Damascus University Journal for engineering sciences
Vo 42 number (1) -2026: 299-306

مجلة جامعة دمشق للعلوم الهندسية
المجلد42 العدد (1) – 2026: 299-306

Case Study of Data Leakage Through Keylogger and Through a Covert Channel in IP Protocol, And the Potential Size of the Leakage

Mohammad Yamen Hallak *[1]

*1. Information Technology Engineer – Master's Degree in Computer Systems and Networks Engineering – Faculty of Information Technology Engineering – Damascus University - yamen.hallak@damascusuniversity.edu.sy

Received: 18/6/2023
Accepted: 24/8/2023

Abstract:

The threats surrounding computer data are still growing with network and technical progress around the world, and in parallel; there has been an increased interest in the security of computer data and maintaining the privacy of data transmitted over the network. Leakage of user data is a serious security threat due to the disclosure of the privacy of data that may be confidential and should only be viewed by authorized parties. With the emergence of covert channels, the risk of data leakage increased even more due to the ability of these channels to leak data in a hidden way that is difficult to detect, as these channels depend on the basis of their work to hide themselves. In this research, a network application was developed that eavesdrops on the user's keyboard (Keylogger), and leaks the characters that the user has pressed, by designing a covert channel represented by the TTL field of the IP protocol, and clarifying how this channel works, and the amount of data that will be leaked through this field only.

Keywords: Covert Channels, Keylogger.

ISSN (online): 2789-6854
http://journal.damascusuniversity.edu.sy/index.php/index/index

دراسة حالة تسريب البيانات من خلال مدوّن ضغطات لوحة المفاتيح وعبر قناة مخفيّة في البروتوكول IP وحجم التّسريب المحتمل

محمّد يامن حلّاق [1*]

[1*] .مهندس معلوماتيّة، ماجستير في هندسة النّظم والشّبكات الحاسوبيّة – كليّة الهندسة المعلوماتيّة – جامعة دمشق – yamen.hallak@damascusuniversity.edu.sy

الملخص:

مازالت التّهديدات التي تحيط بالبيانات الحاسوبيّة تتنامى مع التّقدّم الشّبكي والتّقني حول العالم، وعلى التّوازي؛ ازداد الاهتمام بأمن البيانات الحاسوبيّة والمحافظة على خصوصيّة البيانات المنقولة عبر الشّبكة. إنّ تسريب بيانات المستخدمين يعتبر تهديداً أمنيّاً خطيراً نظراً لكشف خصوصيّة البيانات التي قد تكون سرّيّة ولا يجب الاطلاع عليها إلّا من الأطراف المخوّلة لذلك. ومع ظهور القنوات المخفيّة ازداد خطر تسريب البيانات بشكل أكبر نظراً لقدرة تلك القنوات على تسريب البيانات بشكل خفي ومن الصّعب كشفه، حيث أنّ هذه القنوات تعتمد في أساس عملها على إخفاء نفسها. جرى في هذا البحث تطوير تطبيق شبكي يتنصّت على لوحة مفاتيح المستخدم (Keylogger)، ويقوم بتسريب المحارف التي قام المستخدم بالضّغط عليها، وذلك من خلال تصميم قناة مخفيّة متمثّلة بالحقل TTL من البروتوكول IP، وتوضيح كيفيّة عمل هذه القناة، وحجم البيانات التي سيجري تسريبها من خلال هذا الحقل فقط.

الكلمات المفتاحية: القنوات المخفيّة، Keylogger

.

تاريخ الإيداع: 2023/**6/18**
تاريخ القبول: 2023/8/24

experiment). After that, it will conduct an analysis of the network traffic to ensure the validity of the data leakage and to measure the amount of data that will be leaked by relying only on this field, and it will be ensured that the data to be leaked does not constitute a significant volume or a noticeable burden on network traffic (Caviglione, 2021).

The rest of the paper will be organized as follows: Section (2) presents related works on similar research; Section (3) provides a description of the experiment; Section (4) covers the practical experiment; Section (5) studies the results that have been obtained, and finally, Section (6) summarizes the paper.

