Buletinul Ştiinţific al Universităţii "Politehnica" din Timişoara

Seria ELECTRONICĂ şi TELECOMUNICAŢII
TRANSACTIONS on ELECTRONICS and COMMUNICATIONS

Tom 53(67), Fascicola 2, 2008

Design and Implementation of VoIP on Wireless LAN

Seifedine Kadry[1], Khaled Smaili[2], Ali Kalakech[3]

Abstract – Voice over IP (VoIP), also known as Internet telephony, is a form of voice communication that uses data networks to transmit audio signals. VoIP isn't secure since it uses the Internet to which many people connect simultaneously. In this paper, we designed and implemented a Wireless VoIP + OpenVPN system with which secure telephone calls are possible.
Keywords: VoIP, VPN, IPSec, Security, IEEE 802.11

I. INTRODUCTION

The emergence and continual growth of wireless local area networks (LANs) are being driven by the need to lower the costs associated with network infrastructures and to support mobile networking applications. They also represent a solution for the creation of ad-hoc networks in emergency conditions within areas where dense wireless networks exist. VoIP service is based on Internet technologies. With traditional PSTN (public switched telephone network), it is not trivial to eavesdrop because the connection is established in the form of a 1 : 1 circuit. However, VoIP isn't as secure since it uses the Internet to which many people connect simultaneously. In the case of a wireless Internet environment, its security may be further compromised of access point vulnerability. In this paper, we designed and implemented a Wireless VoIP + VPN system with which secure telephone calls are possible using the open project SIP VoIP Gateway 'Asterisk' and 'OpenVPN'. With Wireless VoIP + VPN , we can save money and improve the level of security by integrating voice data with streaming and encryption. In other words, we can get total security by integrating Wireless VoIP and VPN.

II. VoIP SECURITY

We used 'Asterisk[3]' which is an open project for VoIP communication in wireless LAN environments. For client programming, we used QT/Embedded (**Qt** (pronounced "cute" by its creators) is a cross-platform application development framework, widely used for the development of GUI programs) which is an embedded LINUX GUI (Graphical User Interface) library. We use SIP (Session Initiation Protocol)[1] for configuration of mutual connections and RTP (Real Time Transport Protocol) [2] when transmitting voice packets. The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. It can be used to create two-party, multiparty, or multicast sessions that include Internet telephone calls, multimedia distribution, and multimedia conferences. (see RFC 3261). SIP has the following characteristics:

- Transport-independent, because SIP can be used with UDP(User Datagram Protocol), TCP(Transport Control Protocol), ATM (Asynchronous Transfer Mode) & so on.
- Text-based, allowing for humans to read SIP messages.

The Real-time Transport Protocol (or RTP) defines a standardized packet format for delivering audio and video over the Internet. It was originally designed as a multicast protocol, but has since been applied in many unicast applications. It is frequently used in streaming media systems (in conjunction with RTSP) as well as videoconferencing and push to talk systems (in conjunction with H.323 or SIP), making it the technical foundation of the Voice over IP industry. VoWLAN (Voice over WLAN) is a method of sending voice information in digital form over a wireless broadband network. Essentially, VoWLAN is VoIP delivered through wireless technology. The technology is sometimes called "VoWi-Fi" or "Wi-Fi VoIP" because it uses the IEEE 802.11 set of specifications (informally known collectively as Wi-Fi) for transporting data over wireless local area networks and the Internet.

Most wireless local area networks (WLANs) today are built on Wi-Fi technologies, i.e., those based on the IEEE 802.11 wireless standard. IEEE 802.11 is a set of standards for wireless local area network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands. Due

[1] Lebanese University, Faculty of Sciences. Beirut-Lebanon, e-mail skadry@gmail.com
[2] Lebanese University, Faculty of Sciences e-mail ksmeily@hotmail.com
[3] Lebanese University, Faculty of Business e-mail ali_kalakech@hotmail.com

to security reasons, 802.11 employs the wired equivalent privacy (WEP) protocol. WEP was intended to give the wireless data-link a level of security similar to that of naturally-built in wires and optical links. WEP's goals are to provide access control, data confidentiality and data integrity. It does this by using symmetric key mechanisms. With WEP, all devices must have entered into them by the network administrator with a secret WEP key. This is usually done manually. It is by now well known that WEP is extremely vulnerable and can not be counted on to defend against even casual attackers [13] since there are scripts available online that can defeat WEP in a matter of minutes. While there are many proposed fixes for WEP, most of them are not applicable until the next generation of wireless hardware due to their increased computational requirements.

