

# Measurement of the Usage of Several Secure Internet Protocols from Internet Traces

Yunfeng Fei, John Jones, Kyriakos Lakkas, Yuhong Zheng

*Abstract:*

*In recent years many common applications have been modified to take advantage of modern cryptography algorithms to enhance security in Internet communications. This paper presents an overview of several widely used secure Internet services, such as remote login, file transfer and domain name resolution applications. Trace data is used to derive measurements of prevalence for each of these protocols. The results obtained suggest that most of these secure services are not currently widely used.*

## **1. Introduction:**

In recent years many common applications have been modified to take advantage of modern cryptography algorithms to enhance security in Internet communications. A good example of such applications is secure web access via the secure socket layer. While electronic commerce growth has driven the expansion of secure web traffic for online purchasing, it is uncertain whether the secure versions of several other common Internet applications are being widely used. To address this issue, we have used trace data provided by the National Laboratory for Applied Network Research (NLANR) [1] and the Cooperative Association for Internet Data Analysis (CAIDA) [2] Coral Reef trace analysis tools [3] to measure the prevalence of several secure applications like SSH, SCP, DNSSEC, and IPsec.

This paper is structured as follows. Section 2 briefly presents the secure applications addressed, while comparing them with their insecure versions. The methodology used to extract the desired data from the trace files is provided in section 3. Section 4 presents the results and section 5 discusses the findings.

## **2. Secure Internet Services and Applications:**

While there are many Internet services available, only a few are widely used today. We have chosen to focus on three such services, namely remote login, file transfer and domain name resolution. We also examine the use of IPsec, because it provides a general framework for providing secure communication. The following paragraphs present each of these services.

### **2.1 Remote Login (SSH vs. Telnet):**

Remote login programs are familiar to nearly every computer user, especially those who have used time sharing systems, Unix, or even Bulletin Board Systems (BBS). Remote login allows users to

make use of a machine over the network as if they were actually sitting in front of it. Telnet is a commonly used remote login protocol that sends unencrypted keystroke messages to the remote machine (including login information). The secure remote login protocol is called Secure Shell (SSH). SSH corrects Telnet's security problems by encrypting the entire traffic stream. It uses the Secure Socket Layer (SSL) to establish a secure TCP connection between the server and the client.

## **2.2 File Transfer (SCP vs. FTP):**

File transfer is probably the most common use of the Internet today. Although most of this type of traffic is handled by Hyper Text Transfer Protocol (HTTP), many files are not publicly available and thus require authentication. The File Transfer Protocol (FTP) has been the most widely used protocol for providing such user based file transfers. FTP, like Telnet, sends both the login information and the file data unencrypted over the network. This poses a security threat, since any node in the network path can intercept this data. The SSH protocol provides a file transfer mechanism called Secure Copy (SCP) that uses the same encrypted channel as SSH to send files securely over the network. SCP has replaced the Remote Copy (RCP) program originally distributed with Berkley Unix.

## **2.3 Domain Name Resolution (Secure DNS):**

The Domain Name System (DNS) is a critical component of the Internet. It provides a mechanism for resolving host names into IP addresses and vice versa. Since every host on the Internet depends on this information to communicate with other hosts, DNS was designed to be a public database, without security in mind. Unfortunately, this design decision leaves DNS vulnerable to the spread of inaccurate and incorrect information. In response to these security issues DNSSEC extensions have been introduced and deployed [4]. These security enhancements use cryptographic digital signatures to provide authentication and data integrity for name lookup, dynamic update and public key distribution.

## **2.4 IP level security (IPsec):**

Internet Protocol (IP) is the fundamental cornerstone of the Internet. It was designed to provide a basic datagram delivery service across multiple networks. The design philosophy placed the responsibility for providing enhanced services, such as reliability and security, to higher-level protocols layered upon IP. Many current applications require that the data transmitted over the Internet to be both encrypted and authenticated. IPsec is a framework designed to provide security services to the IP layer, instead of specifying any encryption algorithms or authentication / key exchange protocols. This is achieved by the use of two "traffic security" protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP) [5].

