Design Universal Security Scheme for Broadband Router

Xiaozhuo Gu[1,2] and Jianzu Yang[2]
(Corresponding author: Xiaozhuo Gu)

National Digital Switching System Engineering & Technological R&D Center, China[1]
Information Engineering University, China[2]
No 783 Po Box 1001, 450002, Henan, China
(Email: guxiaozhuo@yahoo.com, yjzxxgc@gmail.com)

(Received Aug. 29, 2007; revised and accepted Jan. 30, 2008)

Abstract

Taking account of defections existed in general methods of implementing IP security (IPsec) in broadband routers, a secure scheme based on fast path and slow path of routers was put forward. The scheme implements IPsec with Encryption chip and IPsec software combined, and adopts Encryption adaptive board to support multi-encryption chips. No requirement for change in original hardware architecture of broadband router makes the scheme universal. Wire-speed data forwarding and encryption are processed in fast path, while local data and protocol data which are non-real time tasks are processed in slow path, in which IPsec security policy (SP) and security association (SA) are also transferred. The scheme was tested in SR1880s, and testing results showed that the proposed scheme can satisfy the security needs of broadband router.

Keywords: Encryption chip, fast path, IPsec software, security architecture, slow path

1 Introduction

IP security protocol (IPsec) is running in IP layer to protect communications between peers and enforced to implement in IPv6 protocol [2, 9]. With development of Next Generation Internet (NGI) which bases on IPv6, routers are required to implement IPsec. Small routers can accomplish this function using software, whereas it is not practical for large-scale router, such as broadband router. Owing to this, specific encryption chip was developed to improve processing speed. Through study on existing security architecture that implements IPsec in broadband router using hardware accelerators [4, 10], such as Look-aside and FlowThrough architecture, we found the key problem we should solve is to design a universal and efficient security architecture which can implement IPsec in broadband router without changing the original hardware architecture and sacrificing the whole performance of the router.

To achieve this, we design universal security architecture, based on Encryption adaptive board, fast path, and slow path, which will have practical meaning to broadband router. Actually, Integrating IPsec in Network processor (NP) or Application specific integrated circuit (ASIC) will achieve higher performance, but it's not the focus we concentrated on.

2 General Security Architecture of Broadband Router

2.1 Universal System Architecture of Broadband Router System

architecture of broadband router has experienced bus-based router architectures with single processor, bus-based router architectures with multiple processors, switch-based router architectures with multiple processors, and switch-based router architectures with fully distributed processors [1, 5, 6, 7, 8]. Switch fabric architectures with distributed paralleled-multiple processors, shown in Figure 1, is universal system architecture of router at present [1, 5, 6, 7, 8]. This architecture is constituted of Network processing unit, Master control unit, and High-speed switching network. Network processing unit comprises two parts, Line card interface module and Forwarding module.

Line card interface module receives physical frame arriving on line, extracts IP packet from physical frame and sends it to Forwarding module. It also receives IP packet from High-speed switching network, then encapsulates the packet into physical frame, and sends it out finally. Forwarding module is designed to process the packet in IP layer. It forwards the processed IP packet to High-speed switching network. Master control unit manages routing calculation, network management, device configura-

