International Journal of Information Technology and Knowledge Management
January June 2009, Volume 2, No. 1, pp. 41-44

PERFORMANCE EVALUATION OF WIRELESS IPSEC VPN

Supriya Pruthi[*] & Gagan Pruthi[**]

When the wireless communications is coming to the offices and the homes, security has always been a significant issue. Today we have continuously growing markets for the wireless LANs, but there is big black hole in the security of this kind of networks. There is currently enormous interest in the design of secure wireless networks. In wireless networks free-space radio transmission makes eavesdropping easy and may result in unauthorized access. Virtual Private networks (VPN) have emerged as a solution. VPN is a network that employs encrypted tunnels to exchange securely protected data.

This paper gives an overview of security issues. The primary objective of paper is to present the implementation of a secure IPSec wireless VPN and evaluates its performance. An IPSec based VPN is constructed between the mobile node and the IPSec Gateway. UDP and TCP performance analysis was done to evaluate the effects of IPSec services on the wireless VPN.

Keywords: VPN, IPSec, TCP, UDP

1. Introduction

In the wireless LAN environment we have to deal with all the same security problems, which we have in the conventional wired LAN environment. But then we have some security issues, which are stressed when we are using the radio path [1, 2, and 3].

1. Eavesdropping

Free space transmission introduces new opportunities for *eavesdropping* in wireless networks. Eavesdropping is very easy in the radio environment, when one sends a message over the radio path, everyone equipped with a suitable transceiver in the range of the transmission can eavesdrop the message. The sender or intended receiver has no means to know if the transmission has been eavesdrop or not, so this kind of eavesdropping is absolutely undetectable.

2. Transitive Trust

When we have a wireless LAN as a part of our enterprise network, it offers one interface to the attacker, requiring no physical arrangements, to intrude on our network. In wired networks we can always track the wire from our computer to the next network node, but when we are working in the wireless environment there is no such way to find out with whom we are talking to. That makes the efficient authentication mechanisms crucial for the security of the wireless LANs. In all cases both parties of the transmission should be able to authenticate each other.

3. Denial of Service

Due the nature of the radio transmission the wireless LANs are very vulnerable against denial of service attacks. If attacker has powerful enough transceiver, he can easily generate such radio interference that our wireless LAN is unable to communicate using radio path. This kind of attack can be done from outside of our site, for example from a van parked on the street or from an apartment in the next block. Equipment needed to commit this kind of attack can be bought from any electronic store with reasonable price and any short-wave radio enthusiast knowledge is needed to construct the equipment.

Author [7] also lists some other security issues: unintentional interference, user location, jamming, service degradation and social engineering. All these issues required some efficient network security technologies to get better wireless network security.

Virtual Private Network (VPN)

A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee [4]. Advantages of a VPN over alternative technologies include improved scalability and cost savings particularly for wireless networking and network management [5].

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end,

[*] Senior Lecturer, ITM, Gurgaon,
E-mail: *Supriya_raheja@rediffmail.com*

[**] Senior Engg., Ericsson India Pvt. Ltd.

send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted [4, 5, and 6]. The various VPN protocols are defined by a large number of standards and recommendations that are codified by the IETF. IPSec is the most dominant protocol for secure VPNs.

IPsec is a suite of protocols for securing IP communications by authenticating and encrypting each IP packet of a data stream. IPsec uses the following protocols to perform various functions: Authentication header (AH), Encapsulated Security Protocol (ESP) & Internet Key Exchange (IKE). Many open source are used to implement IPSec. In this project OpenSWAN is used for IPSec implementation [9].

2. IPSEC IMPLEMENTATION

2.1 Architecture of OpenSWAN

OpenSWAN [12] was used to implement IPSec VPN. OpenSWAN was chosen as implementation source partly because of the range of features it provides and partly because it has an open source code that can be modified and extended. In this project, IPSec VPN is implemented using OpenSWAN with Linux operating system (kernel 2.6). The version 2.2-1of OpenSWAN has been used in this study.

The OpenSWAN, which implements a subset of the IPSec protocol, is installed and configured on it to perform the IPSec gateway functions. OpenSWAN is the freely available IPSec-based VPN software. To implement IPSec, OpenSWAN consists three main parts (As shown in Fig 1):

- KLIPS (kernel IPSec) implements AH, ESP, and packet handling within the kernel
- Pluto (an IKE daemon) implements IKE, negotiating connections with other systems
- Various scripts provide an administrator's interface to the machinery.