A service set identifier, or SSID, is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one. So, anyone can gain access to a wireless AP with some tools such as NetStumbler which can detect Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards since the SSID is broadcasted to the users of the AP. VoWLAN can also easily eavesdropped by packet sniffing tools like Ethereal. Eavesdroppers have the ability to capture plain and cipher text and get shared key using a protocol analyzer. So, it is susceptible to man-in-the-middle attacks. An attack targeting ARP (Address Resolution Protocol) is a typical man-in-middle attack. This attack exploits the essential point of ARP that enables hackers to impersonate the computer that the user wants to communicate with.

III. SECURE PROTOCOLS

SSL[4]: The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS)[5], which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

OpenSSL is an open source implementation of the SSL and TLS protocols. The core library (written in the C programming language) implements the basic cryptographic functions and provides various utility functions. Wrappers allowing the use of the OpenSSL library in a variety of computer languages are available.

IPSec: IPSec is defined as a set of standards that verifies, authenticates, and encrypts data at the IP packet level. It is used to provide data security for network transmissions. IPSec is a suite of protocols that allows secure, encrypted communication between two computers over an unsecured network. It has two goals: to protect IP packets, and to provide a defense against network attacks. So by operating at the network level, IPSec protections do not interfere with existing application software or protocols, and packets protected by IPSec can be handled by existing routers and routing hosts (see Fig. 1).

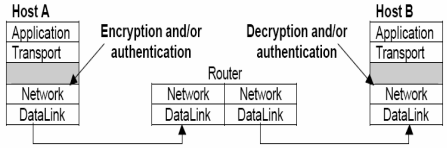

Fig. 1 Transparency of IPSec encryption

The administrator sets a series of rules called an IPSec policy. These rules contain filters that specify what types of traffic require encryption, digital signing, or both. Then every packet that the computer sends is assessed to find whether it matches the conditions of the policy. If it matches the policy conditions, it can be either encrypted or signed according to the policy. This process is transparent to the user and applications that initiate the data transmission.

IPSec policies are delivered to all targeted computers. The policy tells the IPSec driver how to behave and defines the security associations that can establish. Security associations govern what encryption protocols are used for what types of traffic and what authentication methods are negotiated [6].

VPN: One of the most important solutions to viruses and hackers threats is virtual private network "VPN" that makes the network between companies and users secured by using IP security and secure tunnel protocol procedures (see Figure 2) also VPN is authenticated and encrypted for security. So, the idea of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one. VPNs provide the ability for two offices to communicate with each other in such a way that it looks like they're directly connected over a private leased line. The session between them, although going over the Internet, is private (because the link is encrypted), and the link is convenient, because each one can see each others' internal resources without showing them off to the entire world. Basically, 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. Making VPN can extend geographic connectivity, improve security and productivity, and simplify network topology. VPN also provides global networking opportunities and telecommuter support.

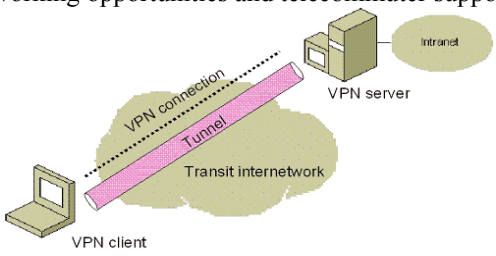

Fig. 2 VPN with secure tunnel protocol

OpenVPN[7, 8] uses the OpenSSL library to provide encryption of both the data and control channels. It lets OpenSSL do all the encryption and authentication work, allowing OpenVPN to use all the ciphers available in the OpenSSL package. It can also use the HMAC packet authentication feature to add an additional layer of security to the connection (referred to as an "HMAC Firewall" by the creator). It can also use hardware acceleration to get better encryption performance. OpenVPN is a full-featured SSL VPN solution which can accommodate a wide range of configurations, including remote access, site-to-site VPNs, WiFi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls.

