Security Awareness: A Lesson from Tcpdump and Ethereal

Mohd Fo'ad Rohani [1] Mohd Aizaini Maarof [2], Ali Selamat [3]
Faculty of Computer Science and Information Systems,
University Teknologi Malaysia,
81300 Skudai, Johor.
Email: foad@fsksm.utm.my [1], maarofma@fsksm.utm.my [2], aselamat@fsksm.utm.my [3]

ASTRACT

Ethernet has survived for several decades as essential media for LAN technology because of its relative inexpensive and reasonably fast. Shared Ethernet uses broadcast technology where CSMA/CD acts as medium access control. CSMA/CD deploys principle of media sharing and the drawback is promiscuous mode, whereby network interface device could intercept all packet frames that traveling on the wire. This has a significant impact on the security of Internet application. HTTP, FTP, E-MAIL and TELNET are daily applications, which offer secure transaction or unsecured transaction. However, users do not aware of the security provided by the services. They usually use unsecured transaction because of simplicity or unaware of security awareness. This behavior is vulnerable to packet-sniffing tools, such as sniffit, tcpdump and ethereal. These tools could intercept the traveling packet and extract sensitive information, such as user login and password or unencrypted data payload. This paper explores network security awareness from the perspective of packet-sniffing tools over unsecured application. The study uses tcpdump and ethereal, which are two of the most popular packet-sniffing tools. From the experiment, it is shown that vital information, such as login and password, could be compromised easily from the packet if users do not consider security awareness seriously.

KEYWORDS

security awareness, tcpdump, ethereal, internet secured transaction.

1. Introduction

Ethernet has survived for several decades as essential media for LAN technology because of its relative inexpensive and reasonably fast. Shared Ethernet uses broadcast technique where CSMA/CD acts as medium access control. CSMA/CD deploys principle of media sharing and the drawback of this principle is promiscuous mode [8]. In promiscuous mode, network interface device is allowed to intercept and read each network packet that arrives in its entirety. Promiscuous mode gives a great impact on the security of Internet application. It permits passive attack, such as a sniffing program, and collecting information related to the selected victim. A passive attacks is a nature of eavesdropping network packet with intention to password cracking, exploiting security flaws or exploiting bugs in operating systems and network [2].

Internet application, such as HTTP, FTP or E-mail, offers service protocols both in secured mode or unsecured mode. However, most of normal user unaware of these services and simply select unsecured service for daily Internet usage [3]. This paper discusses on how sensitive information in the intercepted network packet frame, such as login and password, could be easily revealed to intruder, if user does not consider security awareness seriously. Section 2 explains Internet application protocols, security awareness and packet-sniffing method. Section 3 discusses the example of sniffing activities and finally section 4 gives conclusion.

2. Internet application Protocols

Many Internet users are familiar with the higher layer application protocols that use TCP/IP to get to the Internet. These include the World Wide Web's Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), Telnet (Telnet)

which lets user logon to remote computers, and the Simple Mail Transfer Protocol (SMTP).
Most Internet services are examples of client–server applications. The client communicates with the server through a session. To make a server request, the client sends a message to the server over the session, and specific virtual port number will be assigned. Figure 1 shows example of the default session port that has been set for a server.

Port	State	Service
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
80/tcp	open	http
110/tcp	open	pop-3
111/tcp	open	sunrpc
443/tcp	open	https
631/tcp	open	ipp
783/tcp	open	hp-alarm-mgr
995/tcp	open	pop3s
1024/tcp	open	kdm
1025/tcp	open	NFS-or-IIS
6000/tcp	open	X11

Figure 1 Default service port number

Internet application protocols such as HTTP (port 80), FTP (port 21), TELNET (port 23) and E-MAIL (port 110) are examples of plain and unsecured protocols. It is not hard for intruder to intercept and get the account and password information as the packet is passed along the Ethernet. Several others privacy information like financial account numbers, private e-mail data and low-level protocol information (e.g., IP addresses and TCP sequence numbers) could also be revealed.

As an alternative, Netscape introduce Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) as secured web protocol. It is built into browsers that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses Secure Socket Layer (SSL) as a sub-layer under its regular HTTP application layer [9]. As a comparison, by default HTTPS uses port 443 and HTTP uses port 80 in its interactions with the lower layer in TCP/IP model.

If user retrieves e-mail from his UNIX server using Post Office Protocols (POP3), he actually exchanges all information and password in a clear text. This means that anyone with access to the network path between his server and its clients can discover his password [10]. And since most Unix systems use the same password for email access and shell access, user could lose a lot more than exclusive access to user email. For this reason, it is recommended that user use POP3S which operate open SSL to secure POP3 transfers to protect them from eavesdropping.

