and prompts the Database Trusted Guard to give the confusing process access to the same object that is being used by the aforementioned two processes. In this case, the two processes will be confused about which process has performed the last operation on the shared object. Therefore, this breaks up any potential covert communication, if we assume that the two processes have an intention to leak classified information covertly.

5.2.4 The User

This unit represents a user who wishes to access the TCB. In other words, the user who wishes to access an object in a classified database (Multilevel Security System).

5.3 How ETCBT Works

A user is granted an access class, a list of user allowed processes to be executed on the TCB, and a permanent login identifier. These are permanent privileges unless a change is required by the system security policy. The Theater Office is responsible for providing the aforementioned privileges. Then the user uses his log on identifier and encryption key/keys to only communicate with the Theater Office.

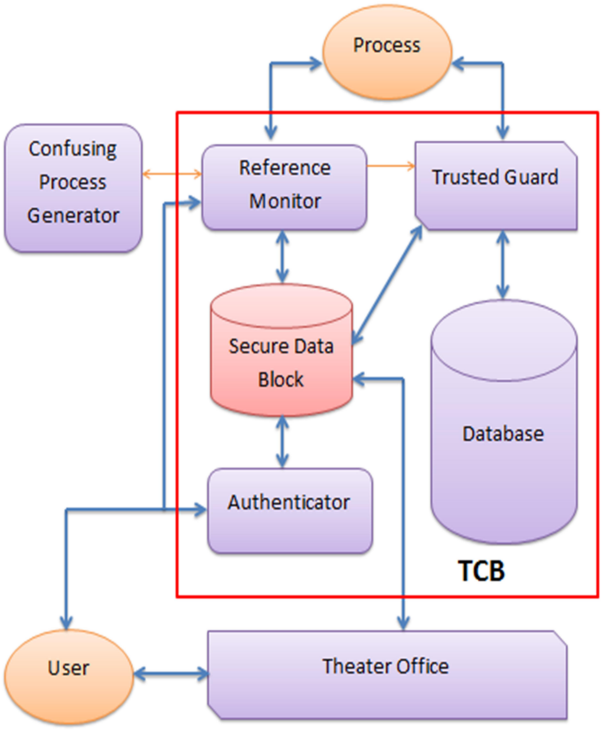

Figure 6: ETCBT design diagram

When a user needs to access an object, they send their plain login identifier to the Theater Office - unencrypted identifier. That means the user must be identified by the Theater Office. Then the Theater Office does the following scenarios simultaneously:

1) Send encrypted "pass information" to the user, which includes a temporary login identifier along with a new user encryption key to be used to communicate with the TCB.

2) Send a "ticket" to the TCB through the Secure Data Block unit, which is connected to all other TCB's components. The ticket is an encrypted packet that consists of the following parts:

   - The "pass-information" which is encrypted with a shared key between the TCB Authenticator and the Theater Office.
   - Users' login identifiers and a list of their allowed processes to be executed on the TCB. This information is encrypted with a key. This key is shared between the Theater Office and the TCB Reference Monitor.
   - Users' login identifiers and their access classes are both encrypted with a key. This key is

shared between the Theater Office and the TCB Trusted Guard.

These scenarios ensure separate communication between the Theater Office and the TCB's components. This design relies on cryptography to secure the communication between its components as described above. So, each component has a logical separate secure path to the other components, which ensures the separation between the users and the processes are working on their behalf. In return, this will successfully prevent any attempts to establish any covert communication.

