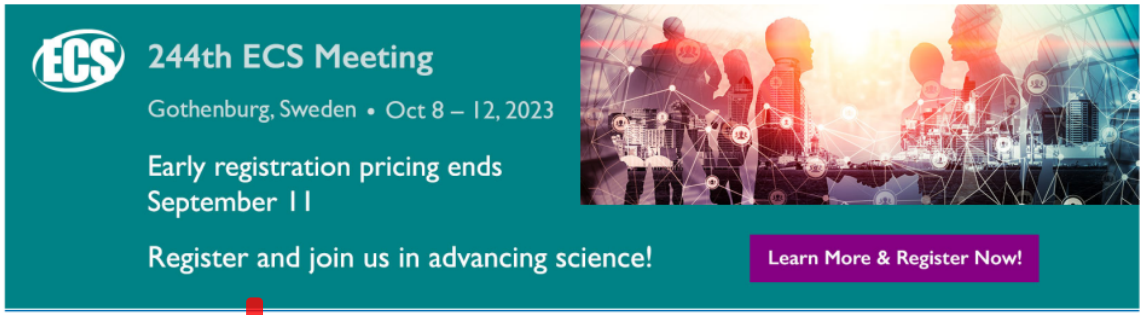
9_Protecting Data By Socket Programming Steganography

by WT Handoko

Submission date: 26-Oct-2023 08:38PM (UTC+0700)
Submission ID: 2206703412
File name: 9_Protecting_Data_By_Socket_Programming_Steganography.pdf (637.29K)
Word count: 2886
Character count: 15745

Protecting Data By Socket Programming Steganography



Protecting Data By Socket Programming Steganography

WT Handoko[1], E Ardhianto[2*], K Hadiono[3], FA Sutanto[4]
[1,2,3,4]Universitas Stikubank

Email : [*]ekaardhianto@edu.unisbank.ac.id

Abstract. This paper aims to observe the techniques and methods of securing data using socket programming steganography. This work observes the development of the art of steganographic techniques which focus on computer network devices by visiting articles which published in journals and proceedings. The results obtained that the development of steganography is not only on data which stored on local disk, but also utilizes computer network devices to transmitting the data. Steganography techniques have several modifications in the algorithm to secure data on the network using stegnography that uses socket programming. This results show the evolutions of steganography techniques on network devices for better data security.

1. Introduction

Network path is a line that connects communication between many entities. This line provides services for sending data from sender to receiver. The data sent will run through a network layer mechanism that is processed by a program called socket programming.

In data protection, cryptographic techniques can provide security by encrypting and decrypting [1]. Even so attacks on a ciphertext can still occur. This is because of cryptography mechanism, the product of cryptography still shows suspicion of an undisclosed message. Steganography comes by hiding messages into a cover. The advantage of steganography is that unauthorized people are not realize of the existence of a message [1]. The role of the internet and communication networks is now accommodating in the exchange of data and information. This is very beneficial for accelerating the delivery of a message. But keep in mind that the confidentiality of data and information is something that needs attention. Steganography mechanism can provide power in hiding data through a cover [2].

In 2003, a study conducted a merging of steganography with network technology called Network Steganography [3]. This is become new approach for hiding data in TCP/IP network layer protocol [1]. This will result in data hiding becoming stronger and more difficult to detect. TCP / IP has been perfectly developed and offers many performance improvements for secure access and data transfer [4]. Many devices that are currently connected to each other are easily controlled using socket programming [5]. The main point of network steganography is to use 7 protocols in Open System Interconnection (OSI) as a cover of data [3]. This article presents the development of protection data using steganography with it's algorithm modifications and using socket programming at the network layer.

2. Method

The research method used in this paper is visitting articles which published in journals and proceedings. Several phases of work are planning, condutcing and reporting, which can be illustrated as below in figure 1.

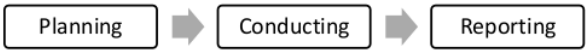


Figure 1. Phases of Work

Planning phase is the initial stage in conducting research. This phase determines the topic and the Research Question (RQ) which will be used as a guide for the process of conducting research. As a topic taken is socket programming steganography. The RQs used are "Are there research activities on stegaography in the network carried out at transport or network layers?" as RQ1, "What is the steganography process that takes place at the transport or network layer?" as RQ2 and "is there still a possibility of developing steganography in the network layer?" as RQ3.

