IPSec Implementation and Management Methods

James H. Wiebe
Master's student, ECE Dept., University of Windsor, Windsor, ON N9B 3P4
wiebe7@uwindsor.ca

***Abstract*—An overview of security systems for IPSec implementation and its management, including the concept of layered functional architecture, which is paramount in network management, is discussed. It is shown that the state of the art in the literature contemplates systematic approaches to IPSec. When IPSec functionality is implemented in vertical functional layers, it provides strong security that can be applied to all traffic crossing the perimeter. A number of proposed structured IPSec management architectures and off-the-shelf implementations are investigated. Software, ASIC and FPGA implementations are overviewed. Finally, an application of IPSec to wireless security is discussed.**

***Index Terms*—IPSec, Network management, Cryptographic implementations**

I. INTRODUCTION

THE state of the art in IPSec (Secure Internet Protocol) implementations has progressed well since 1994, when the need for a relatively low-level and transparent security service was first formally identified. This made IPSec an afterthought to IPv4, unfortunately, although it is a required part of any IPv6 implementation. IPSec is a complex standard for encrypting internet communications at the packet or network level; it can authenticate and/or encrypt packet contents, without or with including the level 3 (IP) packet header. It also has an anti-replay service. Authentication is referred to as AH (Authentication Header) and encryption (confidentiality), is referred to as ESP (Encapsulating Security Protocol). Including the IP header in the above security services, is referred to as Tunnel Mode; not including the header, is referred to as Transport Mode.

II. ACADEMIC RESEARCH

A. Design Framework Proposals

Ref. [1] has pointed out the paradigm of low-level to high-level interactions and that at each level, the needs of technology, the organization and government mandates must be taken into account. The security of E-business should be designed along with the E-business and not added-in as an afterthought.

Ref. [2] has proposed a three-level architecture for security management for distributed multimedia services, arranged in three layers: service, middleware and network. Note that functionality at any level requires implementation at its level and at all lower levels; for example the policy rules need handling here at the Middleware level as well as the Network level.

Ref. [3] has proposed "C-ISCAP" (Controlled Internet Secure Connectivity Assurance Platform), which is an internet information security system based on IPSec (Fig. 1). Here, ISE stands for "Internet Security Evaluation System", which evaluates system safety and attempts to proactively identify threats. SEPS (or SPES) is the security policy database, SEMS is the Security Management System, "AUTOKEM" is the automatic key exchange mechanism, using a CA (Certificate Authority) to prevent "Man In The Middle" attacks, UKEM is the "Universal Key Management System", SPDB is the Security Policy Database, SADB is the Security Association Database and "UGINE" is the "Universal IPsec Engine".

A design at the Mechanisms and Primitives level (see Section IV) was provided in [4] in proposing a multi-accelerator. Each accelerator was provided with its own work queue, and a scheduler distributed the work among the accelerators and the CPU. A scheduling algorithm was developed that controlled this distribution of IPSec packet processing. Soft QoS (Quality of Service) could be supported in that higher-priority bit streams would be provided with a higher-priority access to the scheduler.

Ref. [5] proposed a system of policy distribution using a four-layer architecture of management, processing, consumer and target, with the policy database serving the upper three layers. A policy server defines, stores, and configures policies

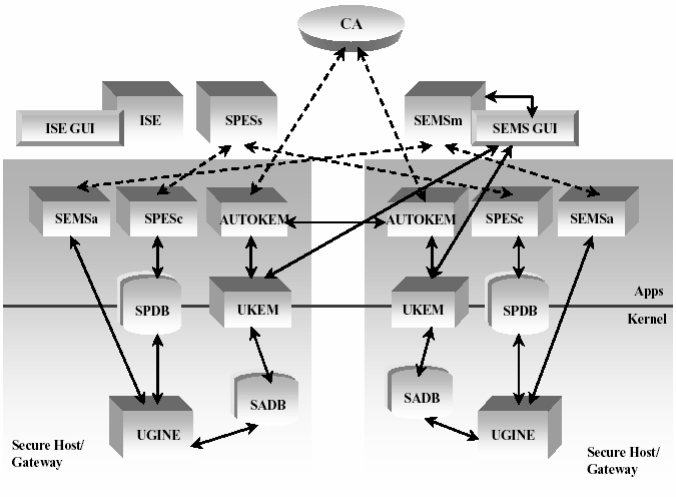

Fig. 1. C-ISCAP ([3] Fig. 1. Reproduced with kind permission of Springer Science and Business Media)

for the ultimate target systems and the policies are distributed to the targets using IETF standard protocols. The usefulness of this can be appreciated if a large company has hundreds of IPSec installations to be configured throughout a large region.

As can be seen from the foregoing, the state of the art in the literature contemplates some systematic approaches to IPSec. What seems to be needed here is a unifying paradigm.

B. *Software Implementations*

It was found in [6] that the Free S/WAN implementation incurred greater performance degradation than 802.1X due to its end-to-end security with double authentication, a stronger encryption method as well as better key management and tunneling. One result was that in using DES for FTP, degradation of performance was worse than the degradation for HTTP in going from 802.1X to Free S/WAN [6].