6 Approach Evaluation Criteria

Our evaluation is based on implementations of real scenarios that are expected to reflect realistic results which prove our approach's expectations. Our design is sought to completely stop any two users - usually with different access levels - to benefit from their covert communication. To initiate a covert channel, two users who are presented inside the systems by two different processes, have to identify each other. One of the two users is the sender of the illicit information and the other is the receiver. Our design hides all users' identities from the TCB. Our design does not prevent; nor does it worry about; illicit signaling between processes, rather, it prevents illicit signaled information to reach its intended receiver. Hiding users' identities prevents any potential covert communication between any two users. Our approach establishes a trusted path service which ensures users direct and uncompromised secure communication with TCB; the Trusted Guard is placed between a process and the database. Each TCB component is forced to know the least information about users necessary to serve them; and is certainly not aware of their identities. Therefore, our evaluation is dependent on the cryptosystem used; we assume it to be effective in terms of its efficiency and usability. The evaluation procedure may consider either symmetric or asymmetric cryptosystem. Taking into account the development in cryptosystem techniques; *e.g.*, Elliptic Curve Cryptography (ECC) challenges RSA. ECC attains better security in case of using a smaller key compared to RSA [19]; consequently; it decreases the processing overhead and that is one important criterion when it comes to evaluating a cryptosystem's performance. Any suitable supported programming language may be used to implement our design, *e.g.*, C++. while this section demonstrates our approach's evaluation criteria, the implementation and evaluation results are left as future work, as indicated in Section 8.

7 Conclusion and Discussion

Based on hiding all user identities from the TCB and thus from the processes that are operating on their behalf, an efficient design has been proposed by this paper to prevent any two users with different classes (*i.e.* Top Secret level and Confidential level) from initiating a covert communication channel. As a matter of fact, the design is not preventing two processes from being communicated covertly. However, the process that passes a covert message never knows to which user the receiving process belongs. So, at the level of processes communication, the processes will never identify each other on the level of the true users that they are operating on their behalf. This design is expected to totally overcome the covert channel problem in multilevel security systems even if there are only two processes running at the same time. When there are only two active processes, the design introduces a so called "confusing process" to confuse the two active processes and thus prevents them from having a successful covert communication.

With the rapid development of computer networks, many enterprises build up their local network. Defiantly, these networked computers store a great amount of data or information and the users continuously exchange information over the network. This phenomenon has boosted the need for secure communication [24]. In this sense, some recent woks have been presented such as those at [2, 32].

An extension of the Bell-Lapadula model to suit local area networks, called the L-BLP model, has been proposed in [32]. This is where each host is assigned a security level, and then according to these levels the monitoring device controls all communications between these hosts by applying the L-BLP security policy. The L-BLP defines system topologies and builds up new state transition rules to control the flow of information securely. This represents a multilevel security local area network MSL. The L-BLP model allows a low-level host to send information to another with a high level and prevent a high-level host sending information to a low-level host. However, this scenario isn't valid for a TCP/IP network, which requires a Knowledge message (ACK) to ensure packet delivery. When a packet is sent by a low host to a high one, the low host waits to receive the ACK message, but the high host is prevented by L-BLP model policy from sending any information to the low host. Solving this problem (by allowing the high host to send an ACK message to the low one) causes a covert channel scenario as a high host can exploit the ACK message to pass information to a low host which is against security rules [24]. Our design is expected to solve this problem as it is mainly based on the separation between a user and the process that operates on their behalf. If a user (a Host in terms of network) acknowledges another user (another Host), this acknowledgment is within the level of the users. Therefore, the processes are not being involved as per our design policy and thus prevent any attempt to handle any covert communication.

8 Future Work

Our future work would be focused in verifying our design through a real or simulated environment to give realistic results. In addition, this design is expected to be extended to suit a network environment as an approach to fix network-based covert channels. The network covert channel techniques are dramatically increased, developed and pose a real challenge.

References

[1] A. Asimi, Y. Asimi, A. Abdellah, and Y. Sadqi, "Strong zero-knowledge authentication based on virtual passwords," *International Journal Network Security*, vol. 18, no. 4, pp. 601–616, 2016.

[2] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, "Ethane: Taking control of the enterprise," in *ACM SIGCOMM Computer Communication Review*, vol. 37, pp. 1–12, 2007.

[3] P. Dong, H. Qian, Z. Lu, and S. Lan, "A network covert channel based on packet classification," *International Journal Network Security*, vol. 14, no. 2, pp. 109–116, 2012.

[4] M. A. Elsadig and Y. A. Fadlalla, "Survey on covert storage channel in computer network protocols: Detection and mitigation techniques," in *The International Conference on Advances in Information Processing and Communication Technology (IPCT'16)*, pp. 79–85, 2016.

[5] M. A. Elsadig and Y. A. Fadlalla, "Survey on covert storage channel in computer network protocols: Detection and mitigation techniques," *International Journal of Advances in Computer Networks and Its Security*, vol. 6, no. 3, pp. 11–17, 2016.