1. Related Works

Some similar works that dealt with covert channels in their subjects were studied. In ((Smeets et al,. 2006), (DOD, 1985)), covert channels were classified into two types: 1) Storage Covert Channels, where one procedure writes directly or indirectly to a specific location, and another procedure reads from the same place, thus leaking data between the communicating parties (and this is the model that will be used in this research); and 2) Timing Covert Channels, where timing properties are modified to leak data ((Vishnoi, 2018), (Zander et al,. 2007)).

By reading ((Smeets et al,. 2006), (Zander et al,. 2007)), many IP, TCP, ICMP, and other protocol fields were mentioned that could be exploited to leak data covertly, and those papers also discussed some theoretical proposals that could be used to prevent these channels.

In (Orkhavi et al,. 2010), covert channels were classified, and the design and implementation of attacks were discussed based on the transmission mechanism, whether the channel was storage or timing, and based on the network, operating system, hardware, and others. As mentioned in (Zander et al,. 2007), the concept of payload tunneling was discussed to achieve data leakage by including a protocol within the payload of another protocol, creating a covert channel capable of bypassing firewalls that may prevent one of the protocol types (such as including the SSH protocol within the IP protocol payload to bypass the firewall).

Regarding the detection of covert channels, research ((Chen et al,. 2021), (Hammouda et al,. 2008),

Introduction:

The increasing capacity and availability of modern communication features have led users to utilize networks more frequently, resulting in a more complex user behavior on the network. This, in turn, has increased the potential for network violations. Therefore, monitoring and analyzing current events on the network is essential for forensic auditing in order to obtain evidence of violations ((Callado et al., 2009),(Sikos et al., 2020)). The leakage of data is considered a network violation that poses a danger to users' data. The data being leaked may be sensitive, and the leakage occurs through communication channels, which is described by the concept of a covert channel (Frolova et al,. 2021).

Scientific research has dealt with the concept of covert channel due to its importance in causing a violation in the channels of communication and the leakage of data between parts of the same network or even outside the network, which leads to disclosure of the privacy of users' data. The concept of the covert channel was mentioned for the first time through a note made by (Lampson) in 1973, who considered that covert channels are channels that are not intended for transmitting information at all, and likewise the burden of service programs on system performance (Lampson, 1973). In another definition, covert channel is a communication channel that allows information to be transmitted in a way that violates the system security policy ((Smeets et al,. 2006), (DOD, 1985), (Rowland, 1997)), and its danger lies in being an invisible, undetectable, and dangerous security attack (Elsading et al,. 2018).

The basic idea of a covert channel is to hide secret messages (covertly) within overt network packets, exploiting redundant or unused fields in network communication protocols so that data can be leaked. Therefore, a protocol is needed to be used as a carrier for the leaked data ((Vishnoi, 2018), (Zander et al,. 2007)).

In this research, the case of hiding data within the TTL field of the IP protocol will be discussed by carrying the value of the character that is pressed on the keyboard by the user (Keylogging), so that the data that the user types on the keyboard will be leaked by injecting it into the TTL field and directing it to the attacker via the network application (which will be described in the

Time to Live (TTL) field. Figure (1) illustrates IPv4 packet header (RFC 791, 1981) and the size of TTL field within it:

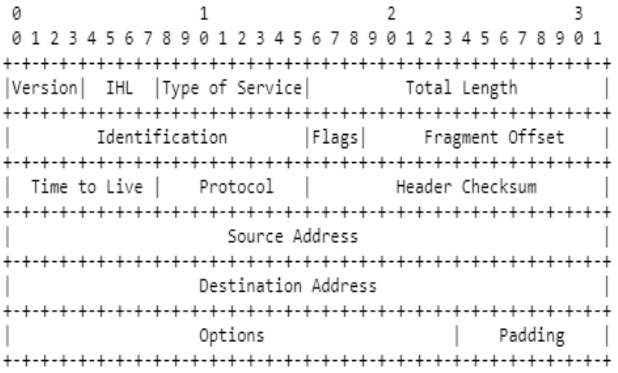

Figure (1) IPv4 protocol header according to RFC 791

The data represented by the TTL field, which contains the value of the character that the user pressed on the keyboard, will be leaked. The packet will then be sent to the attacker, who will analyze the network traffic and extract the IP packets that were received from the victim. The attacker will read from the same location that the malicious network application wrote on (i.e., the TTL field) and extract the value of the TTL field, which will contain the value of the leaked data from the victim, including the character that was pressed on the keyboard. Figure (2) shows the operational specifications that were tested, including the topology and network parameters.

