International Journal of Latest Trends in Engineering and Technology
Vol.(9)Issue(4), pp.241-246
DOI: http://dx.doi.org/10.21172/1.94.37
e-ISSN:2278-621X

A SURVEY ON EFFECTIVENESS OF COVERT CHANNELS AS SECURE TOOL FOR SENSITIVE DATA TRANSFER

Amarpreet Singh[1], Dr.Vijay Dhir[2]

Abstract*:* - From the last decade a shift has been observed in the mindset of an individual and organizations with respect to the demand from limited access of information to ultimate access of critical and sensitive information. To fulfill this need of achieving ultimate access, there is a demand of new technology.

The wide range of innovations and emergence of technologies can be seen during the period ranging from Wired connectivity to the era of ad hoc wireless networks. In a nut shell it frees the devices from hard connections such as wires and cables. But on the other hand wireless networks have become the fertile ground for new attacks due to its flexible parametric factors. It raises the security concerns of all types of data but especially of the critical and sensitive data of an individual and organization. This has paved way for large number of researchers to carry out their researches pivoting around the security of critical and sensitive information. This paper reviews the effectiveness of covert channel in providing the security to the sensitive information along with its applications.

Keywords: - Covert, Ad-hoc wireless network, covert channel

1. INTRODUCTION

Among the different components of any system, process or organization it has been noticed that data is the component that has found an utmost importance. For every system it is data that comes out be the driving force that leads to the success of that particular system. With the growth in network and its associated technologies most of the business and organizations have developed information centric processes.

With this growth the last decade has also seen the rise in attacks on such information centric business processes. This leads to the requirement of maintaining the multilevel security and confidentiality of sensitive and critical information. More we succeed in this aspect more is the success rate of any venture.

Many security measures are suggested to counter these attacks such as cryptography, steganography, watermarking and covert channels. Cryptography hides the contents of the message from an attacker, but not the existence of the message. Steganography and watermarking bring a variety of very important techniques how to hide important information in an undetectable and/or irremovable way in audio and video data. They even hide the very existence of the message in the communicating data. But the covert channel is different from them.

A covert channel is a mechanism in which a sender and a receiver set up a compromised logical link between the processes running at their ends to secretly exchange critical information without being detected by third party. A covert channel is designed to be hidden within the normal communication traffic of a legitimate logical channel, such as TCP or UDP. Secret information is amalgamated in the legitimate channel packets in such a way that only the end applications can detect and retrieve this information. Anyone else watching the network traffic is unable to detect the presence of such information in the legitimate channel packets. A covert network is so entitled in the real world scenario because it is secreted from the admittance control apparatuses of secure functioning systems since it don't deal with the genuine data transfer processes and consequently cannot be sensed or measured by the security appliances that motivate secure operating schemes [1][2].

Covert Channels have been defined for the first time by Lampson in 1973. A path of communication that wasn't designed for [that sort of] communication between two processes. It was authorized to communicate, but not in the way they actually are. [32]

According to 1985 U.S. DoD publication a covert channel is "a communication channel that can be exploited by a process to transfer information in a manner that violates system security policy" [29].

According to Murdoch [19], a covert channel can be described as a communication in a computer system where the sender and the receiver plan to leak information over a channel which is not designed for that communication to take place, in violation of a required access control policy.

G.J. Simmons discussed one of the most common and perhaps the best vehicle for discussing the dynamics of covert communications is found in what is known as the "prisoners' problem" initially by in 1983.[31]

Actually word covert is derived from the word overt which means open. Covert is opposite of overt so it means hidden or under cover. So covert channel play a dual role with regard to network communication. At a particular instant it may turn out

[1] Research Scholar, IKG PTU Jalandhar, Punjab, India
[2] Prof. Research Scholar, IKG PTU Jalandhar, Punjab, India

to be a threat to an entity. But at other time it can be used as subversive means of achieving confidentiality and maintaining anonymity for another. It can be used to protect privacy or increase security of critical communication. Because a covert channel hides within a legitimate logical channel, it is a very simple yet effective mechanism for exchanging information between two end applications without alerting any firewalls or intrusion detectors on the network. For extremely sensitive applications, it may be advantageous to transmit certain data covertly. This provides an additional layer of security to that provided by the different layers of the protocol stack. Covert channels are best suited for sensitive data and their success rate is high if data burst is small**.**

2. COVERT CHANNEL:TYPES

2.1 Covert storage channels

Involves the direct or indirect writing to storage location by one process and direct or indirect reading of the storage by another process. They exploit the attributes of the resources shared between the two compromised processes running at the sender and receiver end. Such attributes may be. Sectors on a disk, unused bits in a packet header or the payload. [30]

A covert storage channel transfers information through the setting of bits by one program and the reading of those bits by another. Covert storage channels occur when out-of-band data is stored in messages for the purpose of memory reuse. Examples would include using a file intended to hold only audit information to convey user passwords--using the name of a file or perhaps status bits associated with it that can be read by all users to signal the contents of the file.