[6] M. A. Elsadig and Y. A. Fadlalla, "Network protocol covert channels: Countermeasures techniques," in *9th IEEE-GCC Conference and Exhibition (GCCCE'17)*, pp. 706–714, 2017.

[7] M. A. Elsadig and Y. A. Fadlalla, "Performance analysis of popular manet protocols," in *9th IEEE-GCC Conference and Exhibition (GCCCE'17)*, pp. 1085–1089, 2017.

[8] M. A. Elsadig and Y. A. Fadlalla, "Vanets security issues and challenges: A survey," *Indian Journal of Science and Technology*, vol. 9, no. 28, 2016.

[9] Y. Fadlalla, *Approaches to Resolving Covert Storage Channels in Multilevel Secure Systems*, 1997. ISBN:0-612-23861-X.

[10] O. S. Faragallah, E. M. El-Rabaie, F. E. A. El-Samie, A. I. Sallam, and H. S. El-Sayed, *Multilevel Security for Relational Databases*, pp.304, 2014.

[11] T. S. A. Fatayer, "Generated un-detectability covert channel algorithm for dynamic secure communication using encryption and authentication," in *Palestinian International Conference on Information and Communication Technology (PICICT'17)*, pp. 6–9, May 2017.

[12] T. S. Fatayer and K. A. A. Timraz, "Mlscpc: Multilevel security using covert channel to achieve privacy through cloud computing," in *World Symposium on Computer Networks and Information Security (WSCNIS'15)*, pp. 1–6, 2015.

[13] D. Gollmann, "Computer security," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 2, no. 5, pp. 544–554, 2010.

[14] Y. Huang and X. Ma, "A security model based on database system," in *International Conference on Electrical and Control Engineering (ICECE'10)*, pp. 4954–4957, 2010.

[15] M. S. Hwang, S. K. Chong, and T. Y. Chen, "Dos-resistant id-based password authentication scheme using smart cards," *Journal of Systems and Software*, vol. 83, no. 1, pp. 163–172, 2010.

[16] S. Jajodia and R. Sandhu, "Toward a multilevel secure relational data model," *ACM SIGMOD Record*, vol. 20, no. 2, pp. 50–59, 1991.

[17] O. Kaiwartya, M. Prasad, S. Prakash, D. Samadhiya, A. H. Abdullah, and A. O. A. Rahman, "An investigation on biometric internet security.," *International Journal Network Security*, vol. 19, no. 2, pp. 167–176, 2017.

[18] N. Kaur, R. Singh, M. Misra, and A. K. Sarje, "Concurrency control for multilevel secure databases," *International Journal Network Security*, vol. 9, no. 1, pp. 70–81, 2009.

[19] A. V. N. Krishna, A. H. Narayana, and S. K. Murthy, "A hybrid digital signature scheme on dependable and secure data," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 87–93, 2017.

[20] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[21] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and computer applications*, vol. 33, no. 1, pp. 1–5, 2010.

[22] C. T. Li and M. S. Hwang, "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *Network*, vol. 3, no. 4, pp. 5, 2010.

[23] S. B. Lipner, "The birth and death of the orange book," *IEEE Annals of the History of Computing*, vol. 37, no. 2, pp. 19–31, 2015.

[24] X. Liu, H. Xue, X. Feng, and Y. Dai, "Design of the multi-level security network switch system which restricts covert channel," in *IEEE 3rd International Conference on Communication Software and Networks (ICCSN'11)*, pp. 233–237, 2011.

[25] Y. J. Liu, C. C. Chang, and S. C. Chang, "An efficient and secure smart card based password authentication scheme," *International Journal of Network Security*, vol. 19, no. 1, pp. 1-10, 2017.

