An Enterprise Security Model AAPN (Authenticator AccessPoint VPN) for WLAN using Intel- IXP1200 Network Processor

K.RATHI ANAND, DR.C.CHELLAPPAN
Department of computer science and engineering
Anna University
Guindy, Chennai-25
INDIA

Abstract: - This paper provides a security model for WLAN networks built using a network processor. This model encompasses the best security practices for the enterprise WLAN environment by integrating the 802.1x protocol functionality and VPN functionality in the AccessPoint.The model is named as "Authenticator AccessPoint VPN" (AAPN). Cryptographic functions have been widely implemented in network devices and this model is implemented using a network processor, Intel IXP1200, a widely used network processor. This paper focuses more on developing AAPN on the Intel IXP1200 and discusses the benefits of developing it in the network processor from the perspective of medium-large Enterprise WLAN.

Key-Words: - Security model, Wireless LAN, Acess Point, IPSEC, 802.11,Enterprise WLAN

1 Introduction

A WLAN environment requires a number of security mechanisms to be implemented for a secure transmission of data. There are several dedicated processors in the market for running these security mechanisms individually. Salient trend has it that many network devices integrate cryptographic functions to gratify the increasing needs of security. Especially encryption/decryption and digital signature algorithms are expensive and dramatically affect the overall performance. Hardware solutions suffer from cost and flexibility while software approaches compensate the drawbacks at the cost of performance. Network Processor, a device between GPP (General Purpose Processor) and ASIC (Application Specific Integrated Circuit) caters for the requirements of performance and flexibility simultaneously. We have implemented our model AAPN (Authenticator AcessPoint VPN) using the network processor-Intel IXP1200. AAPN authenticates wireless clients using the 802.1x protocol and tunnels the packets to wired network using the IPSEC.

2 Network Processor

In this section we analyze the general architecture of prevailing commercial network processors, using INTEL IXP series as an example. To satisfy the requirements of intelligent processing, most commercial network processors are designed with following technologies:

- Pipeline and parallel mechanism. Network processors can contain multiple processing elements which are organized either in pipeline or parallel manners
- Optimized memory units. Memory access is an expensive task. This feature provides the feasibility of latency hiding and reimburses the drawback of small cache.
- Special ALU instructions. This is originally used to accelerate route applications, which still suits cryptographic applications' needs.
- Hardware multithread. Many network processors apply "zero switching overhead" hardware threads to increase utilization rate.

All these features help network processors to achieve better performance; in this article we use Intel IXP1200 as the platform, which typically incarnates all characteristics mentioned above.

Intel IXP1200 is the most widely used network processor, it is made up of 6 high speed Microengines and one Strong ARM management core. Each microengine owns 4 hardware threads and only one thread can be activated at any time. Microengines and StrongArm are all RISC based processors sharing memory, bus and other off chip resources, while microengines carry fast path applications and StrongArm does slow path jobs.

3 Wlan Security

The 802.11b WLAN included a default encryption standard WEP (WIRED EQUIVALENT PRIVACY), which was proven flawed [6]. A plethora of security mechanisms were proposed by

several organizations in order to realize a secure WLAN environment. Among these solutions we have selected two proven technologies from the enterprise WLAN perspective viz. VPN using IPSEC [9] and 802.1x[8] to provide an end-to-end security for WLAN. We have incorporated these two features into an access point (AP),which is the interface for the wired and the wireless network. Restricting access to and from the AP from the wireless side is performed using 802.1x and while the wired side is protected with IPSEC security, as this model includes the functionality of Access point, 802.1x and VPN it has been named as "Authenticator Access point VPN"(AAPN).Before discussing AAPN functionality lets have an overview of 802.1x (EAP-MD5) and VPN employing IPSEC.

3.1 Authentication Protocol 802.1x

The enforcement of strong user authentication is critical to securing access to wireless LANs. IEEE 802.1x is a port-based authentication protocol to secure communications over 802.11 Wireless LANs. This standard defines the Extensible Authentication Protocol (EAP), which uses a central authentication server to authenticate each user on the network. The 802.1X protocol framework, with its many supported EAP protocols, provides standard user authentication. Here AAPN supports EAP-MD5 type.Therefore this model does not support WEP.