Conducting stage is the implementation of research activities. In this phase several steps are taken, the strategy of selecting literature, filtering literature and assessing quality, as shown in figure 2.

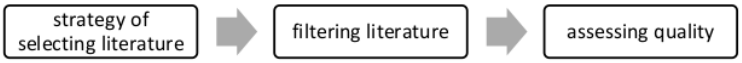


Figure 2. Implementation Phase

The first step in the implementation phase is a strategy for selecting literature, which is preceded by selecting keywords and sources of literature. After determining the source and search restriction, the next step is to determine the keywords which are then followed by filtering literature. The quality assessment done by accessing the scimagojr.com to see the quality of the journals that contain the articles obtained. The next step in quality assessment is to synthesize the articles obtained by reading the entire article so that it matches the topic and the research question specified.

3. Results and Discussions

The source of the literature used is a database of research articles contained on the page scholar.google.com. The literature search process is limited to articles in the form of journals and proceeding conferences with the publication year 2015 to three quarter 2019.

In this research, articles are searched by using several keywords. The first keyword is "steganography in socket programming", which on the search page produces 345 results. In the first search, after reading the title and abstract 14 articles were produced which were quite suitable and could be fully downloaded. The second term is "steganography socket programming" which features 261 articles. In the second search produced 14 articles that can be fully downloaded. And the third term is "steganography in transport layer", in the third search found 20 articles that can be fully downloaded. So, it obtained 48 articles with relevance based on the title and abstract. There are 40 papers published in journals which 4 papers published in Q1 journals, 2 papers published in Q2 journals, 4 published papers in Q3 journals, 4 published papers in Q4 journals and 26 papers published in journals unknown refered to schimagojr.com. 8 papers are published in proceeding conferences.

In quality assessment phase, it resulted 30 articles that are quite relevant and there are 12 articles that are relevant to the question reaearch. Table 2 shows relevance between the topic and question research.

Tabel 1. Paper's Qualifications

	Journal Qualification					Total
	Q1	**Q2**	**Q3**	**Q4**	**Unknown**	
Paper's on Journal	4	2	4	4	26	40
Proceeding Conference	-	-	-	-	-	8

Table 2. Relevance of articles to the topic

No	Paper's Index	Qualification	Topic Discussion		
			Cryptography	Steganography	Transport / Network Layer
1	[6]	-	Y	Y	-
2	[1]	-	Y	Y	Y
3	[7]	-	-	-	Y
4	[8]	-	Y	Y	Y
5	[2]	-	-	Y	Y
6	[3]	Q4	-	Y	Y
7	[9]	Q3	Y	-	Y
8	[10]	Q4	Y	-	Y
9	[11]	-	-	Y	Y
10	[12]	-	Y	-	Y
11	[13]	Q1	-	Y	Y
12	[14]	-	Y	Y	Y
13	[15]	-	Y	-	Y
14	[16]	-	-	Y	-
15	[17]	-	Y	Y	-
16	[18]	-	-	Y	-
17	[19]	-	-	Y	-
18	[20]	-	-	Y	-
19	[21]	-	Y	-	-
20	[22]	Q1	-	Y	-
21	[23]	-	-	-	-
22	[24]	-	Y	Y	-
23	[25]	-	Y	Y	-
24	[26]	Q1	Y	-	-
25	[27]	-	Y	-	-
26	[5]	Q1	-	-	-
27	[4]	Q3	-	-	-
28	[28]	Q1	-	-	-
29	[29]	Q2	-	Y	-
30	[30]	Q3	-	Y	-

Symbol description: "Y" means the obtained article discusses subject based the column, "-" means the opposite. In the discussion section will describe the results of the previous process to answer the Research Question. In the articles obtained, there are 12 articles that are relevant to the topic of discussion and questions on the research question. In this paper there are some research on data security at the transport layer or network layer. Articles that conduct data security research using steganography, cryptography or both by carrying out the process at the transport layer are 8 articles, 1 article processes data security at the network layer and 3 articles conduct observational studies on the mechanism of data security in the communication path.

Table 2 shows that there are developments in securing data in the network layer using cryptographic or steganographic techniques. There are studies that use a combination of cryptography and steganography to provide multiple layers of security [1] [8] [14].