The following table contains a comparison between SSL-VPN against IPSec-VPN.

	SSL-based VPN	IPSec-based VPN
Authentication	One-way authentication tokens Two-way authentication tokens Digital Certificates	Two-way authentication using tokens Digital certificates
Encryption	Strong Encryption Browser based	Strong Encryption Depends on implementation
Overall Security	End to End security Client to Resource encrypted	Edge to client Client to VPN gateway only encrypted
Accessibility	Anywhere anytime access to broadly distributed user base	Access limited to well-defined and controlled user base
Cost	Low No additional client software needed	High Managed client software required
Installation	Plug and play installation No additional client-side software or hardware installation	Often long deployments Requires client-side software or hardware
Simplicity for user	Very user friendly - uses familiar Web browsers No end user training required	Challenging for non-technical users Requires training
Applications Supported	Web-enabled applications File sharing E-mail	All IP-based services
Users	Customers, partners, employees, remote users, vendors etc.	More suited for internal company use
Scalability	Easily deployed and scalable	Scalable on server side Difficult to scale clients

Table 1 SSL-VPN vs IPSEC-VPN

IV. THE QoS ARCHITECTURE FOR VOIP SERVICES

In our design, we consider an IEEE 802.11e wireless network operating in the infrastructure mode to support VoIP applications. In addition, the *Session Initiation Protocol (SIP)* has been widely accepted as the signaling protocol for VoIP to handle the setup, modification, and teardown of VoIP sessions[11, 12], so we adopt it for call setup and management. We also assume that a VoIP session can dynamically adjust its packetization interval (PI) even during communication, where PI represents how frequently voice data should be encapsulated into packets. Our purpose is to guarantee high QoS for admitted VoIP sessions when the network load is not heavy, and to support as many VoIP connections with acceptable QoS as possible when the network load is heavy. RFC 3312 (Integration of Resource Management and SIP) discusses how QoS can be made a precondition for sessions initiated by SIP. These preconditions require that participants reserve network resources before continuing. Inspired by this, we propose an architecture for IEEE 802.11e to incorporate with SIP to conduct resource reservation and admission control.

V. DESIGN AND IMPLEMENTATION OF VOIP USING OPENVPN AND IPSEC

Hardware: We use a PC with Intel's Pentium IV 3.0 GHz CPU with 1024MB RAM as figure 3. It can be connected and interoperated with PSTN with Digium's TMD400P card on PCI. The TDM400P card consists of two FXO modules. One is connected to a typical telephone and VoIP network, the other is for PSTN.

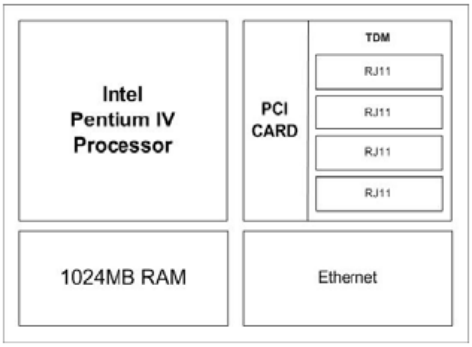

Fig. 3 Block Diagram of Server H/W

We used Bookdoo's IN-DVK-P255B embedded board as a client(Figure 4) with Intel's XScale PXA255 CPU, 128 MB SDRAM, 64MB Flash Memory and PCMCIA interface. We used PCMCIA Wireless LAN Card for IEEE 801.11e connectivity.

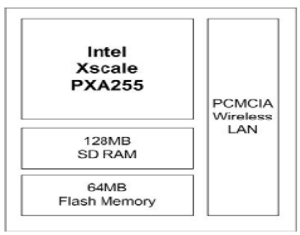

Fig. 4 Block Diagram of client H/W

Software: In this paper, we designed and implemented VPN based VoIP using the open project SIP VoIP Gateway 'Asterisk' and 'Openvpn'.