Initial 802.1X communications begins with an unauthenticated supplicant (i.e., client device) attempting to connect with an authenticator (i.e., 802.11 access point). The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other packets, until the access point can verify the client's identity using an authentication server (e.g., RADIUS). Once authenticated, the access point opens the client's port for other types of traffic.

3.2 Virtual Private Networks

A virtual private network (VPN) refers to a set of solutions and technologies designed to make secure (encrypted) site-to-site and remote-access connections over public networks.

The two primary technical issues in setting up VPNs are tunneling and encryption.

3.2.1 Tunneling

It is the process of encapsulating the protocol header and trailer of one network protocol into the protocol header and trailer of another. Before the packet is sent across the network, it is encapsulated with new header information that allows an intermediary network to recognize and deliver it. Packets in a tunnel mode possess both an outer header that specifies the IPSec processing destination, and an inner header that specifies the ultimate destination for the packet. If Authentication Header is employed in tunnel mode, portions of the outer header are afforded protection, as well as the entire encapsulated packet. When the transmission ends, the tunneling header is stripped off, and the original packet is delivered to the destination. In AAPN, a VPN tunnel employing IPSEC is established at the Layer 2.

3.2.2 Encryption

While tunneling allows data to be carried across a third-party network, it does not protect data against unauthorized inspection or viewing. To ensure tunneled transmissions are not intercepted, traffic over a VPN is typically encrypted.

IPSec uses two major protocols to carry out its purpose. These two protocols are the Authentication Header (AH) and Encapsulating Security Payload (ESP).AAPN uses ESP in tunnel mode and on the top of it applies AH in transport mode.

The encryption /decryption algorithm used in AAPN is 3DES and the authentication algorithm used is the MD5.

4 Assumptions

The following assumptions are made with AAPN

- It is assumed that the WLAN terminals accessing the access point have already been registered and hence the authentication server (RADIUS) sends only the accept message to the access point.
- It is assumed that the VPN servers accessing the access point have already been registered.
- It is assumed that the MAC frames are available to the accesspoint, with all the incoming packets having the same priority, and the payload of the 802.11 packets are lesser than or equal to the maximum payload of Ethernet packets.
- It is assumed that the keys required for the 3DES are distributed in a secure manner.

5 Functional Description Of Aapn

The AAPN accepts authenticated packets from the wireless LAN and sends it to the wired network using the IPSEC.VPN employing IPSEC has been

widely employed by several enterprises to provide high-level security for their networks at low cost, and the 802.1x protocol has been widely used by several enterprises to authenticate each user in the network. Hence the model AAPN with these security mechanisms is better suited for enterprise networks, such as the enterprise WLAN.The functional block diagram of AAPN from Figure1 is described as follows

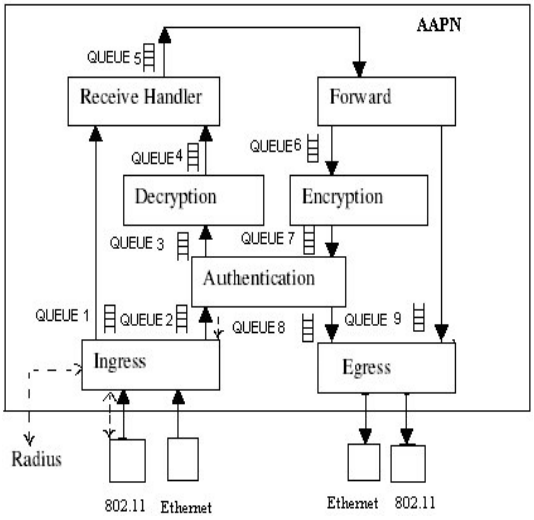

Fig 1.Functional Block Diagram of AAPN

5.1 Ingress

5.1.1 802.11 ingress

A wireless client needs to be authenticated before sending packets; the client sends an EAP-start message. The Ingress block replies with an EAP-request identity message. The Authentication block creates this using the MD5 algorithm. (It is assumed that the client sends an EAP-response packet containing the identity to the authentication server, which verifies the client's identity. The authentication server sends either an accept or reject message to the Ingress block, following which the Ingress block sends an EAP-success packet (or reject packet) to the client. It is assumed that the authentication server sends an accept message and the Ingress sends success packet to the client). Now the Ingress block sends signals to all the buffers, queues and threads. The authenticated client can now send packets. Till this, it is known as the initialization phase and the Ingress block starts the actual ingress processing from this point onwards. The ingress receives packets from 802.11 port and stores them in a buffer in SDRAM.A packet descriptor containing the number of quadwords and bytes is constructed and stored in SRAM.The address of the packet descriptor is sent to queue1, which is read by the Receive Handler.