The process of developing data security using steganography, the majority is done only limited to the application layer. In the article obtained there are several studies in the form of study. Among them observing the development of steganography in the physical layer or link layer by proposing packet modifications and timings on delivery by providing time delay [2]. Other observations conducted security observations on ad-hoc networks that suggested adding a mechanism for key exchange and securing data with cryptographic techniques [12]. As a monitoring tool for packet data flow on transmission media a study uses NS3 to monitor the form of packets sent in IPv4 [7].

Commonly the development of steganography carried out on the network is more likely in the transport layer. Generally it is mentioned that data security is done by encryption and steganography techniques, even though it is applied to the socket [10]. An application using the RSA encryption technique to form a cipher and then transform into binary and split into 20 bits per packet [1]. Other studies have modified the Transport Transport Control Protocol (STCP) by performing multi-level security using secret matrix, secret keys, hidden signatures and steganography [8]. Modification of other shipments via the transport layer is done by permutation of the packet using a table agreed upon by the sender and receiver [3]. Reduction in packet size is also done to prevent transmission bottlenecks in the transmission [9]. Another approach is to use headers in TCP / IP as a cover, but this can only hold 4 characters in each communication transmission [11]. Another proposal is to streamline the data which is done serially by using a cross-layer framework [13].

The process of securing data is still dominated by applying cryptographic and steganographic mechanisms. Even though it is applied in packet size modification, embedding in the header, the secret message that is still embedded is still flowing in the communication path. A study suggests an observation of data traffic in order to analyze packet size anomalies [15].

Data security in the communication channel is expected to continue. This is a number of proposals reported in previous studies, namely by combining several cryptographic and steganographic techniques [6] [10], algorithm modification [13], package size modification [1] [9], insert in to the cover header [11], the addition of a digital signature [14] making observations on data traffic is also needed to see streaming data anomalies [15].

4. Conclusion

From the activities, conclusions can be drawn about evolutions of steganographic techniques in the network layer are such as follows. The development of data security uses steganography combined with cryptography to provide data security, authenticity and integrity of the data as well as provide information trust for the recipient. The development of steganography is also done by modifying the package size, modification by giving additional time to send and using headers as cover data for messages. Even so, the steganography mechanism that is carried out in majority still streams the message data through the transmission media, even though the message has been kept it's confidentiality and has a cover. To support the form of data security running through communication media, a concept of developing data security by observing data traffic conditions for decision making in solving packet size before sending via transmission media are ight be an idea for further developing.

References

[1] Bobade S and Goudar R 2015 Secure Data Communication Using Protocol Steganography in IPv6 *IEEE 2015 International Conference on Computing Communication Control and Automaton*.

[2] Seo J O, Manoharan S and Mahanti A 2016 A Discussion and Review of Network Steganography *2016 IEEE International Conference in Dependable, Autonomic and Secure Computing*.

[3] Peng F X, Jing S H and Rong G H 2017 A New Network Steganographic Method Based in The Transverse Multi-Protocol Collaboration *Journal of Information Hiding and Multimedia Signal Processing* **8(2)** p 445-459.

[4] Rahim R, Simarta J, Purba A, Prayogi M A, Sapta A, Sulaiman O K, Sembiring M A, Ramadhani R, Tambunan A R S, Hasdiana H, Simbolon P, Aisyah S, Juliana J and Suharman S 2018 Internet based remote desktop using INDY and socket component *Internasional Journal of Engineering & Technology* **7(29)** p 44-47.

[5] Hassan E A, Shareef H, Islam M M, Wahyudie E and Abdrabou A A 2018 Improved Smart Power Socket for Monitoring and Controlling Electrical Home Appliances *IEEE Access* **6** p 49292-49305.

[6] Hedge R and Sreenivas T H 2015 Steganography in Ad Hoc Network *International Journal of Computer Science and Information Technologies* **6(6)** p 5405-5408.

[7] Kheddar H and Bouzid M 2015 Implementation of Steganographic Method Based in IPv4 Identification Field over NS-3 *International Journal of Engineering Research and Applications* **5(3)** p 44-48.

[8] Venkadesh P, Dhas J P M and Divya S V 2015 Techniques to enhance security in SCTP for multi-homed networks *IEEE : 2015 Global Conference on Communication Technologies (GCCT)*.

[9] Gulia P and Reena 2017 A Novel Technique of Security Improvement in Ad-hoc Network by using FTP *International Journal of Applied Engineering Research* **12(17)** p 6658-6662.

[10] Dalal S and Devi S 2017 Security Framework against Denial of Service Attacks in Wireless Mesh Network *Global Journal of Pure and Applied Mathematics* **13(2)** p 829-837.