2.2 Covert Timing Channels-

It exploits the temporal or ordering relationship in such a compromised manner that accesses to shared resources can be interpreted by the receiver.

Some common temporal based attributes used in this mechanism are packet inter-arrival times of Internet traffic, system paging rate, I/O or network usage rates, process creation rate, and time slice relinquishment.

Covert timing channels convey information by modulating some aspect of system behavior over time, so that the program receiving the information can observe system behavior and infer protected information. In some instances, knowing when data is transmitted between parties can provide a malicious user with privileged information. Also, externally monitoring the timing of operations can potentially reveal sensitive data.

Covert channels are frequently classified as either storage or timing channels. Some examples of covert timing channels are the system's paging rate, the time a certain transaction requires to execute, and the time it takes to gain access to a shared bus.

3. RELATED WORK

The literature survey reveals the existence of numerous publications by different researchers dealing with various aspects, issues and techniques of designing the covert channel applicable in different environments of a network. Some of them are summarized here:

The first publication on network covert channels is a paper published in 1987 [28]. It points out three covert channels to show the possibility to create a channel through a LAN. This work has been the basis for [27], where the author shows the possibility to create such channels in IEEE 802.2, 3, 4, and 5 networks with padding and unused bits used to transmit information.

A simple covert timing channel with distribution matching is proposed in [18]. The approach processes the network traffic as fixed-length fragment and obtains the histogram of the delays, then uses the binary coding method to embed the message bits.

A relatively high bandwidth covert timing channel for802.11 networks (Covert DCF) is proposed in [16]. It exploits the random back off in the distributed coordinated function (DCF), used to avoid collisions, to provide cover for covert timing channel. Covert DCF provides significant improvements over other covert channels at that time in the area of throughput, while maintaining high accuracy and remaining undetectable.

Communication can be done steadily in the VANET network with the establishment of Covert channels between those nodes [5]. If the covert channel is established in the VANET network, then the security is maintained between High profile vehicle and Security provider vehicle and can share secret data covertly with each other and the attacker or you can say that the other vehicles that are present in this network can't detect the covert channels.

Utilizing the unused fields of the packets for covert channel establishment has been widely investigated [21]. For example, the ACK frame's destination address field can be used as a medium for covert communication in the IEEE 802.11 protocol [23]. MANET's routing protocols can be considered as another space for covert channel establishment [17]. S.Li and A. Ephremides [17] discuss the use of various features in AODV routing algorithm for covert channel establishment. "Timing of the route request", "source sequence number filed in the route request", "lifetime field of the route reply", and "destination ID field in the route request" are some examples of these features. However, most of these covert channels are statistically detectable and cannot be considered as network steganography. In addition, the firewalls and routers are usually configured to change the unused fields to avoid hidden channels [14].

Packet retransmission and rate switching approaches are other means for covert channel establishment in wireless networks [15,25]. In [25], packet retransmission is used to create covert channel. This paper uses the "Retry bit" and "More data" fields for synchronization and the "Destination/ID" field for the covert data transmission. In [15], rate switching of the 802.11

protocol is used for covert channel creation in wireless networks. The target of the rate switching protocol is to choose a data rate that optimizes the node's performance. The proposed covert channel is established between a workstation and an access point (AP). Access point observes the sequence of data rates and decodes the hidden message accordingly. This covert channel has low bit rate with 100% accuracy in decoding the hidden messages. In [4], the probability distribution of the different data rates in the wireless networks is used as a mean for covert channel detection. Euclidean distance is used to calculate the similarity of the probability distribution of the data rates, used by the covert sender, and the possible data rate probability distributions in a wireless network. And with the use of measured Euclidean distance, the established covert channel will be 100% detectable.