The SSL protocol ensures user confidentiality, provides client and server authentication mechanisms and protects against the possibility of data being modified in-transit by a third-party [11]. This security verifies that if the transaction data is intercepted, it cannot be read by anyone other than the member. The identity of each member is automatically authenticated so that unauthorized third parties cannot assume the member's identity and process transactions [12].

2.1 Security awareness.

Awareness is the opening key to security since security cannot takes place if we ourselves are ignorant of the subject matter. We must not only aware that security is important but must also aware about things that we can do to enhance security. The state of awareness is where we realize that there are risks and there are safeguards available. The information systems and networks are interconnected thus making them vulnerable to both external and internal attacks [7].

It is important to challenge the view that users are never motivated to behave in a secure manner. Insecure work practices and low security motivation have been identified by research on information security as major problems that must be addressed [3]. Thus it is important for us to perceive and realize the effect of security failures and the possibility of harm caused to others [7].

Intruder always makes effort to find potential vulnerable that exist in network. By listening to the network, any important data especially root login and password, could be revealed to the intruder. This vulnerable may invite threat, such as malicious program, used to attack the defeated system and make a back door to launch more attack to the network system entirely.

2. 2 Packet Sniffing

Ethernet is a very popular way of connecting LAN computers through shared communication channels [13]. It is because sharing media can reduce significant cost of installation and

produce higher bandwidth for packet transmission. Ethernet protocol works by sending packet information header, which contains the proper destination machine address. Only the network interface with the matching address is supposed to accept the frame. However, in promiscuous mode, a network interface is set to receive and accept all frames, no matter what the frame header says. This will enable the packet-sniffing activity to be done.

Packet sniffers are used by network administrators for many reasons such as: converting binary data in packets to human readable format, troubleshooting problems on a network, network intrusion detection, logging network traffic for forensics and evidence, and discovery of a faulty network card [6]. It can also be used as an extraordinary tool for network analysis or as a hacking tool, which poses a threat. There are many free packet-sniffing tools available for download. Ethereal and tcpdump are two of the most popular tools among network administrators [1].

Ethereal is available for both Windows and Unix, and is particularly user-friendly. It has a graphical user interface to assist in navigating the capture and analysis of packets. Ethereal not only makes network troubleshooting work far easier, but it also aids greatly in network forensics, the art of finding and examining an attack, by giving the analyst a better view [1]. Tcpdump is a UNIX tool (WinDump for windows) used to gather data from a network, decipher the bits and pieces, and display them in a semi-coherent fashion. It is the basis that most packet-sniffing software is comprised of and it can only display packet information header. In this study, ethereal is used as a tool to highlight the importance of security awareness to Internet application because of its powerful features.

3. Experiments and Case Study

The experiments are divided into two categories. The first experiment explores how ethereal can be used to reveal the sensitive user's information over unsecured Internet application protocols. The second experiment is to simulate one of the LAN segment at FSKSM in order to show how the users are practicing security awareness in daily Internet application.

3.1 Ethereal uncovers the real truth

Figure 1 shows user A, B, C and D are in the same LAN segment. Their activity of Internet application is shown in Table 1. While user A, B and C busy with their work, an intruder D is listening on the wire. In this example, the intruder is intended to know the login account and password of user A and also his activities.

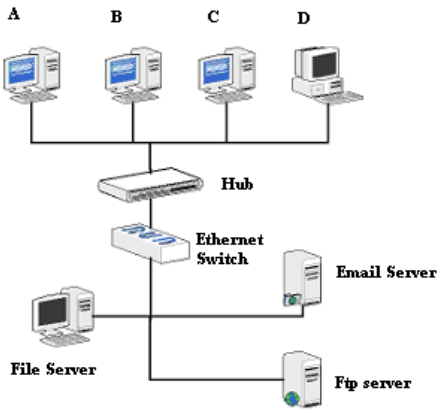

Figure 2 Ethernet communications through Hub.

Table 1 Transaction with unsecured service port and secured service port.

User	Activity	Service (Port)	
A	Check email to Email Server	HTTP (80)	HTTPS (443)
B	File transfer to Ftp Server	FTP (21)	SFTP/SSH (22)
C	Attach to File Server	TELNET (23)	SSH (22)
D	Packet Sniffing	Network interface device in promiscuous mode	

Because of his knowledge of security awareness, user A uses his Web Email (SquirrelMail) by using HTTP (port 80), which is unsecured. Without his conscious, by the time he entered the userid and password to the server, he is in great danger. Figure 3 shows how ethereal can easily exposed the vital login account and password. Figure 4 shows data payload is revealed to the intruder. It is clearly shown HTTP protocol is unsecured and vulnerable to intruder to uncover the sensitive user's information during packet traveling on the wire.