5.1.2 Ethernet ingress

The ingress for Ethernet receives packets from the Ethernet port and stores them in a buffer; the address of the packet descriptor is put into queue2, which is received by the authentication block.

Reserved	NoQuad words	No Bytes
31:11(bits)	10:3(bits)	2:3(bits)

Table1.Packet Descriptor Format.

Destination MAC address	Source MAC address	Pointer to data packet in memory	Port No
6 Bytes	6 Bytes	4 Bytes	2 Bytes

Table 2.Internal Packet Format (IP)

VPNserver address	MAC address
6 Bytes	6 bytes

Table 3.Tunnel Table Format

Destination MAC address	Port No	Time Stamp
6 Bytes	2 Bytes	2 Bytes

Table 4.Bridge Table Format (BT)

5.2 Authentication Block

The authentication block is started even before the reception of packets to create the challenge text for Ingress block. Once the client is authenticated, the authenticator receives the address of the descriptor from Queue2, which is sent by the ingress block. Now the authentication blockverifies the Authentication header (AH) of the Packet using the MD5 algorithm. If the test is passed the, packet is stored in a buffer and the address of the packet descriptor is put in to Queue3, which is sent to the decryption block, else the packet is discarded.

When the authentication block receives the address of the packet descriptor from Queue7, the authentication header is created (in transport mode)for the encapsulated packet using MD5 and it is inserted between the encrypted portion (after the ESP header) and the outer header of the packet. The packet is stored in a buffer and the address of the packet descriptor is placed in

Queue8.

5.3 Decryption

The decryption block receives the address of the packet descriptor from queue3 and decrypts the payload portion of the packet using the 3DES algorithm. The decryption involves three keys where each key is used to decrypt, encrypt and decrypt respectively The decrypted payload is stored in a buffer (thus, the outer header that carries the addresses of the source and the destination (AAPN) VPNservers, and AH header is stripped off) and the address of the packet descriptor is sent to queue4 which is read by the receive handler.

5.4 Receive Handler

5.4.1 Receive handler for Ethernet

The receive handler for Ethernet receives the address of the packet descriptor from queue4. It gets the source and destination address from the Ethernet header. It searches the bridge table (BT). The bridge table has entries mapping station address to ports. If entry is found in the BT only then the timestamp is updated else a new entry is added. If the port number in the entry for that address is equal to source port number, then the memory buffer held by that packet is freed. Else an Internal packet (IP) is constructed which contains the details of source address, destination address, pointer to the actual memory and the port number. It is then placed in queue5 and sent to the forwarding module.

5.4.2 Receive handler for 802.11

It simply gets the address of the packet descriptor from queue1 and performs the operations mentioned above in the 802.11 context. It constructs the IP and it is placed in Queue5, which is sent to the forwarding module.

5.5 Forwarding Module

The forwarding module receives the packets from queue5. If the source port is 802.11, it then constructs the corresponding Ethernet header for these packets, calculates the CRC. It then copies the constructed packets in to a buffer. The address of the packet descriptor is placed in queue6.

If the source port is Ethernet, it calculates the corresponding 802.11 headers and calculates the CRC. It then copies the constructed packets in to a buffer; the address of the packet descriptor is placed in queue9, which is received by the Egress for 802.11.

5.6 Encryption Block

It gets the descriptor address from queue6. It gets the source and destination address from the Ethernet header. A tunnel table is maintained, with the entries mapping the VPN server addresses with the MAC addresses of its internal network. If an entry is found in the table for the source MAC address, then the corresponding server address becomes the source server address in the outer header, and the server address that corresponds to the entry of destination MAC address becomes the destination server address in the outer header. The original header and the payload are encrypted with the 3DES algorithm, the encryption involves three keys where each key is used to encrypt, decrypt and encrypt respectively and the constructed outer header is attached to it.