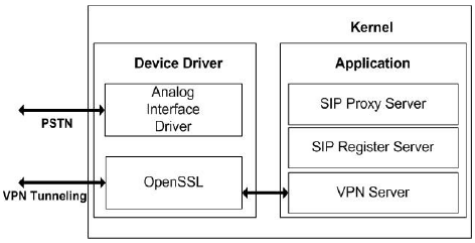

Fig. 5 Block Diagram of Server S/W

As shown in Fig. 5, clients connect to the server and establish VPN connections between the clients, then transmit encrypted packets using a tunnel interface.

Network Configuration:

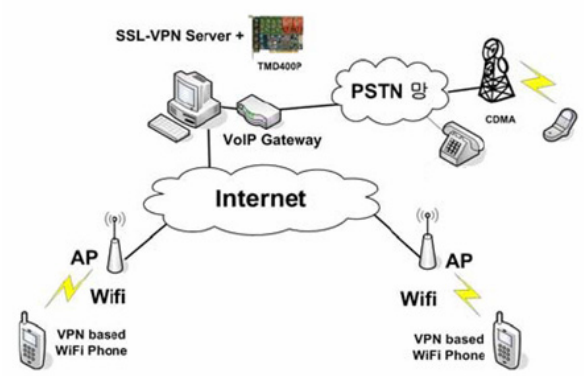

Fig. 6 Network Configuration

We configured the networks as per Figure 6 and used the embedded boards with WiFi as a WiFi phone. The server operates as a SIP Proxy Server and the codec for voice compression is G.711. The server also works as a VPN-Server and is configured to connect authenticated users with the Tunnel-Interface. We can use PSTN networks using the server FXO terminals. We compared the voice quality between a typical VoIP call and our VoVPN call. We measured the Round Trip Time which is the time between sending and receiving voice packets to get the end-to-end packet delay time. We checked that the difference between the end-to-end packet delay time of a typical VoIP call and our VoVPN call is less than a maximum of 15ms. We hypothesize that the greater part of the delay time is used to encapsulate packets for VPN tunneling. It is less than the ITU-T suggested end-to-end packet delay time limit of 150ms ~ 200ms [9, 10].

VI. CONCLUSION

In this paper, we designed and implemented a Wireless VoIP + VPN system with which secure telephone calls are possible using the open project SIP VoIP Gateway 'Asterisk' and 'Openvpn'. With Wireless VoIP + VPN, we can save money and improve the level of security by integrating voice data streaming and encryption. We measured the end-to-end packet delay time of a typical VoIP call and our VoVPN call for performance evaluation. The difference between our system and a typical VoIP call is under 15ms and less than the ITU-T suggested end-to-end packet delay time limit of 150ms ~ 200ms.

REFERENCES

[1] RFC 3261, M. Handley, H. Schulzrinne, E. Schooler, J. Resenberg "SIP: Session Initiation Protocol". *IETF*, Jun 2002.
[2] RFC 1890, "RTP Profile for Audio and Video Conferences with Minimal Control", IETF, Jan. 1996.
[3]http://asterisk.org/about. "What is Asterisk".
[4] “Review of Wireless Internet Security Technologies” , KISA 2001-11.
[5]Stephen A. Thomas, *SSL and TLS Essentials*, Wiley, 2000.
[6] J.H.Nahm, “Compare & Implementation of IPSec VPN vs SSL VPN”, Semyung Uni., 2004
[7]http://openvpn.net/. “OpenVPN"
[8] http://www.ethereal.com/introduction.html, "Features".
[9] TIA/EIA/TSB116, Voice Quality Recommendations for IP Telephony, Mar 2001.
[10] A. Percy, *Understanding Latency in IP Telephony*, Brooktroot Technology.
[11] J. Rosenberg, H. Schulzrinne, E. Schooler, M. Handley, G. Camarillo, A. Johnston, J. peterson, and R. Sparks. *SIP: Session Initiation Protocol, RFC3261 in IETF*. June 2002.
[12] Daniel Conllins. *Carrier Grade Voice over IP Second Edition*. McGraw-Hill Companies, Inc, 2003.
[13] Thuc D. Nguyen, Phu C. Nguyen, Bao N. Tran and Hai Vu "A Software Solution for Defending against Man-in-the-Middle attacks on WLAN" In GESTS transactions on Computer Science and Engineering (www.gests.org) Vol. 24, No. 1, December 2005.