The E-mail Spoofing on the Network Layer Protocols and Countermeasures Besides the Sender Domain Authentication

Shigeo Akashi and Yao Tong

***Abstract*—In this paper, it is shown that application of the OSI reference model to the e-mail spoofing enables us to specify the causal network skills which have been abused and that countermeasures against this cybercrime, which are different from the sender domain authentication, can be developed. Firstly, we see that the phenomena which are brought about by the e-mail spoofing based on the datalink layer protocols are different from the phenomena which are brought about by the e-mail spoofing based on the network layer protocols. Secondly, we develop countermeasures which can discriminate the network segments where the impersonated e-mail users and the impersonators co-exist from the network segments where only the non-impersonated e-mail users exist.**

***Index Terms*—OSI reference model, e-mail spoofing, longest prefix matching rule, disguised packet transmission, sender domain authentication.**

I. Introduction

It is well known that the OSI reference model has been playing so important roles for the purpose of laying the foundation of networks, Therefore, it is quite reasonable that this model can be applied usefully to the development of countermeasures against various kinds of cybercrimes. Since modern cybercrimes are closely related to the network skills ranging from the physical layer protocols to the application layer protocols, it seems to be important for both of the security operation center and the computer security incident response team to classify the cybercrimes in terms of the OSI reference model.

The countermeasures against cybercrimes can be classified into two cases, namely, the global case and the local case, where the global case means the set of countermeasures which are carried out over the wide area networks and the local case means the set of countermeasures which are carried out over the local area networks. As for examples of the countermeasures against the cybercrimes which are classified into the global case, we can refer to the Revised Nirvana and Daedalus which are the system for visualizing network traffic flows over the worldwide network such as the Internet and the system for alerting potential cyberattacks invading from overseas to the nationwide security operation center attached to National Institute of Information and Communications Technology, respectively. As for examples of the countermeasures against the cybercrimes which are classified into the local case, we can refer to cyber security tools such as certificate authorities and antivirus programs. Unfortunately, it is one thing to prevent all Japanese people together from cyberattacks originating from overseas, and it is quite another to prevent each of all Japanese people from being infected with computer viruses by way of the Internet and being extracted private data from his computers, Moreover, the roles being played by the countermeasures belonging to the global case cannot be replaced with the roles being played by the countermeasures belonging to the local case, and the converse replacement does not work well either. Therefore, it is very difficult for the modern countermeasures to protect both of Japanese nation and all Japanese network users simultaneously from modern cybercrimes.

What can be done with the network skills developed by Cisco Systems is to develop new types of countermeasures by applying the OSI reference model to various kinds of cybercrimes, because the OSI reference model has succeeded in formulating almost all network protocols ranging from the local area networks through the wide area networks and in classifying almost all network protocols into the seven layers. As for the domain-based e-mail authentication, we can refer to Crocker, Delany, Hansen, Kucherawy and Zwicky [1]-[3], and as for the mathematical foundation of the computer programming including the network theory, which was laid by computer scientists, we can refer to Knuth [4].

II. Classification of E-mail Spoofing Based on the OSI Reference Model

In this section, we discuss the e-mail spoofing as a cyberattack for which we can specify the maliciously abused network skills in terms of the OSI reference model. As for other types of cyberattacks, we can refer to Ford-Hutchinson [5]. From the point of view of the identification of malicious e-mail senders, this spoofing can be classified into two types, namely, the e-mail spoofing realized by the unidentified senders sending e-mails bound for the authenticated e-mail users, and the e-mail spoofing realized by the impersonators pretending to be some other authenticated e-mail users. As for the former type, we can easily understand the reason why no responses to the e-mails issuing from the unidentified senders can reach anywhere, but as for the latter type, we can anticipate the final destinations for which the responses are bound as the following three cases:

Manuscript received January 5, 2020; revised March 12, 2020. This work was supported in part by Training Center Japan and Cisco Networking Academy.

Shigeo Akashi and Yao Tong are with the Department of Information Sciences, Faculty of Science and Technology, Tokyo University of Science. 2641, Yamazaki, Noda City, Chiba Prefecture, 278-8510, Japan (e-mail: akashi@is.noda.tus.ac.jp, 6316063@ed.tus.ac.jp).

doi: 10.18178/ijiee.2020.10.1.715

Case 1. The responses to the e-mails issuing from the impersonators reach the impersonated authenticated e-mail users whom the impersonators pretend to be.