The ESP header is constructed and attached to it before the outer header. The packet is stored in a buffer; the address of the packet descriptor is placed in queue7, which is read by the authentication block.

5.7 Egress

5.7.1 802.11 Egress

It obtains the address of the packet descriptor from Queue9 and sends the packets to the corresponding 802.11 interface.

5.7.2 Ethernet Egress

It obtains the address of the packet descriptor from Queue8 and sends the packets to the corresponding Ethernet interface.

6 Aapn Performance

Performance estimate of AAPN doing IPSEC and 802.1x is shown in the graph. As 802.1x comes only during the initialization phase, this graph mainly shows the AAPN doing the IPSEC. Performance on the IXP1200 was measured using version2.0 Developer Workbench software assuming a microengine clock rate of 200MHz and an IX bus clock rate of 83MHz.In theory as packet size increases, packet throughput should also increase, but in practice we observe that reduction in throughput occurs, for increasing packet size. This is due to the 64-byte alignment of transmit and receiveFIFOs on the IXP1200.Extra processing and transmission time are required for nonaligned packet segments. Overall, this is sufficient performance to encrypt and authenticate at 1gigabit/sec.

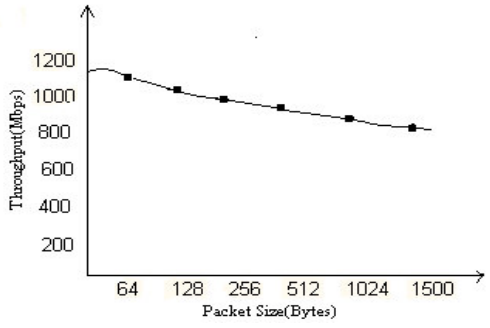

Fig2.Performance estimate of AAPN

7 Conclusion

AAPN authenticates wireless clients using the 802.1x protocol and tunnels the packets to wired network using the IPSEC.AAPN incorporates better security practices from the enterprise WLAN perspective and the main advantage of building this AAPN into a network processor is that; the systems built into network processors can be changed or upgraded quickly. This feature is considered a significant point for building this WLAN security model AAPN because, day by day a plethora of protocols are suggested for securing WLAN environment, and the enterprise network should be flexible enough to adopt a new standard over time without increasing the overall cost required to do it. Together with all these benefits it is also proved that the performance is not compromised for security. Future enhancements can be made to optimize the cryptographic and authentication algorithms used in AAPN.

References

[1] *Kuorilehto, M. et al., "Implementation of wireless LAN access point with quality of service support" IECON 02 [Industrial Electronics Society, IEEE 2002 28thAnnual Conference], Volume: 3, Nov 5-8,2002 Page(s): 2333 –2338.*

[2] *M.Hännikäinen, et al., "Windows NT Software Design And Implementation for a Wireless LAN Base Station", ACM International Workshop on Wireless Mobile Multimedia (WoWMoM'99), August 20, Seattle,USA, pp. 2-9.*

[3] *Intel ® Microengine C Networking Library for the IXP1200 Network Processor, Reference Guide, Version 1.0, December 2001.*

[4] *W.Fegheli, B.Burres, and G.wolrich, K. Elissa, "Security: Adding protection to network via network processor", Intel Technology Journal",vol 6,no 3 ,pp 40-49,August 2002.*

[5] *B.Scheneir and D.Whiting "Fast software encryption: designing encryption algorithms for optimal software speed on Intel Pentium Processor", Proc, Fast Software Encryption, 4th international workshop, Haifa Isreal, pp.240-259, January 1997.*

[6] *J.Walker,"Unsfe at any Key Size: An Analysis of the WEP encapsulation", IEEE 802.11-00/362 IEEEPress,2000www.netsys.com/library/papers/walker-2000-10-27.pdf.*

[7] *www.developer.intel.com*

[8]*ww.mtghouse.com/MDC_EAP_White_Paper.pdf*

[9] *www.hifn.com/info/pr/pressreleases /pdf/20020605.pdf*