[26] W. Meanrach and S. Chittayasothorn, "A bitemporal multilevel secure database system," in *Africon*, pp. 1–7, 2007.
[27] J. Moon, D. Lee, J. Jung, and D. Won, "Improvement of efficient and secure smart card based password authentication scheme," *International Journal Network Security*, vol. 19, no. 6, pp. 1053–1061, 2017.
[28] T. Pham, W. Ma, D. Tran, P. Nguyen, and D. Phung, "Eeg-based user authentication in multilevel security systems," in *International Conference on Advanced Data Mining and Applications*, pp. 513–523, 2013.
[29] F. S. Prass, L. M. Fontoura, and O. M. D. Santos, *A Framework Based on Security Patterns for Transformations*, pp. 319-331.
[30] P. Sapra and S. Kumar, "Development of a concurrency control technique for multilevel secure databases," in *International Conference on Optimization, Reliabilty, and Information Technology (ICROIT'14)*, pp. 111–115, 2014.
[31] P. Sapra, S. Kumar, and R. K. Rathy, "Performance analysis of decomposition techniques in multilevel secure relational database systems," in *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology*, pp. 544–549, 2012.
[32] T. G. Si, Y. X. Zhang, and Y. Q. Dai, "L-blp security model in local area network," *Dianzi Xuebao (Acta Electronica Sinica)*, vol. 35, no. 5, pp. 1005–1008, 2007.
[33] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Advances in Cryptology*, pp. 51–67, 1984.
[34] A. Singh and K. Manchanda, "Establishment of bit selective mode storage covert channel in vanets," in *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC'15)*, pp. 1–4, 2015.
[35] P. D. Stachour and B. Thuraisingham, "Design of ldv: A multilevel secure relational database management system," *IEEE Transactions on Knowledge and Data Engineering*, vol. 2, no. 2, pp. 190–209, 1990.
[36] Y. Sun, X. Guan, and T. Liu, "A new method for authentication based on covert channel," in *Proceedings of the 8th IFIP International Conference on Network and Parallel Computing (NPC'11)*, pp. 160–165, 2011.
[37] M. Thiyagarajan, C. Raveendra, and V. Thiagarasu, "Web service authentication and multilevel security," *Indian Journal of Science and Technology*, vol. 8, no. 15, 2015.
[38] B. Thuraisingham, "Multilevel secure database management system," in *Encyclopedia of Database Systems*, pp. 1789–1792, 2009.
[39] C. S. Tsai, C. C. Lee, and M. S. Hwang, "Password authentication schemes: Current status and key issues," *International Journal Network Security*, vol. 3, no. 2, pp. 101–115, 2006.
[40] S. Wendzel, W. Mazurczyk, and S. Zander, "Unified description for network information hiding methods," *Computer Science*, vol. 22, no. 11, pp. 1456–1486, 2016.
[41] T. C. Williams, *Multi-Level Security Network System*, June 27, 2006. US Patent 7,069,437.
[42] C. C. Yang, C. W. Lee, T. Y. Chang, M. S. Hwang, "A solution to mobile IP registration for AAA", *Lecture Notes in Computer Science*, vol. 2524, pp. 329–337, 2003.
[43] M. Zhang, B. Yang, W. Zhang, and T. Takagi, "Multibiometric based secure encryption, authentication scheme with fuzzy extractor," *International Journal Network Security*, vol. 12, no. 1, pp. 50–57, 2011.

Biography

Muawia A. Elsadig obtained his MSc degree in Computer Network and Bachelor degree in Computer Engineering. His research interests lie in the area of Information Security, Network Security, Cybersecurity, Wireless Sensor Networks, Network Protocols, and Information Extraction; ranging from theory to design to implementation. Elsadig worked at different accredited international universities and has many publications at recognized international journals and conferences.

Dr. Fadlalla is the lead researcher and scientist at InfoSec Consulting in Ontario, Canada. He earned B.Sc. in Computer Science from the State University of New York at Utica, N.Y., USA; M.Sc. and Ph.D. in Computer Science from the University of New Brunswick at Fredericton, New Brunswick, Canada in 1985, 1992, and 1996, respectively. Professor Fadlalla taught at the University of New Brunswick at Fredericton and at the State University of New York at Albany. He is frequently invited nationally and globally to speak on contemporary information security issues. He appears and was featured in Canadian television and newspapers as an information and national security expert; likewise, he was featured in newspapers in France, Morocco, Sudan, and England. Professor Fadlalla is and was an information security consultant to different private companies and government agencies in Canada. He has extensive publications record in the areas of Computer Security, Information Assurance, Cryptography, and Cyber Security. He is a member of numerous professional associations and societies worldwise.