Case 2. The responses to the e-mails issuing from the impersonators reach the impersonators themselves.

Case 3. The responses to the e-mails issuing from the impersonators cannot reach anywhere.

It is difficult for us to identify the network skills as what have been applied to the impersonation, because all the three cases stated above can be observed everywhere. But, if we apply the idea of the OSI reference model to the e-mail spoofing, we can specify the network skills which have been abused. Firstly, we should pay attention to the fact that the e-mail spoofing can be classified into the e-mail spoofing based on the datalink layer protocols and the e-mail spoofing based on the network layer protocols. Since the MAC-addresses and the IP-addresses play so important roles in transmitting frames and in transmitting packets, respectively, it is reasonable that the way applied to realizing the e-mail spoofing based on the datalink layer protocols differs from the way applied to realizing the e-mail spoofing based on the network protocols. Though it is well known that the sender domain authentication can play very important roles in discriminating the impersonators from the impersonated authenticated e-mail users. this countermeasure need to be installed in almost all SMTP servers individually. This is the reason why the sender domain authentication can be regarded as a server-wise countermeasure.

As for the network theoretic environment on which the e-mail spoofing based on the datalink layer occurs, the cybercriminals commit their malicious crimes on the network where the authenticated e-mail users who are impersonated, the authenticated e-mail users who are not impersonated and the impersonators share only one network segment with each other, and the simplest mutual relations among them on the commonly shared network can be illustrated as the following figure:

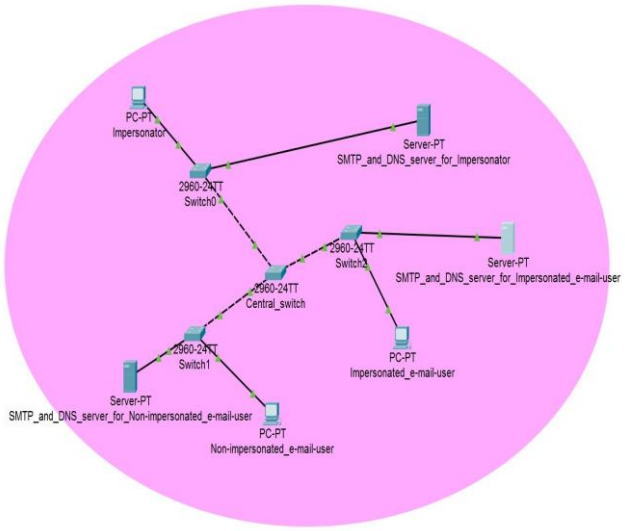

Fig. 1. A network segment where the e-mail spoofing based on the datalink layer protocols occurs.

In Fig. 1, the network segment encircled in purple includes non-impersonated authenticated e-mail users, impersonated authenticated e-mail users and impersonators in the inside.

As for the network theoretic environment on which the e-mail spoofing based on the network layer occurs, the cyber-criminals commit their malicious crimes on three networks, namely the network segment where the authenticated e-mail users who are impersonated exist, the network segment where the authenticated e-mail users who are not impersonated exist and the network segment where the impersonators exist, each of which is strictly separated from the others. The simplest mutual relations among them on these network segments can be illustrated as the following figure:

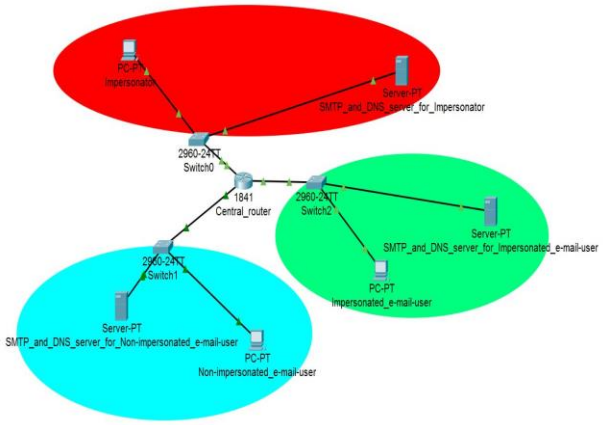

Fig. 2. Network segments where the e-mail spoofing based on the network layer protocols occurs.