CSMA/CA is an algorithm that is used in 802.11 standard to control the medium access in wireless networks [20]. The main feature of CSMA/CA is the randomness observed in the amount of back-off times, selected by the nodes in the busy channel condition. In [13], a covert channel is created by mimicking the behavioral characteristics of 802.11 wireless networks that result in low throughput with high level of covertness. The author of [8] creates a hidden channel using QoS features in 802.11e standard. QoS Control field is added to the frame in 802.11e. The combination of three fields of QoS, CF-Poll able, and CF-Poll request is used to create the covert channel. Paper [11] creates covert communication using the time intervals between the packets at the sender. The main goal of this paper is to create a timing channel that is robust against the noise in the network. The noise on such a channel can be the extra times applied between the packets transmission, forced by CSMA/CA. LDPC coding schemes are used to produce robustness against the noise. However, the bandwidth is wasted because of the LDPC usage, and according to the paper, 0.4 bit can be encoded in each packet.

A covert channel creation method in Ad hoc networks is also presented in [10]. This paper uses AODV routing protocol to create covert channel, while OLSR routing algorithm is used between the legitimate nodes in the network. Legitimate nodes discard the corrupted packets in the network, and the covert nodes extract the hidden data from these packets. In [7], the design of a covert channel in a hybrid network (a network that contains different kinds of networks) is proposed. The combination of Wi-Fi and 3G networks is used for this purpose. One network is used to transmit the key and the other to transmit the hidden message. Covert sender uses DES cryptography algorithm to encrypt the hidden message. The used key is transmitted to the hidden receiver with the use of 3G network, but the covert sender transmits the covert data on the Wi-Fi network.

Although the aforementioned covert channel methods create covert communications, they have some drawbacks. Storage covert channels [23] are not secure. They are detectable and can be eliminated from the system. Some other covert channels are secure enough but suffer from low bit rate [7,8,15,17]. The covert channel proposed in [16] sacrifices its bit rate to achieve high security. The methods mentioned in [27,28] are not practical because they use algorithms that are not practically so common. Some others [15, 25] only care about their long time behavior. Thus, they will be easily detected by short time monitoring of the system behavior. In this paper, a method is proposed to establish a covert channel in IEEE 802.11, which has high security along with high bit rate in comparison with the existing methods.

4. COVERT TECHNIQUES

Highlights of some techniques that how undisclosed communications can be embedded in covert channels is explained as below:

4.1. Unused Header Bits:

By exploiting protocols, such as TCP/IP, it is possible to encode a covert channel using reserved or unused bits of their headers, as proven in [26]. If there is no confirmation on the receiver or the protocol specifications do not impose explicit values, hidden data can be transmitted, (e.g. in "type of service" field of the IP header). In figure 1 we can see TCP/IP header and their exploitable fields, marked as underlined.

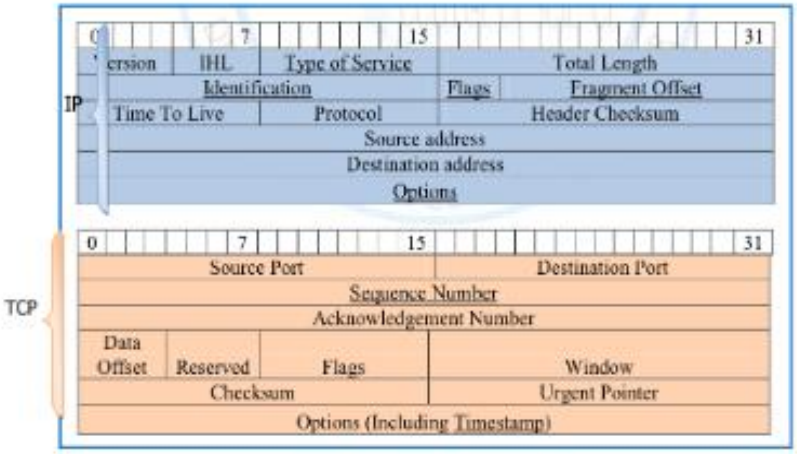

Figure 1. TCP/IP Header Structure [28]

Another possible exploit regards padding bits. Again, if the no specific value is imposed for padding, information can be covert within those bits.

4.2. Optional Header Fields:

In spite of the usage of predefined header extensions regarding discretionary information transport on requisition, several protocols consent unheralded data to be carried in header extensions in order to augment the proficiency of protocols. One simple example is to covert masked data as an IP address in route record option.