If user A always concerns with security awareness, he should use HTTPS protocol instead of HTTP. Figure 5 explains everything. His entire data payload that travels along the

wire is encrypted with SSL and secured. The intruder will have to make a great effort do the decryption process if he insists to uncover the information, which is very difficult.

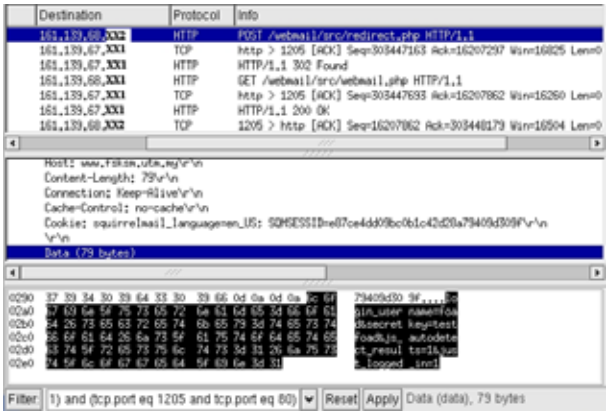

Figure 3 Login account and password of user A is exposed to the intruder (unsecured Web Email).

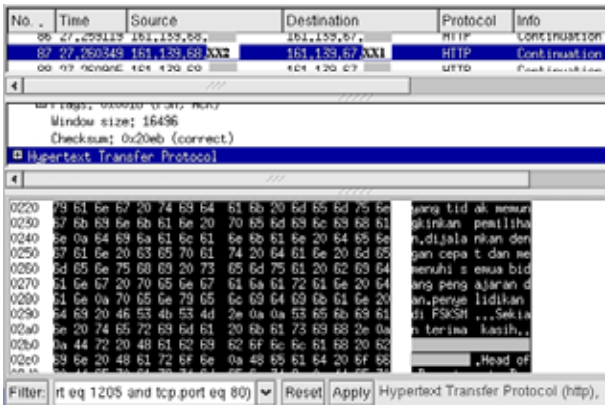

Figure 4 Data Payload is revealed to the intruder (unsecured Web Email)

Users are not advised to use Internet application with unsecured protocols (e.g., FTP and telnet), especially dealing with privacy data. The good thinking is always tried to secure sensitive data with Internet security protocols that have been provided such as SSL or SSH.

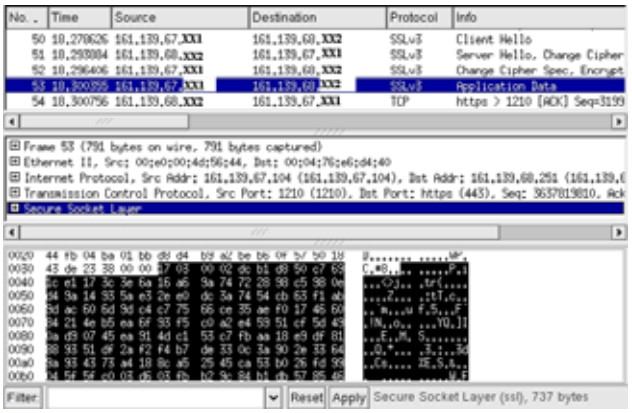

Figure 5 Encrypted Data Payload with Secure Socket Layer (SSLv3).

3.2 Simulation of Security awareness at Computing Labs

A simulation of ethereal program is running for duration of about two and half hours at one of a LAN segment at Computing Labs in FSKSM. The experiment considers all TCP packets that flow on the wire for that duration. The intention is to investigate the security awareness of the Internet application between protocols HTTP vs. HTTPS and POP3 vs. POP3S. Table 2 shows the result of intercepted TCP packets for the simulation.

Table 2 Number of TCP Packet Captured.

Protocol (port)	Number of Connection	Percentage Ratio
HTTP (80)	33258	0.99
HTTPS (443)	455	0.01
POP3 (110)	1209	0.94
POP3S (995)	82	0.06

Timestamp Captured:
Start 2005-05-03 12:25:48.997+08
Stop 2005-05-03 14:49:13.685+08

As shown in Table 2 and Figure 6a, 99% of the packet connections use HTTP protocol and only 1% connections use HTTPS. The vulnerable is when someone transfers sensitive information such as credit card details, personal data, password, secret file or any other private materials with unsecured HTTP protocol. This sensitive information is very privacy and need to be protected. It is afraid if hacker or intruder uncover this essential information, manipulate them and make havoc to the owner or network.