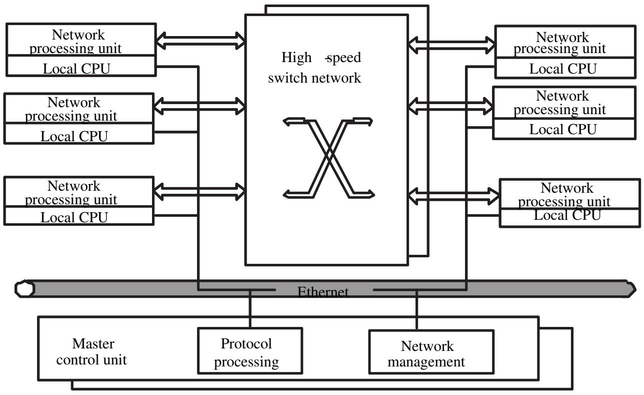


Figure 1: Universal system architecture of broadband router

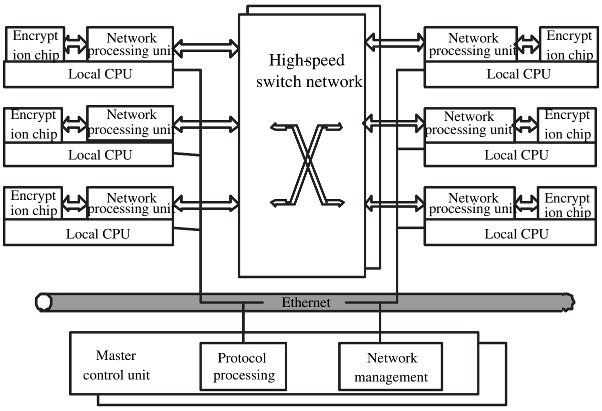


Figure 2: General security architecture of broadband router

tion and control. High-speed switching network switches packets between network processing units and provides services according to different operation levels.

2.2 General Security Architecture of Broadband Router

General method of implementing IPSec, such as FlowThrough security architecture, is to concatenate encryption chip before the network processing unit [4, 10], which is shown in Figure 2. In this architecture, packet processing and decryption functions for inbound traffic are completed before the traffic reaches the network processing unit, freeing the traffic management silicon to handle what it does best. Most of the companies adopt FlowThrough security architecture in designing the security processor at present [4, 10]. However, letting all the packets passing through the security processor aggravates the workloads of security processor.

Further more, one security processor in front of each network processing unit is somewhat a waste. There are three main defections in this security architecture. For the first, each Network processing unit needs one Encryption chip. So each packet passing Network processing unit also passes Encryption chip.

Actually there is a small part of traffic that needs to be processed by Encryption chip, which will lead to waste of Encryption chip and slow the processing speed. Second, for broadband router implementing in single-shelf, the problems of power waste, heat dissipation, and electromagnetic compatibility will become severer and N Encryption chips will get this worse. Last, the architecture requires compatibility of physical criterion and electrical criterion among interfaces of Encryption chip, Network processing unit and High-speed switching network, which will make the architecture more complex.

3 Universal Security Architecture

3.1 Universal Security Architecture of Broadband Router

We design universal security architecture shown in Figure 3, which does not need to change the original hardware architecture of router and has several merits listed below. First, to fully utilize advantages of fast path and slow path, we implement IPsec with Encryption chip to process high-speed forwarding data in fast path, and embed IPsec software inside Master control unit to process nonreal time data in slow path. Second, to make the architecture universal, Encryption adaptive board is adopted and shown in Figure 4.

The numbers of Encryption chip and Encryption adaptive board are both changeable. We can change the number of Encryption chip in one Encryption adaptive board according to anticipated traffic passing through router. When one adaptive board full loaded can not meet the need, more Encryption adaptive boards can be added. Third, considering universal interface of Encryption adaptive board, two types of interface are designed. One is between Encryption adaptive board and High-speed switch network, and the other is between Encryption adaptive board and Local CPU. Adaptive circuit of interface can be implemented with Field programmable gate array (FPGA), so it can support various interface types dynamically.

For the outer physical interface, Encryption adaptive board can support n different types according to demand as shown in Figure 4. Fourth, IPsec software excluding Internet key exchange (IKE) is designed to embed in kernel of Master control unit. Toward different platforms, various interfaces are designed. So it is portable for IPsec software to different platforms.