In Fig. 2, the network segment encircled in blue, the network segment encircled in green and the network segment encircled in red include non-impersonated authenticated e-mail users, impersonated authenticated e-mail users and impersonators, respectively.

III. The Way of E-mail Spoofing Based on the Network Layer Protocols

Exactly speaking, there exists another famous method of realizing the e-mail spoofing based on the application layer protocols, which is called the falsification of the envelopes recorded in the headers of e-mails. Actually, this method can be intentionally applied to only a certain specified e-mail user's correspondence with another specified e-mail user. Therefore, in this section, we introduce another e-mail spoofing which can involve unspecified and many e-mail users and can be realized by constructing disguised packet transmission brought about by the longest prefix matching rule. As for the e-mail spoofing based on the datalink layer protocols, we can refer to Akashi and Tong [6].

Let Deepak and Impersonated_Authenticated_Jitu be a non-impersonated authenticated e-mail user with his e-mail address deepak @cisco.com and an impersonated authenticated e-mail user with his e-mail address jitu@example.com, respectively. Moreover, let the IP address of the SMTP server assigned for Deepak and the IP address of the SMTP server assigned for Authenticated_Jitu be 192.168.0.2/22 and 172.16.0.2/22, respectively. If we assume that Impersonator_Jitu is an impersonator pretending to be Authenticated_Jitu by using jitu@example.com intentionally and assume that the IP address of the SMTP

server assigned for Impersonator_Jitu is 172.16.0.2/23, then the disguised packet transmission can be brought about. Throughout this section, the network segment of the SMTP server assigned for Deepak, the network segment of the SMTP server assigned for Impersonated_Authenticated_Jitu and the network segment of the SMTP server assigned for Impersonator_Jitu are strictly separated from each other.

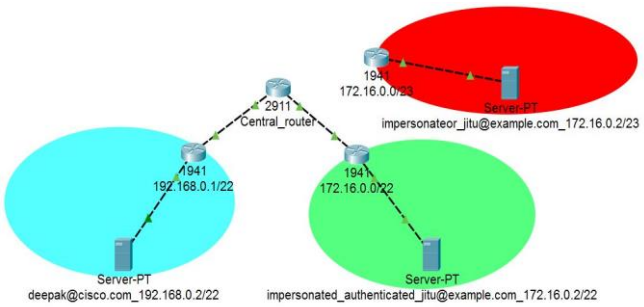

Fig. 3. Network segments where the impersonator has not been connected.

In Fig. 3, an example recording the network environment where Impersonator_Jitu has neither relation to Deepak nor relation to Impersonated_Authenticated_Jitu is illustrated. We can observe that the network segment where Deepak with his e-mail address deepak@cisco.com and the network segment where Jitu with his e-mail address jitu@example.com exists are encircled in blue and in green, respectively. Moreover, the network segment where Impersonator_Jitu with his e-mail address is also jitu@example.com exists is encircled in red. Since the network segment assigned for Impersonator_Jitu has not been connected yet to the Central_router where the network segment assigned for Deepak and the network segment assigned for Impersonated_Authenticated_Jitu have already been connected, the mutual e-mail correspondence between Deepak and Impersonated_Authenticated_Jitu has been available. In other words, both of the e-mail correspondence of Deepak with Impersonated_Authenticated_Jitu and the e-mail correspondence of Impersonated_Authenticated_Jitu with Deepak have been available.

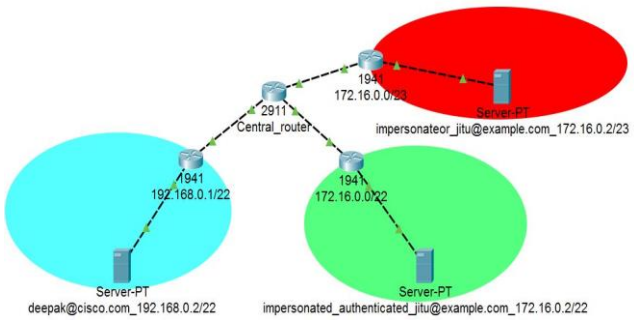

Fig. 4. Network segments where the impersonator has been connected.