Note: The attacker and victim were simulated as virtual machines using VMWare Workstation[1]. Network traffic analysis was performed using TCPDump[2] tool and Wireshark[3] software. The network application that acts as a keylogger and

[1] https://www.vmware.com/products/workstation-pro.html
[2] https://www.tcpdump.org/
[3] https://www.wireshark.org/

(Zander, 2017), (Caviglione, 2021), (Guandi et al,. 2017)) discussed some proposed methods for detecting certain forms of covert channels (such as: specific protocol; specific fields; specific lengths; covert channel limitation, elimination and prevention; the ability of some intrusion detection systems or proposed systems to detect covert channel attacks, etc.). Moving on (Frolova et al,. 2021), a normalization of network traffic was performed to reduce data leakage and detect covert channels of the type "packet length covert channel," which exploits the lengths of network packets to transmit confidential information.

A comprehensive literature review was presented in (Tian et al,. 2020), focusing on previous work related to covert channels, including techniques for constructing network covert channels, covert channel metrics, and attacks against network covert channels. Additionally, the paper addresses modern network environments such as streaming media, blockchain, and IPv6.

By examining previous works, it becomes clear that it is important to discuss covert channels and their potential threats of data leakage, which may be as small as one bit with each data packet transmitted over the network ((Zander et al,. 2007), (Orkhavi et al,. 2010), (Fisk et al,. 2002)). It is also important to access realistic and practical statistical data about data leakage that may occur by exploiting one of the protocol fields, and to display the size of that leak, which may not be noticeable in terms of the size of the network traffic flow.

2.Experiment Description.

In this section, a scenario of an experiment will be presented, where a victim clicks on a malicious network application that is presented to them through phishing concepts based on social engineering (Leonov et al,. 2021). The application operates in the background without the user's knowledge and eavesdrops on the keystrokes that the user presses. A network packet is then formed, containing a covert channel with the content being the value of the character that the user pressed through the keyboard.

Based on previous studies ((Smeets et al,. 2006), (Zander et al,. 2007)) that mentioned several protocols and their fields that can be used to leak data covertly, this research relies on IP protocol as the carrier of the covert channel, specifically the

(e.g., in notepad, on a website, in a program, etc.). By analyzing the network traffic on the attacker's computer, the following output will be observed (the packets will be separated by a line of dashes to distinguish the packets from each other, and the leaked character will be marked in the TTL field):

```
0000    00 0c 29 cc 1a 23 00 0c 29 10 e5 b6 08 00 45
04    ..)..#..).....E.
0010    00 14 00 00 40 00 48 06 93 19 c0 a8 12 ad c0
a8    ....@.H.........
0020    12
b5
  ..
---------------------------------------------------------------------
0000    00 0c 29 cc 1a 23 00 0c 29 10 e5 b6 08 00 45
04    ..)..#..).....E.
0010    00 14 00 00 40 00 45 06 93 19 c0 a8 12 ad c0
a8    ....@.E.........
0020    12
b5
  ..
---------------------------------------------------------------------
0000    00 0c 29 cc 1a 23 00 0c 29 10 e5 b6 08 00 45
04    ..)..#..).....E.
0010    00 14 00 00 40 00 4c 06 93 19 c0 a8 12 ad c0
a8    ....@.L.........
0020    12
b5
  ..
---------------------------------------------------------------------

0000    00 0c 29 cc 1a 23 00 0c 29 10 e5 b6 08 00 45
04    ..)..#..).....E.
0010    00 14 00 00 40 00 4c 06 93 19 c0 a8 12 ad c0
a8    ....@.L.........
0020    12
b5
  ..
---------------------------------------------------------------------
0000    00 0c 29 cc 1a 23 00 0c 29 10 e5 b6 08 00 45
04    ..)..#..).....E.
0010    00 14 00 00 40 00 4f 06 93 19 c0 a8 12 ad c0
a8    ....@.O.........
0020    12
b5
  ..
```

Consequently, the success of data leakage will be observed, as it was fully injected in the victim and reached the attacker, and could be easily extracted through simple tools in network traffic analysis.