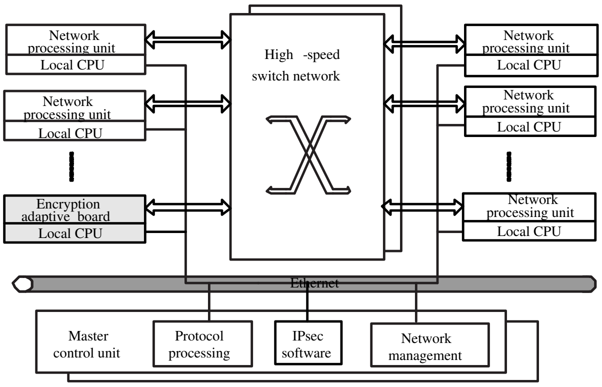


Figure 3: Universal security architecture of broadband router

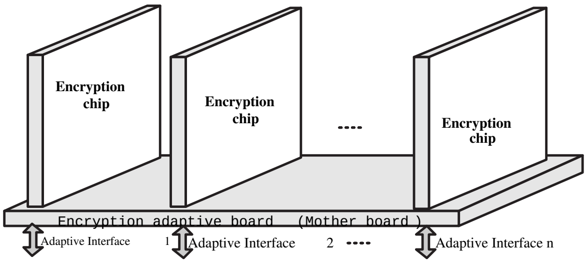


Figure 4: Universal encryption adapter board

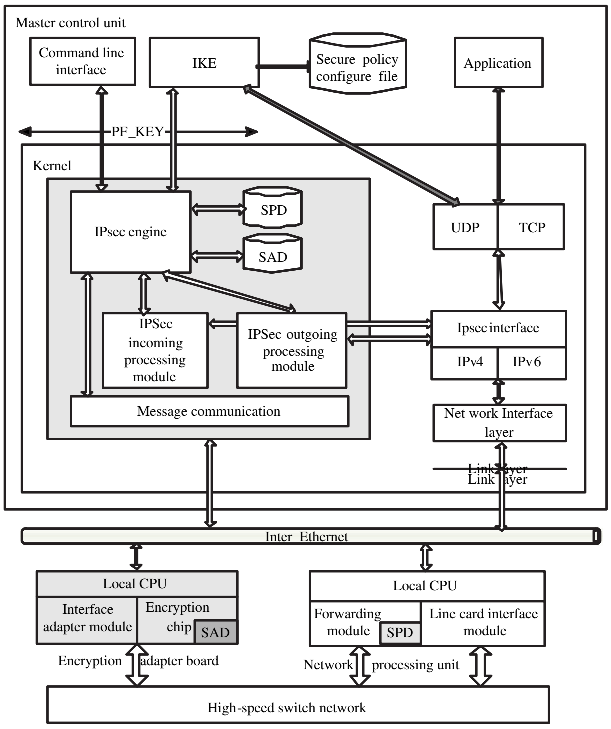


Figure 5: Detailed universal security architecture

3.2 Detailed Universal Security Architecture Based on Fast Path and Slow Path

Figure 5 shows detailed universal security architecture of broadband router. For packet passing through fast path, Encryption chip performs encryption or decryption according to requirement. Whereas for packets passing through slow path, Master control unit controls IPsec incoming processing module and IPsec outgoing processing module to perform decryption and encryption separately. Two modes work together to provide security protection for the traffic passing through router. Command line interface (CLI), IPsec engine and IKE work together to provide security policy (SP) and security association (SA) for both modes.

3.3 Encryption and Decryption Flow in Fast Path

When system is powered on, CLI begins to add SPs to IPsec Engine. Then IPsec engine transfers these SPs to Forwarding module via inter Ethernet. In the condition of manual key configuration, SAs are also added to IPsec engine by CLI and transferred to Encryption chip. For packet passing through the router, it is first received by Line card interface module. Packet whose destination is not local router is transferred to Forwarding module. Then Forwarding module executes lookup in its security policy database (SPD) to see whether there has SP for this packet. If it has, the packet will be labeled encryption or decryption flag and forwarded to Encryption chip. If CLI didn't add SA manually or the packet of this application is first coming, there will not be appropriate SA in security association database (SAD) of Encryption chip for this packet. In this case, Encryption chip disposes the packet and sends Acquire message to IPsec engine. Then IPsec engine sends Acquire message to waken IKE, and IKE begins to negotiate with the peer. Otherwise for packet needing encryption, Encryption chip gets encryption type and encryption key from SAD to perform encryption. For packet needing decryption, Encryption chip gets decryption type and decryption key from SAD according to source and destination addresses, protocol type, and security parameter index (SPI) to perform decryption. Then the encrypted or decrypted packet is sent to High-speed switching network and sent out through Line card interface module finally. The detailed flow can be seen in [3].