4.3. Semantic Overloading of Header Fields:

A different approach regarding covert techniques is the semantic overloading. It consists of exploiting syntactic variations of the overt channel to encode covert data whilst the channel is maintained semantically identical. For example, hidden content can be encoded using TCP sequence numbers in TCP header. In order to do it, the client chooses the ISN (Initial Sequence Number), and it should be carefully chosen to prevent new incarnations sequence numbers to overlap with the ISNs previous ones. One example of a covert channel created in these circumstances is the use of each ISNs most significant byte, while enforcing the remainders to be set as zero, as proven in [4]. Higher layer protocols, mainly text based ones, like Hypertext Transfer Protocol (HTTP), offer further opportunities. By simply varying the use of upper and lower case, or the amount of spaces interleaving words, covert channel can be created.

4.4. Packet and Message Sequence Timing:

Another technique relies on sequence timing. To establish a covert channel, in every time interval the sender adjusts its packet rate, while on the receiver's side, in order to decode the concealed data, he needs to measure the rate of the packets in each time interval. However, packet timing channels required synchronization mechanisms at both, sender and receiver sides, in order to alter the packet rate and obtain proper readings at the destination.

4.5. Payload Tunneling:

This technique consists of using the payload tunneling one protocol into another. The major goal of this approach is to bypass firewalls responsible for restraining outgoing transmissions to a brief set of authorized application protocols, such as HTTP. Such methods can even be applied to Domain Name Server (DNS), tunneling information through the protocol. In this case, the client would request a name resolution for the host in the form of host.covertserver.com, where covertserver.com would be a modified DNS server participating in the covert channel, and host would be encoded covert data. All the covert information would be sent from the DNS server to the client in the DNS responses as text records.

5. APPLICATIONS OF COVERT CHANNELS

Applications of covert channels with some practical implementations are given below:

5.1. Covert Communication in Social Networks:

With facebook's acceptance and usage spreading worldwide, it became a craved target for covert channels. Such exploitation was performed in [12]. In this article, the authors have successfully implemented means to use social networks as a pipe for covert communications, specifically targeting facebook. The authors created an application, named FaceCat which operates based on users facebook accounts. Firstly, the software reaches for long-term cookies stored in cache. After successfully retrieved said cookies, the software starts to operate as an authenticated facebook user.

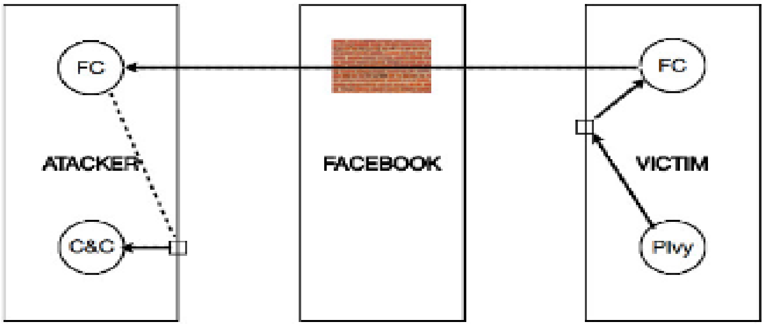

Figure 2. FaceCat operation method (from [12])

By manipulating cookies, a TCP session is established between the master node wall, the "attacker", and unrelated account walls, the "victims". The master node writes its own cookie on its wall, and waits for connections. FaceCat is now able to read the cookie and, using a method, which authors called "pass-the-cookie", gain the ability to write on master's wall. Communications works using Base64 encoding as well as sequence numbers. The authors choose facebook's mobile interface as it was easier to parse and obtain the encoded messages and use Poison Ivy as a Remote Administration Tool (RAT), with the purpose of interpreting concealed data.

5.2. Covert Communication with skype:

Skype is currently one of the most used P2P communication systems with a number of users of around 35 million [3]. Using the IP protocol, skype communication is made in a high cryptographic manner. Such communication aims to guarantee privacy for Skype users, but it also covers said communication from firewalls as they usually do not verify ciphered contents and therefore creates an ideal ambient for covert communication. Skype uses the UDP protocol for communications and, as many other protocols, it is susceptible to covert techniques, such as network covert storage channels through packet field manipulation. In [9], the authors successfully used Skype's 70 bit packets that do not carry speech, to conceal communications success-

Fully. Such exploit is due to Skype's method of transmitting data. Even though no dialog is being performed, like text or audio communication, skype continuously send data packets during the session time, as explained in [3].