2. Results Studying

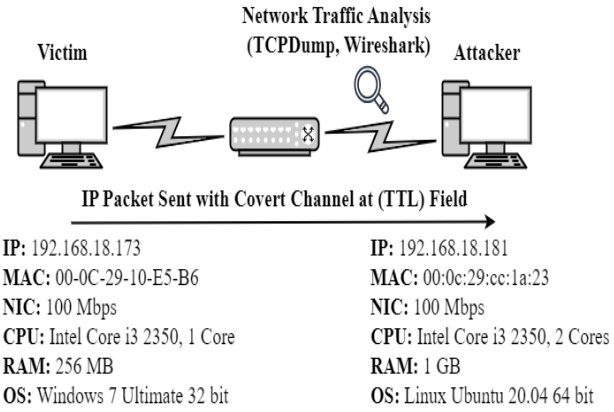

Figure (2)- Network topology and operational specifications that the experiment was conducted on

creates the packet that contains the covert channel was developed using Winpcap[4] library.

The network application that will run on the victim's computer follows the following general algorithm[5]:

```
Hide The Program from Taskbar;
While (true)
Character = Get(Key_Pressed); //Keylogging

Set Fields of IP_Packet (SRC_MAC, DST_MAC,
SRC_IP, DST_IP, TOS,…);
IP_TTL = Character;
Send_Packet(IP_Packet);
End
```

It is worth mentioning here that character encoding was done by adopting the Extended ASCII[6] table, where characters are represented using 8 bits (with the same size as the TTL field).

1. p

ractical experiment

In this section, a practical experiment will be conducted using a simple example to observe the functioning of the experiment.

By running the proposed application on the victim's computer as an experiment, the victim will type the following word "HELLO" anywhere they choose

[4] https://www.winpcap.org/

[5] The full code can be accessed through the following link: https://github.com/YamenHallak/Data-Leakage-Through-KeyLoggers-and-Through-a-Covert-Channel-in-IP-Protocol/blob/main/Data-Leakage-Through-KeyLoggers-and-Through-a-Covert-Channel-in-IP-Protocol.cpp

[6] https://www.ascii-code.com/

working days)	60 minute	250,800	244.9 KB
	120 minute	501,600	489.8 KB
	180 minute	752,400	734.8 KB
annually (250 working days)	1 minute	47,500	46.39 KB
	60 minute	2,850,000	2.7 MB
	120 minute	5,700,000	5.4 MB
	180 minute	8,550,000	8.1 MB

Upon examining websites that measure typing speed, it was found that the average typing speed is about 40-41 words per minute ((tybaa.com, n. d.), (rataype.com, n. d.)), which translates to approximately 190-200 characters being typed per minute (livechat.com, n. d.). Assuming that the leaked character is represented by 8 bits (depending on the size of the TTL field), and given that 190 characters are being typed, Table (1) shows some approximate statistics.

Thus, it was observed that the number of characters being leaked is not insignificant, especially if they contain confidential data. However, the data size of the leaked characters is small and does not impose a significant burden on the computer network (Caviglione, 2021). It only takes 8.1 megabytes to leak more than 8.5 million characters annually (if typing is only for 3 hours per day).

3. Conclusion:

In summarizing the research, the paper highlights the danger of covert channels to users' data privacy. This paper presents a network application designed to listen for a user's keyboard input and leak it within the TTL field of the IP protocol, creating a covert channel. The practical experiment conducted in this paper demonstrates that approximately 8.5 million characters can be leaked annually using only one field of 1-byte size, without significantly affecting the volume of network traffic.

Based on the foregoing, it is clear that there is a need for a comprehensive discussion of covert channels to understand their formation and the extent of data leakage. This leaves an opportunity for researchers to conduct further statistics related to data leakage through other forms of covert channels and to find deterrent solutions for those channels through detection, prevention or limitation.

Funding: this Research Is Funded By DamascusUniversity-Funder No (501100020595).

Table (1) - Approximately statistics related to the size of data leakage over time

Rate	Typing Time	Number of clicks (the number of characters that are leaked)	Leaked Data Size
Daily	1 minute	190	0.186 KB
	60 minute	11,400	11.13 KB
	120 minute	22,800	22.27 KB
	180 minute	34,200	33.39 KB
Monthly (22	1 minute	4,180	4.08 KB

DoD Trusted Computer System Evaluation Criteria. (1985). Supercedes CSC-STD-001-83, dtd 15 Aug 83.