[11] Kadhim J M and Abed A E 2017 Steganography Using TCP/IP's Sequence Number *Al-Nahrain Journal of Science* **20(4)** p 102-108.

[12] Reena and Gulia P 2017 Review of Security in AD-HOC Network Using FTP *Advances in Computational Sciences and Technology* **10(5)** p 1417-1426.

[13] Shamieh F and Wang X 2018 Dynamic Cross-Layer Signaling Exchange for Realtime and On Demand Multimedia Streams *IEEE Transactions On Multimedia* **17(10)** p 1-12.

[14] Ruban I, Chuiko N L , Mukhin V, Kornaga Y, Grishko I and Smirnov A 2018 The Method of Hidden Terminal Transmission of Network Attack Signatures *International Journal Computer Network and Information Security* **4** p 1-9.

[15] Troegeler B and Watters P 2018 Steganographic Transports: A Vector for Hidden Secret Internets? *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications*.

[16] Nair K, Asher K and Joshi J 2015 Implementing Semi-Blind Image Steganography with Improved Concealment *IJCA Proceedings on International Conference on Computer Technology*.

[17] Nagendrudu S and Reddy V R 2015 Integration of BPCS Steganography and Visual Cryptography for Secure e-Pay *International Journal on Computer Science Engineering and Technology* **5(6)** p 162-165.

[18] Manujala G R and Danti A 2015 Embedding Multiple Images in A Single Image using Bit Plane Complexity Segmentation (BPCS) Steganography *Asian Journal of Mathematics and Computer Research* **2(3)** p 136-142.

[19] Raman I G and Kaliyamurthie K P 2015 An Adaptive Data Hiding Scheme for Domain Based Secret Data in Random Order to Increase Steganography Using IWT *International Journal Advanced Networking and Applications* **6(5)** p 2464-2467.

[20] Kumar R and Dhiman M 2015 Secured Image Transmission Using a Novel Neural Network Approach and Secret Image Sharing Technique *International Journal of Signal Processing, Image Processing and Pattern Recognition* **8(1)** p 161-192.

[21] Adebayo O S, Olalere M and Ugwu J N 2015 Implementation of N-Cryptographic Multilevel Cryptography Using RSA and Substitution Cryptosystem *MIS Review* **20(2)** p57-76.

[22] Mazurczyk W and Caviglione L 2015 Steganography in Modern Smartphones and Mitigation Techniques *IEEE Communications Surveys & Tutorials* **17(1)** p 334-357.

[23] S Singaravelan A and K Kowsalya M 2016 Design and Implementation of Standby Power Saving Smart Socket with Wireless Sensor Network *2nd Internasional Conference on Intelegent Computing, Communication & Convergance*.

[24] Akolkal S, Kokulwar Y, Neharkar A and Pawar D 2016 Secure Payment System using Steganography and Visual Cryptography *Internasional Journal of Computing and Technology* **3(1)** p 58-61.

[25] Brar S S 2016 Double Layer Image Security System using Encryption and Steganography *International Journal Computer Network and Information Security* **3** p 27-33.

[26] Morovati K , Ghorbani A and Kadam S 2016 A network based document management model to prevent data extrusion *Computers & Security* **59** p 71-91.

[27] Demirol D, Das R and Tuna G 2017 An android application to secure text message *IEEE 2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*.

[28] Wijayarathna C and Arachchilage N A G 2018 Why Johnny Can't Develop a Secure Application? A Usability Analysis of Java Secure Socket Extension API *Computers & Security* **80** p 54-73.

[29] Xin G, Liu Y, Yang Y and Cao Y 2018 An Adaptive Audio Steganography for Covert Wireless Communication *Security and Communication Networks* **2018** p 1-10.

[30] Issa Y A, Ottom M A and Tamrawi A 2019 eHealth Cloud Security Challenges: A Survey *Journal of Healthcare Engineering* **2019** p 1-15.

9_Protecting Data By Socket Programming Steganography

ORIGINALITY REPORT

12%	9%	7%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

7%

★ M R Adrian, D H Kurniawan, A Faza, J Maulina, M R Shihab. "A Brief Look at Software Defined Network (SDN) Implementation: Gaining Benefits and Coping with the Challenges at a Telecommunication Company", IOP Conference Series: Materials Science and Engineering, 2020

Publication

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	Off		