In Fig. 4, an example recording the network environment where Imperonator_Jitu exists is illustrated. Neither the e-mail correspondence of Deepak with Impersonated_Authenticated_Jitu nor the e-mail correspondence of Impersonated_Authenticated_Jitu with Deepak is available, because the network segment assigned for Impersonator_Jitu has been connected to the Central_router where the network segment assigned for Deepak and the network segment assigned for Impersonated_Authenticated_Jitu have already been connected. However, both of the e-mail correspondence of Deepak with Impersonator_Jitu and the e-mail correspondence of Impersonator_Jitu with Deepak are available. These phenomena show that the mutual e-mail correspondence between Deepak and Impersonator_Jitu takes strict priority over the mutual e-mail correspondence between Deepak and Impersonated_Authenticated_Jitu.

The reason why these phenomena occur can be clarified in terms of the longest prefix matching rule and TCP three-way handshake, which has been used in the first automated course of establishing TCP session between two SMTP servers. Exactly speaking, though the longest prefix matching rule plays an important role in transmitting packets as possible as exactly and TCP three-way handshake also plays an important role in transmitting packets as possible as in the most reliable way, both the longest prefix matching rule and the TCP three-way handshake have established wrongly the e-mail correspondence between Deepak and Impersonator_Jitu in case that we use these two network skills simultaneously. This fact means that the longest prefix matching rule and TCP three-way handshake are not compatible together with each other under this environment.

There is an example recording the sequential transmission of packets commuting between Deepak and Impersonated_Authenticated_Jitu as the following:

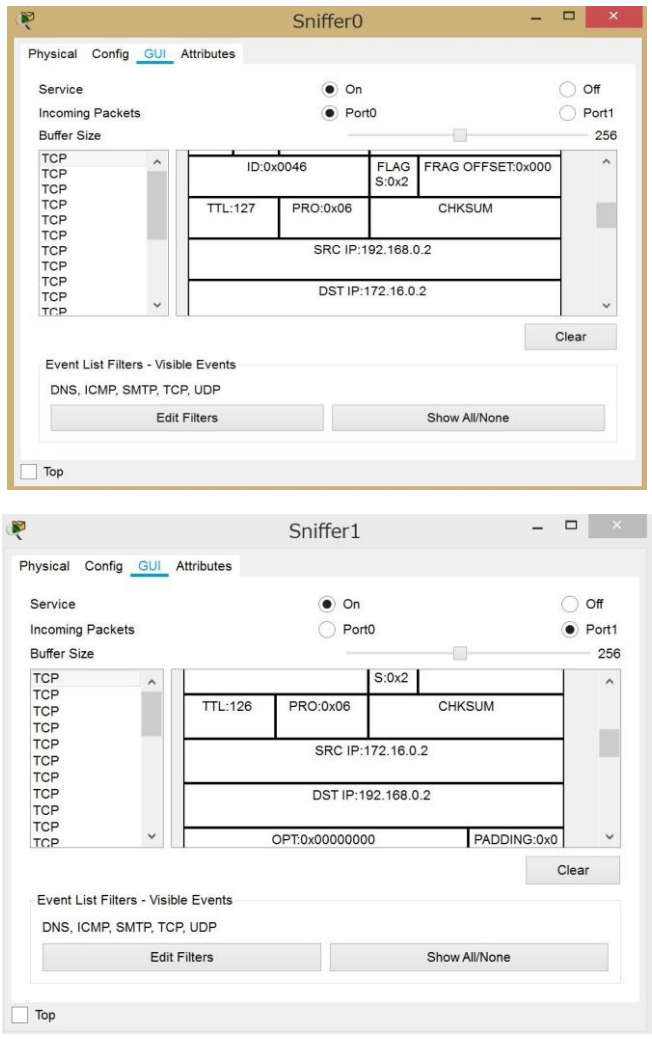

Fig. 5. Failure in TCP three-way handshake accompanying e-mail correspondence of Authenticated_Jitu with Deepak.