5.3. Covert Communication in TCP/IP:

We must start this discussion by firstly introducing some concepts regarding TCP/IP. TCP/IP is a computer networking model and a set of communication protocols widely used on the Internet. It is composed by the TCP protocol for reliable communication and IP protocol for routing functions. The protocol's header is the combination of both, TCP and IP. In [26], Craig H. Rowland successfully implemented undisclosed communications using TCP/IP packet headers, adopting three different approaches.

5.3.1 Manipulation of the IP Identification Field:

TCP/IP uses the IP identification field to reassemble packet ordering at the destination node. If - by some reason - a packet was to be lost along the way, the destination router would be aware of the lack of such packet and could not reconstruct data accurately until a retransmission of the packet would be received. By using a simple method of placing the ASCII representation of the characters he wished to encode in the identification field, Rowland managed to pass the word ”HELLO” hidden, being subsequently reconstructed at the destination node. This method consists of having the client host to build a packet with the correct destination host, encoded IP ID field and data regarding the source host. The remote host, while listening on a passive socket, receives the packet and decodes the information. Although effective, this implementation is easily detectable by firewalls and there is a high probability of losing data due to the need of packet overwriting by routers (TTL for example).

5.3.2 Initial Sequence Number Field:

The second approach taken by the author consists in modifying the Initial Sequence Number Field. This field is used in the three-way handshake implemented by TCP in order to establish a reliable protocol negotiation with a remote server. It comes as an ideal field to conceal communications as it has a reserved 32 bit size. As in the previous example, the author encapsulates ASCII coding that refers to a given character in this field. They define the communication as a synchronized communication and encapsulate the ASCII code, taking in account the generation of more realistic sequence numbers through divisions.

5.3.3 The TCP Acknowledge Sequence Number Field "Bounce":

Finally, the author refers to a third and last method entitled as The TCP Acknowledge Sequence Number Field "Bounce". In this method, the author uses basic IP spoofing (packet manipulation in order to forge the sender IP address) and bouncing technique (using IP spoofing, a packet is sent to a given server that then replies with an ACK/SYN with ISN +1). Basically, a packet is created with forged source IP address, port, destination IP address (the target system), destination port and a TCP SYN number forget with the data they wish to transmit. Then, it is sent to a bounce server that receives the packet, increments ISN by one number and replies to the forget IP address in the packet. The receiver system expects communication from the bounce server and when received, it interprets the ISN number minus one and therefore the ASCII value of the character.

6. CONCLUSION AND FUTURE SCOPE

Thus going through the different review papers it is observed covert channel can be used as an effective tool to provide the security to critical and sensitive data in the wireless adhoc networks. Its effectiveness increases many folds if sensitive data is of short burst as then it becomes very difficult for the third party to detect that a secret communication is being going on between the sender and receiver. It is transferring information and data even in high security without altering the firewall or security contents. We also studied its applications on skype, facebook etc.

This study also suggests that covert channel is an emerging and hot topic for researchers. Many new algorithms can be generated and many old algorithms can be exploited to make covert channel technique more secure and effective in ad hoc wireless communication.

7. REFERENCES

[1] P. Prendergast, "Covert Channels over Network Traffic: Methods, Metrics, and Mitigations", Department of defense science and technology (2017).

[2] F. Rezaei, M. Hempel, H. Sharif, "Towards a Reliable Detection of Covert Timing Channels over Real-Time Network Traffic", IEEE Transactions on Dependable and Secure Computing 14, no. 3,pp: 249-264, 2017.

[3] Jiangtao Zhai, Mingqian Wang, Guangjie Liu, and Yuewei Dai. Skylen: a skype-based length covert channel,2015

[4] Zhao H, Chen M. WLAN covert timing channel detection. Wireless Telecommunications Symposium (WTS) 2015; 2015: 1–5.

[5] Kimi Manchanda, Amarpreet Singh, "Covert Communication in VANETS using Internet Protocol Header Bit", International Journal of Computer Applications, Volume 123, Issue No. 17, August 2015.

[6] Asst Prof Dr Ziyad Tariq Mustafa and Authman Waleed Khalid. Packet steganography using ip id,2014.

[7] Zhang D, Du P, Yang Z, Dong L. Research on Covert Channels Based on Multiple Networks, Web technologies and applications 2014: 365–375.