3.4 Encryption and Decryption Flow in Slow Path

If the destination of incoming packet is local router, the packet is transferred to Master control unit through slow path by Local CPU of Line card interface module. Packet sent out by Master control unit also goes through slow path. For these two types traffics, IPsec software performs encryption or decryption according to requirement. For incoming packet whose destination is local, it is sent to Master control unit by Line card interface module. Receiving packet, IPsec interface checks the next header of the packet. If the next header is Authentication Header (AH) or Encapsulating Security Payload (ESP), IPsec interface calls IPsec incoming processing module to process the packet. Then IPsec incoming processing module communicates with IPsec engine to get SA and perform decryption. If SA for this packet does not exist, the packet will be disposed and IPsec engine sends Acquire message through PF_KEY socket to IKE to waken IKE for negotiating SA. For outgoing packet sent by Master control unit, the packet is first sent to IPsec outgoing processing module to check whether the packet needs encryption or not. When receiving packet, IPsec outgoing processing module communicates with IPsec engine to get SP. If there doesn't exist SP for this packet, the packet will be processed through usual flow. If there exists SP, IPsec outgoing processing module continue communicates with IPsec engine for SA to perform encryption. If SA does not exist, the packet is disposed and IPsec engine sends Acquire message to IKE to negotiate SA. Otherwise the packet is encrypted and sent out through Line card interface module. The detailed flow can also be found in [3].

4 Testing

We implemented our design in SR1880s, a secure broadband router developed by National Digital Switching System Engineering & Technological R&D Center of China (NDSC). Testing is carried out in this router. We design two frameworks to test two modes separately.

1) Testing Framework for Encryption Chip:
We tested the function of both encryption and decryption of Encryption chip using IPv6 raw socket program. Testing framework is shown in Figure 6. The framework comprises one broadband router and two personal computers (PC). PC 1 and PC 2 are connected to two Network processing units respectively. We use manual SA to make our test convenient. At first, SP and SA that need encryption from PC 1 to PC 2 were added to Network processing units and Encryption chip by CLI respectively. To validate correctness of the encryption result by Encryption chip, PC 1 ran program which sends raw IPv6 packet. Packet PC 1 sent was first received by Network processing unit 1, and then forwarded to Encryption chip through High-speed switching network to perform encryption. After encryption, the packet was sent back to high-speed switching network and sent out by Network processing unit 2. Finally the packet was received by PC 2, where the original file PC 1 sent was stored in advance. We encrypted original file in PC 2 and compared it with received encrypted packet to check correctness. The way to validate correctness of decryption is the same as above except that SP and SA from PC 1 to PC 2 were decryption. The packet was encrypted in PC 1 and sent out.. Then the encrypted packet was forwarded to Encryption chip for decryption and received by PC 2 finally. Receiving the plain packet, PC 2 compared it with original file saved in advance.

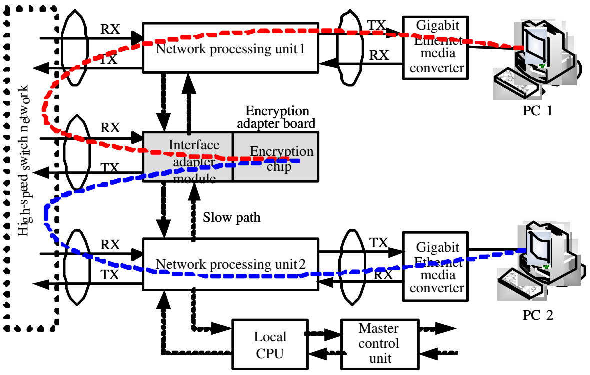
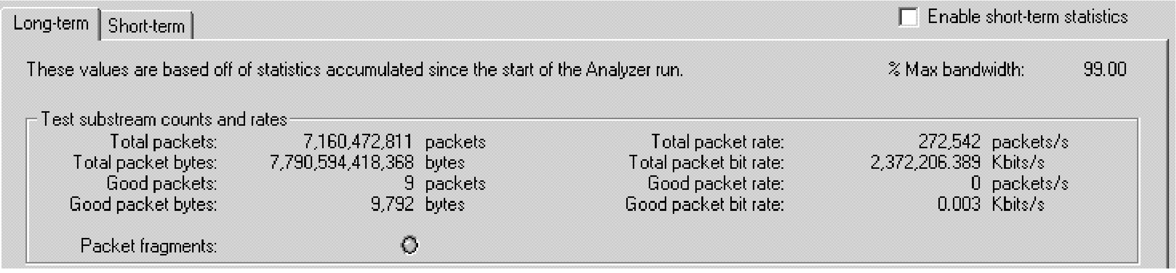