Fig. 5 shows that Impersonated_Authenticated_Jitu has failed in TCP three-way handshake accompanying his e-mail correspondence with Deepak. Exactly speaking, the upper half of this figure records the sequence of packets originating in Deepak and the lower half records the sequence of packets originating in Impersonated_Authenticated_Jitu. Since TCP session between Impersonated_Authenticated_Jitu and Deepak has not been established, none of the e-mail packets issuing from Impersonated_Authenticated_Jitu can reach Deepak.

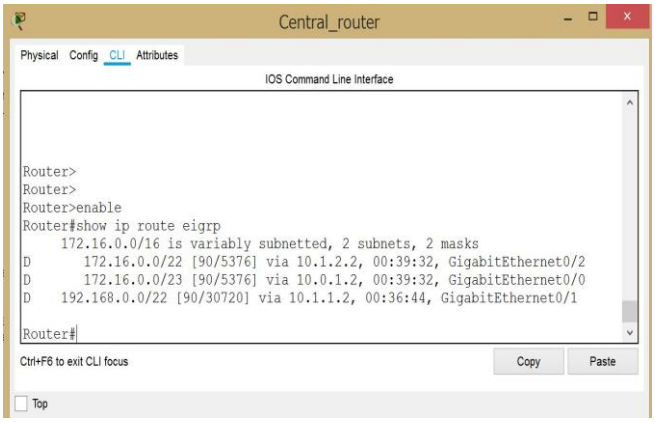

Fig. 6. Routing table of Central router in Fig. 4.

Fig. 6 gives the reason why TCP session between Impersonated_Authenticated_Jitu and Deepak cannot be established. Though the network address containing the IP address of the SMTP server assigned for Impersonator_Jitu, which is equal to 172.16.0.0/23, is properly included in the network address containing the IP address of the SMTP server assigned for Impersonated_Authenticated_Jitu, which is equal to 172.16.0.0/22, the interface advertising 172.16.0.0/23 is different from the interface advertising 172.16.0.0/22. Therefore, it is reasonable that the longest prefix matching rule has an influence on the transmission of the packets which are bound for the SMTP server whose address is 172.16.0.2. Under the condition that the sender is Impersonted_Authenticated_Jitu and the recipient is Deepak, TCP three-way handshake should be composed of the following sequentially lined three packets:

1. SYN-packet from Impersonated_Authenticated_Jitu to Deepak.
2. 2. SYN-ACK-packet from Deepak to Impersonated_ Authnticated_ Jitu.
3. ACK-packet from Impersonated_Authenticated_Jitu to Deepak.

Though SYN-packets from Impersonated_Authenticated_ Jitu to Deepak can reach the network segment where Deepak exists, SYN-ACK-packets from Deepak to Impersonated_ Authenticated_Jitu cannot reach the network segment where Impersonated_Authenticated_Jitu exists but can reach the network segment where Impersonator_Jitu exists, and this fact implies that Impersonated_Authenticated_Jitu cannot send his ACK-packet back to Deepak. Eventually, Impersonated_Authenticated_Jitu cannot send his e-mail to Deepak. This is the reason why the longest prefix matching rule is not compatible with TCP three-way handshake which should be required in the course of establishing TCP session.

On the contrary to the previous case, there is another example recording the sequential transmission of packets commuting between Deepak and Impersonator_Jitu as the following:

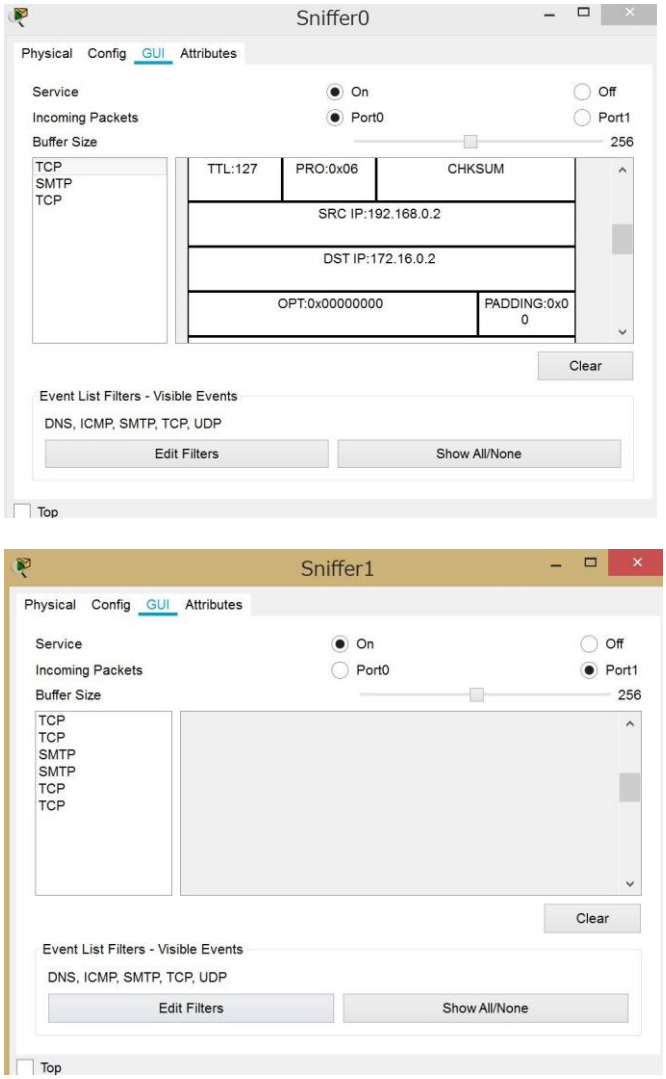

Fig. 7. Success in TCP three-way handshake accompanying e-mail correspondence of Impersonator_Jitu with Deepak.

Fig. 7 shows that Impersonator_Jitu has succeeded in TCP three-way handshake accompanying his e-mail correspondence with Deepak. Exactly speaking, the upper half of this figure records the sequence of packets originating in Deepak and the lower half records the sequence of packets originating in Impersonatot_Jitu. After TCP session between Impersonator_Jitu and Deepak has been established, any e-mail packets issuing from Impersonator_Jitu can reach Deepak. But unfortunately, any responses to the e-mail packets issuing from Deepak have come to reach not Impersonated_Authenticated_Jitu but Impersonator_Jitu.

Here we can use Fig. 6 for explaining the reason why TCP session between Impersonator_Jitu and Deepak can be established. Since the network address containing the IP address of the SMTP server assigned for Impersonator_Jitu, which is equal to 172.16.0.0/23, is properly included in the network address containing the SMTP server assigned for Impersonated_Authenticated_Jitu, which is equal to 172.16.0.0/22, and the interface advertising 172.16.0.0/23 is different from the interface advertising 172.16.0.0/22, the longest prefix matching rule forwards any packet which is

bound for 172.16.0.2 through the interface advertising the network address 172.16.0.0/23. Under the condition that the sender is Impersonator_Jitu and the recipient is Deepak, TCP three-way handshake should be composed of the following sequentially lined three packets:

1. SYN-packet from Impersonator_Jitu to Deepak.
2. 2. SYN-ACK-packet from Deepak to Impersonator_Jitu.
3. 3. ACK packet from Impersonator_Jitu to Deepak.

Since SYN-packets from Impersonator_Jitu to Deepak can reach the network segment where Deepak exists, SYN-ACK-packets from Deepak to Impersonator_Jitu can also reach the network segment where Impersonator_Jitu exists, and this fact implies that Impersonator_Jitu can issue ACK-packet from him to Deepak. Eventually, Impersonator_Jitu can send his e-mail to Deepak. Unfortunately, it is possible that Deepak has already misunderstood Impersonator_Jitu for Impersonated_Authenticated_Jitu, while Deepakcorresponds with Impersonator_Jitu.

IV. Comparison of the E-mail Spoofing Based on the Network Layer Protocols with the E-mail Spoofing Based on the Datalink Layer Protocols

The difference between the e-mail spoofing based on the datalink layer protocols and the e-mail spoofing based on the network layer protocols results from whether the way of e-mail correspondence is based on IP-addresses or based on MAC-addresses. Since what is correspondent to the longest prefix matching rule in the network layer protocols does not exist in the datalink layer protocols, what we should call the disguised frame transmission cannot be constructed in the datalink layers. These consideration enables us to summarize the difference between these spoofing as the following Table I:

TABLE I: Classification of the E-mail Spoofing

Transmission of e-mails	E-mail spoofing based on the datalink protocols	E-mail spoofing based on the network protocols
Causal network skills	forged private DNS and private SMTP servers, which can be easily constructed	falsification of the envelopes attached to e-mails, the longest prefix matching rule
From I to IA	impossible	impossible
From I to NIA	possible	possible
From IA to I	impossible	impossible
From IA to NIA	possible	impossible
From NIA to I	impossible	possible
From NIA to IA	possible	impossible

where I, IA and NIA mean the impersonator, the impersonated authenticated e-mail user and the non-impersonated authenticated e-mail user, respectively. As for the elementary guidance of cybersecurity, we can refer to Kaspersky Home Security Resource Center [7], and as for the standard textbook of cybersecurity, we can refer to Santos and Muniz [8] and [9].

V. A Conditional Countermeasure Against E-mail Spoofing Based on the Network Layer Protocols

It is much better for the e-mail users to use ICMP commands such as ping and traceroute immediately before they send their e-mails to the SMTP servers assigned for their recipients. Nevertheless, there are many network segments on which the network administrators force ICMP commands not to be available intentionally. Now, if we assume that a SMTP server assigned for an e-mail recipient is used not only as the SMTP server but also as a HTTP server for the purpose of making its web contents known to the public, then a sender can solve the problem asking whether his SMTP server is impersonated or not by visiting the website on the recipient's multipurpose server used both as SMTP server and HTTP server, because HTTP and SMTP can be regarded as protocols belonging to TCP and therefore, they should follow the procedures for establishing TCP sessions, which are common among the transport layer protocols. Finally, the e-mail sender can confide that he is not impersonated by any impersonator pretending to be himself, if he can browse the web contents presented by the recipient's multipurpose server. Actually, this countermeasure is double-edged, which is illustrated as the following figure:

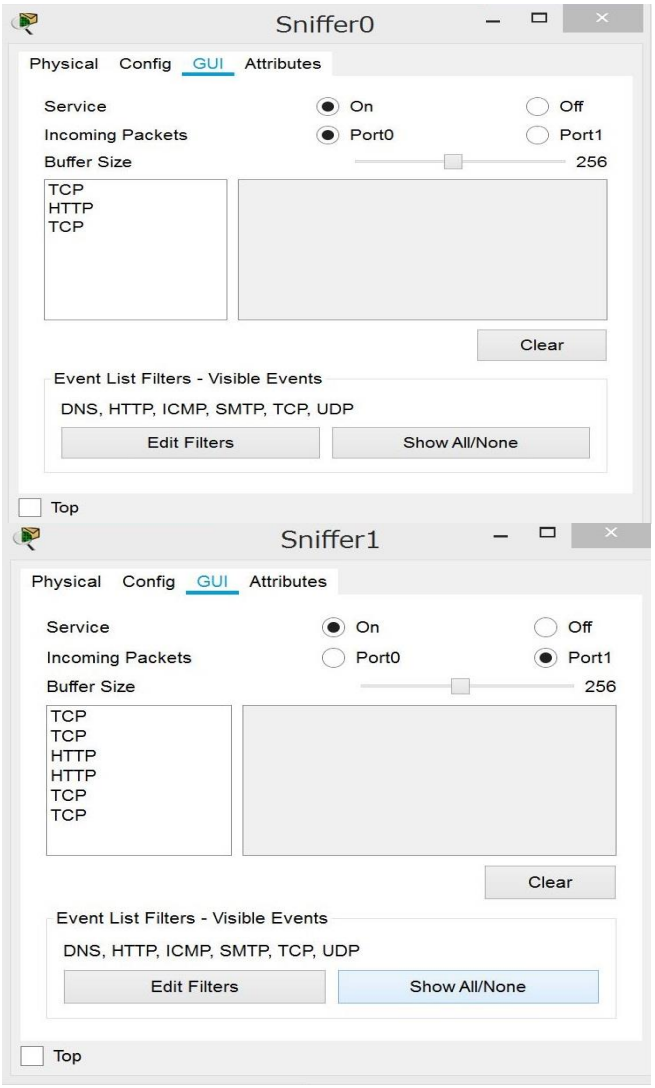

Fig. 8. Success in TCP three-way handshake accompanying the web-browsing procedure by Impersonator_Jitu.