Elsadig, M. A., & Fadlalla, Y. A. (2018). Packet Length Covert Channel: A Detection Scheme. https://doi.org/10.1109/cais.2018.8442026 .

Fisk, G., Fisk, M., Papadopoulos, C., & Neil, J. (2002, December 18). Eliminating Steganography in Internet Traffic with Active Wardens. Information Hiding, 18–35. https://doi.org/10.1007/3-540-36415-3_2.

Frolova, D., Kogos, K., & Epishkina, A. (2021). Traffic Normalization for Covert Channel Protecting. https://doi.org/10.1109/elconrus51938.2021.9396163 .

Gunadi, H., Zander, S. (2017). Comparison of IDS Suitability for Covert Channels Detection. Murdoch University IT NSRG Technical Report 20170818A.

HAMMOUDA, S., MAALEJ, L., & TRABELSI, Z. (2008). Towards Optimized TCP/IP Covert Channels Detection, IDS and Firewall Integration. 1-5. 10.1109/NTMS.2008.ECP.101.

Lampson, B. (1973). A note to the confinement problem. Communications of the ACM, 16(10), 613–615.

Leonov, P. Y., Vorobyev, A. S., Ezhova, A. A., Kotelyanets, O. S., Zavalishina, A., & Morozov, N. (2021). The Main Social Engineering Techniques Aimed at Hacking Information Systems. In 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). https://doi.org/10.1109/usbereit51232.2021.9455031 .

LiveChat | Web Live Chat Software & Online Customer Support. LiveChat. https://www.livechat.com/.

Okhravi, Hamed & Bak, Stanley & King, Samuel. (2010). Design, implementation and evaluation of covert channel attacks. 481 - 487. 10.1109/THS.2010.5654967.

Postel, Jon: RFC 791 - Internet Protocol Specification, 1981, http://www.ietf.org/rfc/rfc791.txt.

Ratatype — Online Touch Typing Tutor and Typing Lessons. https://www.ratatype.com/.

Rowland, C. H. (1997). Covert channels in the TCP/IP protocol suite. First Monday, 2(5). https://doi.org/10.5210/fm.v2i5.528.

References:

Callado, A., Kamienski, C., Szabo, G., Gero, B. P., Kelner, J., Fernandes, S., & Sadok, D. (2009). A Survey on Internet Traffic Identification. IEEE Communications Surveys & Tutorials, 11(3), 37–52. https://doi.org/10.1109/surv.2009.090304

Caviglione, L. (2021). Trends and Challenges in Network Covert Channels Countermeasures. Applied Sciences, 11(4), 1641. https://doi.org/10.3390/app11041641

Chen, S., Lang, B., Liu, H., Li, D., & Palmer, N. D. (2021). DNS covert channel detection method using the LSTM model. Computers & Security, 104, 102095. https://doi.org/10.1016/j.cose.2020.102095

Sikos, Leslie. (2020). Packet Analysis for Network Forensics: A Comprehensive Survey. Digital Investigation. 32C. 10.1016/j.fsidi.2019.200892.

Smeets, M., Koot, M. (2006) Covert Channels, Research Report. University of Amsterdam, Amsterdam.

Tian, J., Xiong, G., Li, Z., & Gou, G. (2020). A Survey of Key Technologies for Constructing Network Covert Channel. Security and Communication Networks, 2020, 1–20. https://doi.org/10.1155/2020/8892896

Vishnoi, Vibhor. (2018). AN OFFLINE AND EFFICIENT STORAGE COVERT CHANNEL DETECTION MECHANISM. 10.1729/Journal.22251.

Zander, S. (2017). Bro Covert Channel Detection (BroCCaDe) Framework: Scope and Background.

Zander, Sebastian & Armitage, Grenville & Branch, Philip. (2007). Covert channels and countermeasures in computer network protocols. IEEE Communications Surveys and Tutorials. 9. 44-57. 10.1109/COMST.2007.4317620.

تدرب على إدخال الباء، التاء، النون، الياء والمسافة. أكاديمية الطباعة. https://www.tybaa.com/.