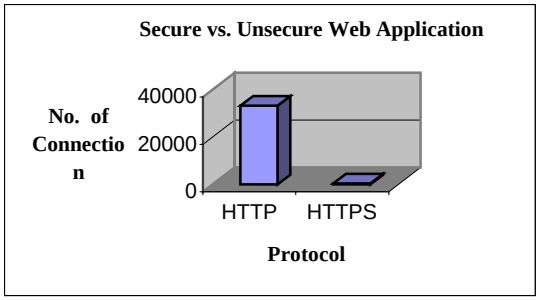

Figure 6a The usage of protocols HTTP vs. HTTPS

Similarly, the result shows POP3 protocols are also preferred than POP3S. From Table 2 and Figure 6b,it is shown that 94% of e-mail user connections are unsecured compared to only 6% secured. The user who uses POP3 protocol will suffer information leakage greater than user who uses POP3S.

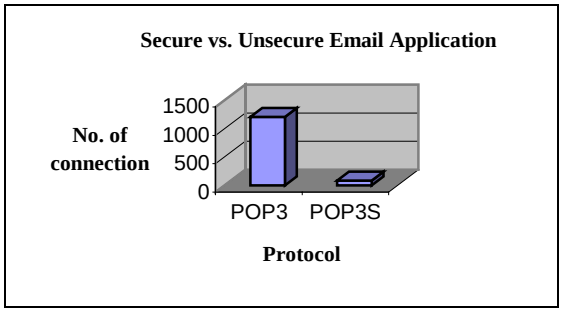

Figure 6b The usage of protocols POP3 vs. POP3S

4. Conclusion

The structure of LAN Ethernet shared media is easily exposed to packet-sniffing activities. Unsecured Internet transaction will be vulnerable for hacking activities. Hence, it is important to increase Internet security awareness among the users. The stringent security policy in a big organization is a good approach to hinder sensitive and privacy data to be revealed to the intruder. It is really important to understand the behavior of network packet that traveling on the wire to study how to strengthen existing network security architecture and conducting network forensics research for future direction.

5. Acknowledgements

This research is supported by UTM and partially by MOSTE.

References:

[1] F. Fuentes, D. C. Kar . Ethereal vs. Tcpdump: a comparative study on packet sniffing tools for educational purpose. Journal of Computing Sciences in Colleges Volume 20, Issue 4 (April 2005) Pages: 169 – 176.

[2] M.D.Vivo, G.O.D. Vivo, G. Isern Internet security attacks at the basic levels ACM SIGOPS Operating Systems Review, Volume 32 Issue 2. (April 1998) Pages: 4 - 15

[3] A. Adams, M. A. Sasse Users are not the enemy, Communications of the ACM, Volume 42 Issue 12 December 1999

[4] C. McCoy, R. T. Fowler "You are the key to security": establishing a successful security awareness program. Proceedings of the 32nd annual ACM SIGUCCS conference on User services. October 2004 Pages: 346 - 349

[5] P. T. Eugster Kernel korner: Linux socket filter: sniffing bytes over the network. Linux Journal, Volume 2001 Issue 86. June 2001

[6] Window Security Official Site, Interpreting network traffic: a network intrusion detector's look at suspicious events, http://secinf.net/info/ids/intv2-8.htm, 2004.

[7] N. M. Nawi, H. Jazri Inculcating The 'Culture of ICT Security', National ICT Security and Emergency Response Centre (NISER) http://www.niser.org.my/resources.html Mei 4, 2005

[8] C. Brenton Topology Security Microsoft TechNet, http://www.microsoft.com/technet/security/topics/networksecurity/topology.mspx (2005)

[9] Webopedia: Online encyclopedia dedicated to computer tecnology http://www.webopedia.com/TERM/S/SSL.html (2004)

[10] C. Rose Securing POP3 Over SSL http://sharkysoft.com/tutorials/linuxtips/pop3s/ (2000)

[11] Data and System Security IntegriCharge Transaction Infrastructure for the Internet Economy https://admin.assurebuy.com/security.htm (2001)

[12] Security World Wide Online Creator's Registry http://www.worldwideocr.com/Sec.asp (2005)

[13] Ethernet Tutorial - Network Basics Solution by Intellicom http://www.intellicom.se/ethernet_tutorial_1.shtml