Figure 6: Framework of testing Encryption chip

2) Testing Framework for IPsec software inside Master Control Unit:
We tested encryption and decryption of IPsec software using framework shown in Figure 7. PC 1 is connected to one of Gigabit Ethernet interfaces of Network processing unit 1, while PC 2 is connected to Master control unit using telnet to manipulate the operation in the router. Manual SA was also adopted in this test. Testing flow is the same as in Figure 6, excluding the program PC 2 ran in Figure 6 was ran in Master control unit in Figure 7. To validate the correctness of the decryption result by IPsec software, SP and SA that need decryption from PC 1 to the router were added. Packet was first encrypted in PC1 and sent out, and then transferred to Master control unit through slow path by Network processing unit 1. Receiving the packet, Master control unit called IPsec incoming processing module to decrypt the packet and the decrypted packet was received by the receiving program ran in Master control unit, in which we stored the original file in advance to execute comparison. To validate the correctness of the encryption, SP and SA from the router to PC 1 need encryption were added. The packet sent by sending program, which ran in Master control unit, was firstly encrypted by IPsec outgoing processing module in kernel, then sent to Network processing unit 1 through slow path, and finally received by PC 1, in which the original file was saved and encrypted in advance for comparison. The speed of implementing IPsec with software is much slower than implementing IPsec with Encryption chip. Yet data passing through slow path are non-real time tasks, IPsec software is capable of processing these traffic.

Table 1: Statistical data of 1024-byte packets encrypted with 256-bit AES key



```
☐ Enable short-term statistics

These values are based off of statistics accumulated since the start of the Analyzer run.    % Max bandwidth:    99.00

Test substream counts and rates
        Total packets:        7,160,472,811  packets        Total packet rate:        272,542  packets/s
    Total packet bytes:   7,790,594,418,368  bytes      Total packet bit rate:  2,372,206.389  Kbits/s
         Good packets:                    9  packets         Good packet rate:              0  packets/s
    Good packet bytes:                9,792  bytes       Good packet bit rate:          0.003  Kbits/s

    Packet fragments:   ○
```