## **3. Trace Analysis Methodology:**

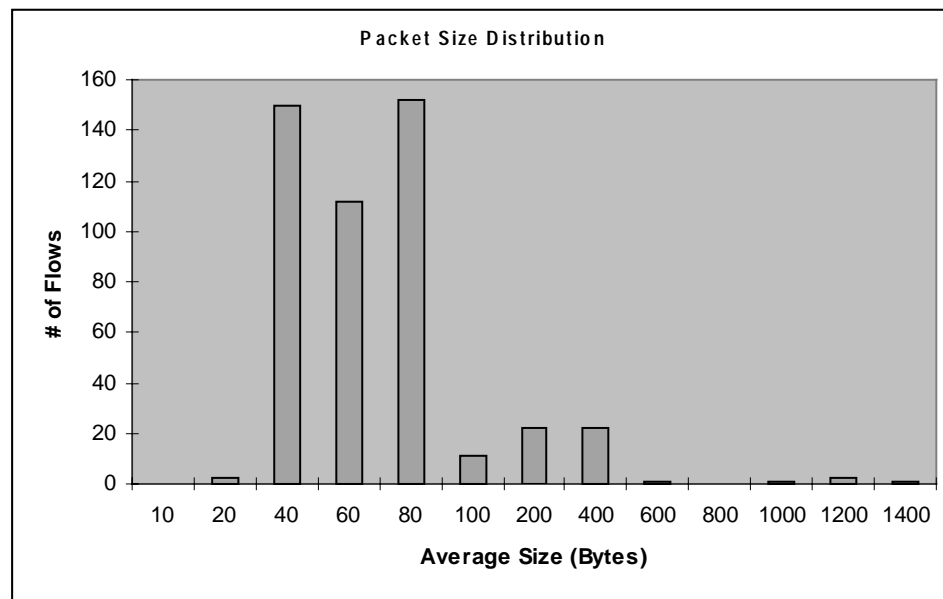
In order to determine the usage of the protocols described above, we used data derived from traces of actual Internet traffic. Trace files were provided by NLANR. The trace file analysis was a two step process. First we used tools provided by Cooperative Association for Internet Data Analysis

(CAIDA) to read the trace files. We then implemented a filter to extract data pertinent to our analysis from the trace files. The following paragraphs describe the specific methods we used for each of the four services we examined.

### **3.1 Remote Login (SSH vs. Telnet):**

Since Telnet is assigned its own TCP port (23) which no other protocols use, it is easy to separate Telnet traffic by filtering out traffic not on this port. We quantify Telnet traffic by the number of distinct connections. This information is extracted by identifying unique flows using the source and destination IP addresses available in the trace data.

Obtaining similar results for SSH traffic was not as easy, since SSH shares TCP port 22 with SCP. To differentiate between SSH and SCP flows we calculated the average packet size in addition to the procedure followed for Telnet traffic. Since SCP is a file transfer protocol we expected that its average packet size would be much larger than SSH which just transmits keystrokes and screen refresh messages. This intuition was confirmed by plotting the packet size distribution for port 22. We observed the pattern showed in Figure 1. This distribution allowed us to count the number of distinct SSH connections in the trace data by setting the threshold to 100 bytes.



**Figure 1:** *Packet Size Distribution.*

### **3.2 File Transfer (SCP vs. FTP):**

As with Telnet, FTP is assigned its own exclusive TCP port (20). FTP traffic was quantified and measured in the exact same way as Telnet traffic (number of distinct connections). Likewise SCP traffic was measured and quantified in the exact same way as SSH traffic.

### **3.3 Domain Name Resolution (Secure DNS):**

DNS packets (secure and insecure) use exclusively both TCP and UDP ports 53. In order to differentiate between secure (DNSSEC) and insecure (standard DNS) packets we have to look into the DNS header. The DNS header [7] is shown in figure 2:

										1	1	1	1	1	1
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
ID															
QR	Opcode				AA	TC	RD	RA	Z			RCODE			
QDCOUNT															
ANCOUNT															
NSCOUNT															
ARCOUNT															

**Figure 2:** *DNS Header Format.*

The original DNS reserves the Z field for future use, and it must be zero (000) in all queries and responses. Two bits (authentic data (AD) and checking disabled (CD)) are allocated from this Z field to be used by the DNSSEC. AD is used in a response message to state that the name resolution has been verified by the source. CD is a client option to indicate that verified data is not required. Since secure DNS traffic commonly sets one or both of the AD and CD bits while normal DNS clears them we can differentiate between the two types of DNS traffic by observing these bits in the DNS header.

Since the DNS header is the payload for either TCP or UDP packets and the traces do not contain this information for size and privacy reasons, we do not have this data. Without the DNS header we are unable to differentiate between secure and normal DNS packets.

### **3.4 IP level security (IPsec):**

Since IPsec uses either the AH or ESP protocols which are assigned IP protocol numbers 51 and 50 respectively, we can easily extract these packets from the traces. To quantify IPsec data we count the number of packets. We do not use the number of flows for IPsec traffic (as we did for the previous cases), because any given flow may use both normal IP and secure IP in different segments of its path (tunneling). We believe that comparing two IP protocols by their packet counts results in valid conclusions.

## **4. Results:**

The next four paragraphs present the results obtained by applying the above methodologies to the trace data obtained from [8] (Table 1).