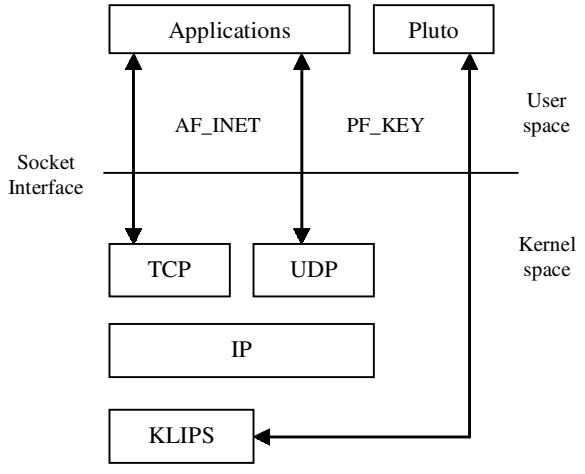

Figure 1: Architecture of OpenSWAN IPSec

IPSec was installed and started correctly

Version check and ipsec on-path	**OK**
Checking for KLIPS support in kernel	**OK**
Checking for RSA private key (/etc/ipsec.secrets)	**OK**
Checking that Pluto is running	**OK**

The IKE daemon "racoon" has also been ported to Linux. This daemon is able to setup automatically keyed IPSec connections. Racoon supports the authentication using preshared keys, X.509 certificates and Kerberos. The certificate and the private key are stored in the certificate path /etc/certs. The certificates and the certificate revocation lists are stored in PEM format as generated with OpenSSL.

Security Verification

A practical way to verify that the packets are encrypted with the correct algorithm is to inter-operate with a trusted IPSec implementation. In one sense this test bed itself is a proof of the correctness of the IPSec connection. It has to be concluded that they are all encrypting with RSA, or none of them is. As long as one independent IPSec implementation is trustable, the other one is as well.

A simple ping test was done to make sure the data is ESP-encapsulated. Ethereal Network Analyzer was used to capture the traffic from and to the interface to which the IPSec interface is bound. There are no ICMP packets, but a few ESP packets can be seen between the relevant machines in both directions.

3. PERFORMANCE EVALUATION

3.1 Testing Environment

The Test bed is built on IEEE 802.11 Wireless LAN. The mobile node (remote user) is an IBM Laptop. OpenSSL is installed on it to provide VPN service for the mobile node. The base station is configured as the wireless bridge. The base station is connected directly to the public network "N1". The IPSec gateway is a PC running Linux; patched OpenSWAN 2.2.1 & OpenSSL are installed & configured on it which provides the certificates for authentication. The firewall rules on the IPSec gateway were specified using IPTables in Linux.

The hardware environment is configured as shown in fig. The specification of hardware used is as follows:

PC for IPSec Gateway

- CPU: Intel® Core™2 Duo processor E7300, 2.66 GHz
- OS: Red Hat Linux 9.0 Kernel 2.6
- OpenSWAN 2.2.1

- OpenSSL

Laptop as a mobile node

- HP laptop
- CPU: Intel® Core™2 Duo Processor T7300, 2.0 GHz
- OS: Red Hat Linux 9.0 Kernel 2.6
- OpenSSL

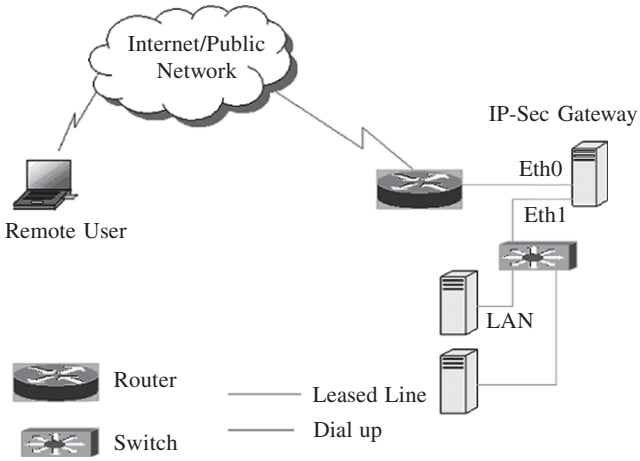

Figure 2

3.2 Experimental Objective

The purpose of the performance evaluation is to get detailed description of how IPSec services affect the behavior of wireless VPNs. Two base stations were used in this analysis. One base station (LT2) was with in 6-7 meters of the mobile node and the other was mounted on the wall about 25 meters from the mobile node. A single test consisted of executing the network traffic generator with appropriate parameters (like peer name, packet size, no. of packets etc.) and calculating the test results on the mobile nodes. Each test with unique parameters was repeated more than 5 times & the average value was used in analysis.

3.3 Analysis

We can see the UDP loss rate for various packet sizes from fig. 3 the signal from the base station (LT1) is weaker than the signal from LT2, so when the packet size increases, the UDP loss rate also increases. The higher packet loss rate is 85-90% for the packet sizes evaluated.