Fig. 8 shows that Impersonator_Jitu has succeeded in TCP three-way handshake accompanying the procedure which Impersonator_Jitu needs to follow when he wants to browse

the web contents presented by the multipurpose server assigned for Deepak. In other words, Impersonator_ Jitu's success in browsing the web contents presented by Deepak means his success in impersonating Authenticated_ Jitu. More exactly speaking, the upper half of this figure records the sequence of packets originating in Deepak and the lower half records the sequence of packets originating in Impersonator_Jitu, and these figures show that, after the TCP session between Impersonator_Jitu and Deepak has been established, any HTTP packets issuing from Impersonator_ Jitu can reach Deepak, and conversely, any HTTP packets issuing from Deepak can reach Impersonator_Jitu.

VI. Conclusion

There are two famous technical problems which are brought about by the legitimate packet transmission protocols, namely, the problem brought about by the longest prefix matching rule and the equal cost multipath problem. When we discuss the difficulties caused by troublesome relations between two network segments with their network addresses 172.16.0.0/22 and 172.16.0.0/23, each of which are separated from the other, the former problem has played important roles in specifying the causal network skills. Actually, when we discuss other difficulties caused by troublesome relations between two network segments sharing 172.16.0.0/22 and being separated geographically from each other, the equal cost multipath problem will play the same important roles as the problem brought about by the longest prefix matching rule has played, because we can expect to encounter new phenomena which still remain to be investigated. As for the equal cost multipath problem, we can refer to Hopps [10].

Conflict of Interest

The authors declare no conflict of interest.

Author Contribution

The first author conducted the research and wrote the paper; The second author compose the programs for simulation and revised and correct the manuscript of this paper elaborately; all authors had approved the final version.

Acknowledgment

The authors would like to express their hearty gratitude to the referee who has given his suggestive and elaborate advice which enables our joint research paper revised in every respect.

References

[1] D. Crocker, T. Hansen, and M. Kucherawy. (2011). Domain keys identified mail (DKIM) signatures. RFC6376, [Online]. Available: https://tools.ietf.org/html/rfc6376
[2] M. Delany. (2007). Domain-based email authentication using public keys advertised in the DNS (DomainKeys. RFC4870). [Online]. Available: https://tools.ietf.org/html/rfc4870
[3] M. Kucherawy and E. Zwicky. (2015). Domain-based message authentication, reporting, and conformance. RFC7489, [Online]. Available: https://tools.ietf.org/html/rfc7489
[4] D. E. Knuth, *The Art of Computer Programming*, Addison-Wesley Publishing Company, Massachusetts, 2nd ed., 1973.
[5] P. Ford-Hutchinson. (2005). Securing FTP with TLS. RFC4217, [Online]. Available: https://tools.ietf.org/html/rfc4217
[6] S. Akashi and Y. Tong,"Classification of DHCP spoofing and effectiveness of DHCP snooping," in *Proc. 2018 International Conference on Advances in Computer Technology, Information Science and Communication*, Wen-Bing Horng and Yong Yue, Ed. pp. 233-238, ISBN:978-989-758-357-5, 2019.
[7] Kaspersky home security resource center. What is spoofing. [Online]. Available:https://www.kaspersky.com/resource-center/definitions/ip-and-email-spoofing
[8] O. Santos and J. Muniz, *CCNA Cyber Ops Secfnd 210-250*, Cisco Press, Indianapolis, 1st edition, 2017.
[9] O. Santos and J. Muniz, *CCNA Cyber Ops Secops 210-255*, Cisco Press, Indianapolis, 1st edition, 2017.
[10] C. Hopps. (2000). Analysis of an equal-cost multi-path algorithm. RFC 2992. [Online]. Available: https://tools.ietf.org/html/rfc2992

Shigeo Akashi is affiliated with the Department of Information Sciences of the Faculty of Science and Technology at Tokyo University of Science. He has been approved as distinguished Cisco certified active instructor, which is authorized by Cisco Networking Academy since 2013. His major research areas are applied mathematics and cybersecurity.

Yao Tong is affiliated with the Department of Information Sciences of the Faculty of Science and Technology at Tokyo University of Science. Her major research area is cybersecurity.