<i>Trace Name</i>	<i>Run Length</i>
19991207-125019-0	13:26:08
19991207-125019-1	13:26:08
20000125-143640-0	03:11:28
20000125-143640-1	03:11:28

**Table 1:** *Trace Files.*

#### **4.1 Remote Login (SSH vs. Telnet):**

Table 2 contains the number of remote login sessions using Telnet and SSH.

<i>Trace Name</i>	<i>Telnet</i>	<i>SSH</i>
<b>19991207-125019-0</b>	357	240
<b>19991207-125019-1</b>	124	58
<b>20000125-143640-0</b>	87	66
<b>20000125-143640-1</b>	94	63
<b>TOTAL</b>	662	427

**Table 2:** *Remote Login Sessions.*

As the data shows, Telnet is more widely used than SSH. One possible reason for this is that Windows users need to download and install SSH applications while Telnet is freely distributed with Windows. Furthermore, the fact that SSH is not available for export (outside US) reduces its user base.

#### **4.2 File Transfer (SCP vs. FTP):**

Table 3 contains the comparison of FTP and SCP traffic.

<i>Trace Name</i>	<i>FTP</i>	<i>SCP</i>
<b>19991207-125019-0</b>	7361	12
<b>19991207-125019-1</b>	2462	18
<b>20000125-143640-0</b>	2006	2
<b>20000125-143640-1</b>	1470	17
<b>TOTAL</b>	13299	49

**Table 3:** *File Transfer Sessions.*

The table shows that SCP is not frequently used. FTP dominates the file transfer domain (excluding HTTP) and our intuition is that this result would hold even by subtracting anonymous FTP traffic, which has no SCP counterpart.

#### **4.3 IP level security (IPsec):**

There were no IPsec packets in any of the trace files measured. The primary reason for this is that IPsec is not currently widely deployed in the Internet. Also IPsec traffic is expected to be spatially bursty, as only a small fraction of hosts need IP level security.

Table 4 shows the percentage of traffic belonging to each IP protocol.

	<i>1999</i>	<i>2000</i>
<b>TCP</b>	87.1137%	86.1298%
<b>UDP</b>	12.1087%	13.2329%
<b>SMTP</b>	0.7774%	0.6372%
<b>AF</b>	0%	0%
<b>ESP</b>	0%	0%
<b>Other</b>	0.0002%	0.0001%
<b>Total</b>	100%	100%

**Table 4:** *IP Protocol Distribution.*

As the table shows TCP dominates the traffic as expected. Together TCP, UDP, and ICMP packets account for nearly all of the packets observed in the trace files.

## **5. Conclusions:**

We have performed measurements of several commonly used Internet services comparing the usage of secure and insecure protocols to perform them. Remote login, file transfer and IPsec results suggest that end users do not currently make use of the secure versions of these Internet services. For remote login, the difficulty of obtaining SSH client software is a major factor for Telnet's continued preference. We believe that users only use SSH if they are forced to do so by system administration policies. For file transfer, most users are not concerned with secure file transfers. Normally, files requiring such protection are being transferred within a trusted network or higher level protection is being applied. Also the lack of user friendly SCP clients is a major drawback. Finally, since many applications have been developed to provide secure data transmission, the usage of IP level security is really limited.

We believe that security is an issue that will become more important in the years to come. Our intuition is that secure protocols will dominate the remote login and (non-anonymous) file transfer domains in the near future. We also believe that the usage of secure high-level protocols will render IP level security redundant.

## **6. Acknowledgements:**

We would like to thank CAIDA for their project ideas and Coral Reef tools. We would also like to thank Dmitrii for providing extra disk storage and Naomi A Ramos for compiling and installing Coral Reef for us to use.

## **7. References:**

- [1] National Laboratory for Advanced Networking Research  
(URL: <http://moat.nlanr.net/>).

- [2] Cooperative Association for Internet Data Analysis  
(URL: <http://www.caida.org/>).
- [3] Coral Reef  
(URL: <http://www.caida.org/tools/measurement/coralreef/>).
- [4] D. Eastlake, CyberCash, C. Kaufman, Iris. [RFC 2065] Domain Name System Security Extensions, January 1997.  
(URL: <http://www.ietf.org/rfc/rfc2065.txt?number=2065>).
- [5] S. Kent, BBN Corp, R. Atkinson, @Home Network. [RFC 2401] Security Architecture for the Internet Protocol, November 1998.  
(URL: <http://www.ietf.org/rfc/rfc2065.txt?number=2401>).
- [6] Larry Peterson, Bruce Davie. Computer Networks: A Systems Approach Second Edition. Morgan Kaufmann publications.
- [7] P. Mockapetris, ISI. [RFC 1035] Domain Names - Implementation and Specification, Page 25, November 1987.  
(URL: <http://www.ietf.org/rfc/rfc1035.txt?number=1035>).
- [8] Auckland-II Trace Files  
(URL: <http://moat.nlanr.net/Traces/Kiwitraces/auck2.html>).