[8] Zhao H. Covert channels in 802.11 e wireless networks, in Wireless telecommunications symposium (WTS), 2014: 2014.

[9] Wojciech Mazurczyk, Maciej Karas, and Krzysztof Szczypiorski. Skyde: A skype-based steganographic method. arXiv preprint arXiv:1301.3632, 2013.

[10] Salmanian M, Li M. A High Throughput Covert Overlay Network within a MANET, Military communications conference, MILCOM 2013-2013 IEEE 2013: 586-592.

[11] Kiyavash N, Koushanfar F, Coleman TP, Rodrigues M. A timing channel spyware for the CSMA/CA protocol. Information Forensics And Security, IEEE Transactions On 2013; 8(3): 477–487.

[12] Jose Selvi. Covert channels over social networks. In SANS Institute Reading Room site. SANS Institute, 2012.

[13] Ahmadzadeh SA, Agnew G. Behavioral mimicry covert communication. Security and Privacy in Communication Networks 2012; 96: 134–153.

[14] Goher S, Javed B, Saqib N. Covert channel detection:A survey based analysis, in High capacity optical networks and enabling technologies (HONET), 2012 9th international conference on 2012: 057–065.

[15] Calhoun TE, Cao X, Li Y, Beyah R. An 802.11 MAC layer covert channel. Wireless Communications and Mobile Computing 2012; 12(5): 393–405.

[16] Holloway R Beyah R. Covert DCF: A DCF-Based Covert Timing Channel in 802.11 Networks, in Mobile adhoc and sensor systems (MASS), 2011 IEEE 8th international conference on, 2011.

[17] Li S, Ephremides A. Covert channels in ad-hoc wireless networks. Ad Hoc Networks 2010; 8(2): 135–147.

[18] Guangjie Liu, Jiangtao Zhai, Yuewei Dai, Zhiquan WangCovert Timing Channel with Distribution MatchingProceedings of International Conference on Multimedia Information Networking and Security,2009, 565-568

[19] Murdoch, S. J., “Covert channel vulnerabilities in anonymity systems”, Ph.D. thesis, University of Cambridge (2007), technical report UCAM-CL-TR-706.

[20] G. I. . W, IEEE 802.11 WG. Part 11: wireless LAN medium access control, IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), 2007.

[21] Zander S, Armitage GJ, Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys and Tutorials 2007; 9: 44–57.

[22] Sebastian Zander, Grenville Armitage, and Philip Branch. A survey of covert channels and countermeasures in computer network protocols. Communications Surveys & Tutorials, IEEE, 9(3):44–57, 2007.

[23] L. Butti and F. Veysset, Wi-fi advanced stealth, Proc. Black Hat US, Aug, 2006.

[24] Cabuk S, Spafford EH, Brodley CE. “Network Covert Channels: Design, Analysis, Detection, and Elimination. Purdue University: West Lafayette, IN., USA, December 2006.

[25] Christian K, Dittmann J, Lang A, Kühne T. WLAN steganography: a first practical review, Proceedings of the 8th workshop on Multimedia and security 2006: 17–22.

[26] Craig H. Rowland. Covert channels in the tcp/ip protocol suite. First Monday, 2(5), 1997.

[27] M. Wolf, “Covert channels in LAN protocols”, in Proceedings of the Workshop on Local Area Network Security (LANSEC’89) (T.A.Berson and T.Beth, eds.), 1989, pp.91 – 102

[28] C. G. Girling, “Covert channels in LAN’s”, vol. SE-13of 2, IEEE Transactions on Software Engineering, February1987

[29] National Computer Security Center, US DoD, “Trusted Computer System Evaluation Criteria” , Tech. Rep. DOD 5200.28- STD, National Computer Security Center, Dec. 1985, http://csrc.nist.gov/publications/history/dod85.pdf

[30] L. Qiu, Y. Zhang, F. Wang, M. Kyung, and H. Mahajan, “Trusted computer system evaluation criteria”, in National Computer Security Center, Citeseer, 1985.

[31] G. J. Simmons, “The Prisoners’ Problem and the Subliminal Channel”, in Proceedings of Advances in Cryptology (CRYPTO), pp. 51–67, 1983.

[32] B. Lampson, “A Note on the Confinement Problem”, Communications of the. ACM, vol. 16, no. 10, Oct. 1973, pp. 613-615.