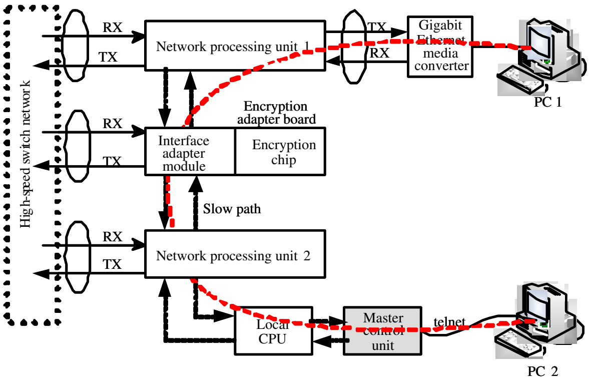


Figure 7: Framework of testing IPsec software

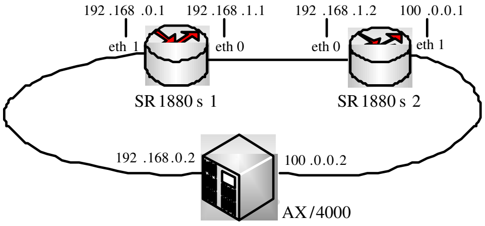


Figure 8: Architecture of speed testing

3) Testing results using tester:
Figure 8 shows the testing architecture using Adtech Ax/4000. AX/4000 was connected to 2.5G POS of two SR1880s, respectively. SP and SA are added manually to make the test convenient. Data flows are followed as this. Packets sent out by AX/4000 were first encrypted by SR1880s 1, then encrypted by SR1880s 2, and finally received by AX/4000. Table 1 shows the statistical data of receiving 1024-byte-long IPv4 packets processed by 256-bit AES key in AX/4000. The figure explains that the speed can up to 2.372Gb/s. Although the processing speed descends slightly with diverse length packets and diverse length keys, the speed can satisfy the network need.

5 Conclusion

We present universal security architecture of implementing IPsec with both encryption chip and IPsec software to fully utilize the advantages of fast path and slow path of broadband router. High-speed Encryption chip is utilized to achieve wire-speed encryption and decryption in fast path, while IPsec software is used to process non-real time data passing through slow path. These two parts working together process the traffic that needs to be protected efficiently. At the same time, implementing this security architecture needs not to change the original hardware architecture of the router, which makes the architecture universal. Additionally, only traffic needing to be protected is forwarded to encryption chip through adoption of Encryption adapter board, which saves processing time. We implemented this scheme in SR1880s and made comprehensive testing. The testing results show that the proposed schemes can protect the traffic passing through the router, and satisfy the security needs of broadband router.

References

[1] L. H. Chang, C. L. Lo, J. J. Lo, W. T. Liu, and C. C. Yang, “Mobility management with distributed AAA architecture,” *International Journal of Network Security*, vol. 4, no. 3, pp. 241-247, 2007.

[2] C. W. Chen, M. C. Chuang, and C. S. Tsai, “An efficient authentication scheme between MANET and WLAN on IPv6 based Internet,” *International Journal of Network Security*, vol. 1, no. 1, pp. 14-23, 2005.

[3] X. Gu, Y. Li, J. Yang, and J. Lan, “Hardware-and-Software-based Security architecture for broadband router,” *International Conference on Information and Communications Security*, pp. 546-555, Raleigh, U.S., 2006.

[4] Hifn, *FlowThrough Security for Gigabit Ethernet*, White paper, Oct. 2006.

[5] R. Jiang, A. Hu, and J. Li, “Formal protocol design of ESIKE based on authentication tests,” *International*

Journal of Network Security, vol. 6, no. 3, pp. 246-254, 2008.

[6] C. Kaufman, *Internet Key Exchange (IKEv2) Protocol*, IETF RFC 4306, Dec. 2005.

[7] S. Kent, and K. Seo, *Security Architecture for the Internet Protocol*, IETF 4301, Dec. 2005.

[8] S. Keshav, and R. Sharma, "Issues and trends in router design," *IEEE Communications Magazines*, vol. 36, no. 5, pp. 144-151, May 1998.

[9] J. Li, P. Zhang, and S. Sampalli, "Improved security mechanism for mobile IPv6," *International Journal of Network Security*, vol. 6, no. 3, pp. 291-300, 2008.

[10] NetOctave, *About the NetOctave FlowThrough Security Architecture*, NetOctave NSP4200 Security Processor, 2002.

Xiaozhuo Gu received her BS, MS from Lanzhou University, China, in 1999 and 2003, respectively. She is currently a PhD student in the department of Broad-band network R&D of the National Digital Switching System Engineering & Technological R&D Center, China. She is a research associate in the design of trusted network architecture in next generation network. Her research interests include network security, group communication, and distributed systems.

Jianzu Yang received his BS, MS from Information Engineering University, China, in 1999 and 2006, respectively. He is currently a research assistant on faculty of department of communication engineering at the University of Information Engineering, Zhengzhou. His research interests include network security, wireless communication, and signal processing.