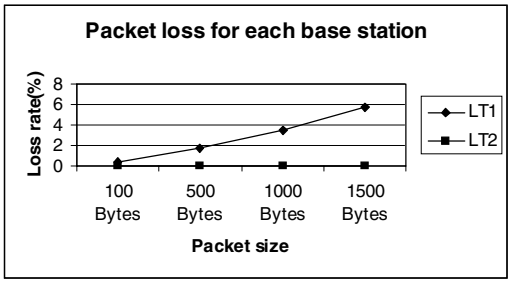

Figure 3: UDP Packet Loss Rate

The result of the UDP throughput (fig 4) shows that even though the signal strength from base station (LT2) to the mobile node was about 150 % of that from base station LT1. The throughput via LT2 was higher than the throughput via LT1 only by a smaller amount (Fig 4). However the throughput difference increases when the packet size increases.

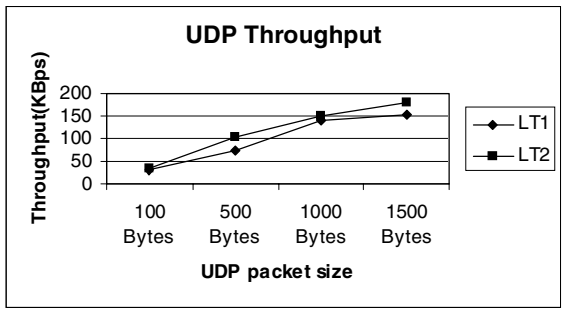

Figure 4: UDP Throughput

Fig 5 shows the experimental results for TCP analysis. TCP throughput without IPSec is roughly 3 times that with IPSec. It can be concluded that IPSec consumes a lot of computing power at both ends of the tunnel. Another observation of TCP throughput is that when packet size was increased, the TCP throughput increased for the connection via base station LT2 but the TCP throughput decreased for the connection via base station LT1. This implies that the different signal strengths, TCP has different optimal packet sizes; a strong signal supports a larger optimal packet size.

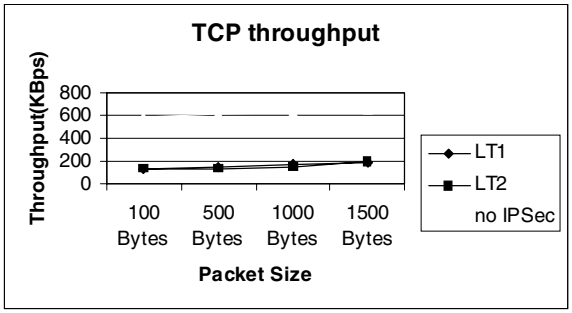

Figure 5: TCP Throughput

4. CONCLUSIONS

To make wireless communication more secure, VPN technology was used in this study. VPN using IPSec security protocol was constructed. The traffic between the wireless node (mobile node) and the IPSec gateway was protected in the IPSec tunnel. OpenSSL is used for the certification. For the completeness of this solution, the relationship of a packet filter firewall and an IPSec gateway was deployed on the basis of OpenSWAN and IPTables on the Linux operating system with kernel 2.4.20.

An IPSec service on wireless networks affects the wireless VPN performance. UDP/TCP performance analysis (loss rate and throughput) was done for data transfer over this VPN. The UDP performance analysis shows that UDP packet loss favors small packet size while the UDP throughput favors strong signals and large packet size. Unlike UDP, TCP has its own mechanism to provide a reliable byte stream. It was found that there exits an optimal packet size for the highest TCP throughput.

References

[1] Russell, S. F., "Wireless Network Security for Users", *Proceedings IEEE International Conference on Information Technology: Coding & Computing*, (2001), 172–177.

[2] Sami Uskela, "Security in Wireless Local Area Networks", *http://www.tml.tkk.fi/Opinnot/Tik110.501/1997/wireless_lan.html*

[3] Korba, L., "Security System for Wireless Local Area Networks", Proceedings of *9th IEEE Int'1 Symp. On Personal, Indoor & Mobile Communications*, (1998), 1550–1554.

[4] R. Venkateswaran, "Virtual Private Networks", *IEEE Potentials*, (Feb. 2001), 11–15.

[5] VPN Website: *compnetworking.about.com/od/**vpn/VPN**_Virtual_Private_Networking.htm*

[6] Roger Younglove, "Virtual Private Networks-how they Work", *Computing & Control Engineering Journal*, (Dec. 2000), 260–262.

[7] Wei Qu, Sampalli Srinivas, "IPSec based Secure Wireless VPN", *IEEE*, (2002), 1107–1111.