In [7], a software implementation of IPSec was done on Linux and several different versions of BSD (Berkeley Software Distribution – of Unix). It was found that encryption of packets was "a major bottleneck", resulting in a factor of ten decrease in throughput in a ping performance test. Authenticating packets caused no significant decrease in throughput in this test. A factor of ten decrease in throughput using ESP (Encapsulating Security Protocol) is evident, and in these tests, the use of AH (Authentication Header) did make significant differences in throughput, reducing throughput by 30% and 50% in UDP transfer and 50% and 60% in TCP for MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm), respectively.

C. *Hardware Implementations*

The heavy overhead incurred by encryption mandates hardware acceleration. Software running on a general-purpose processor can typically produce AES (Advanced Encryption Standard), i.e., Rijndael, throughputs of low tens of Mbps (i.e., 30) [8]. FPGAs (Field-Programmable Gate Arrays) can achieve up to 176 Mbits/s implementing DES (Data Encryption Standard) and up to 964 Mbits/s implementing AES [9]. An ASIC (Application-Specific Integrated Circuit) processor achieved 2.29 Gbits/s of AES throughput in a 0.18µm CMOS standard-cell technology in 2002 [10]. FPGAs offer lower non-recurring engineering costs but higher per-unit costs, suitable for small sales volumes. It is believed that FPGAs will occupy a niche at the low end, below custom chips and ASICs, with volumes up to the 30- to 60-thousands. FPGAs can offer a feature as great as dynamic reconfiguration in addition to off-line reconfiguration. Unused encryption schemes can be compressed for storage [8]. Field upgrades for such things as bug fixes and new standards are possible, even using pin-compatible devices [11].

III. OFF-THE-SHELF IMPLEMENTATIONS

Table 1. presents a survey of several key off-the-shelf IPSec implementations from industry. It is notable that the overriding concern in industry is getting a usefully working device ready on time, i.e., extremely quickly, and there is little patience with complicated standards. For example, the implementers of AT&T Moat [19] discarded IKE in favor of transmitting configuration details via SSH (Secure SHell) and using Linux shell scripts to configure the SADBs (Security Association Databases).

Throughput figures are difficult to obtain, since throughput is greatly system-dependent, especially when software implementations are under test. The network environment can also affect results. Industry is reluctant to publish concrete technical data to avoid competitive technical analysis; the scope of our investigation is limited to published data. Factors of ten to a hundred of speed-up occur when hardware acceleration is used.

IV. VERTICAL LAYERING

The IPSec RFCs (Requests For Comment) [21] are quite complex; a consequence of the committee process that was used [22]. Specific methods of implementation are left completely open, as RFCs always do. It is a formidable task to implement IPSec securely, and implementing even a clearly-specified security standard incorrectly can cause loopholes that allow an attacker to bypass the security. It is proposed to structure a security system into five vertical functional layers: Primitives, Mechanisms, Services, Management and Policies (Fig. 2.). Using this approach reduces the design problem to an exercise in "connecting the dots", thus preventing oversights; when IPSec functionality is implemented in this way, it provides strong security that can be applied to all traffic crossing the perimeter [23].

Modules in the Policy layer include: Prevention and detection of IPSec security violations, Network-wide IPSec implementation policy, and Disaster recovery. Modules in the Management layer include: Policy control and management of security services, Event logging, IPSec services monitoring, User interface, Interoperability and Recovery and backup. Modules in the Services layer include: Integrity, Authentication, Confidentiality, and Anti-replay. Modules in the Mechanisms layer include Encryption, Message authentication, Key management, and Certificates and Digital signatures. Finally, modules at the Primitives layer include

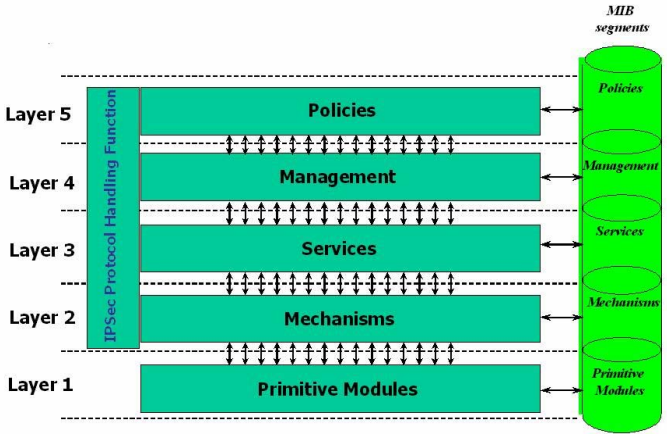

Fig. 2. Five-layer framework for IPSec.

TABLE I – OFF-THE-SHELF IPSEC IMPLEMENTATIONS

Implementation or platform(s)	HW/SW or combinations	Standards / RFCs Supported	Policy / Management	Other Features / Capabilities	Speeds: Throughput, other speeds.
Lucent: Firewall, Management System and Client [12]	Combination; accel. for MD5, SHA-1, DES and 3DES; BITS	Firewall supports FTP and H.323. IEEE 802.1Q (VLAN) tags, RFCs 2085, 2104, 2315, 2393, 2395, 2401-2406, 2437, 2451, 2898, 2986, PKCS 1, 3, 5, 7, 8, 10.	LSMS (Lucent Security Management System) – divisibility.	Logging, alarms (loss of comm., performance degradation), Accounting, DDoS-hardening	One LSMS is fast enough to support 1,000 devices and up to 20,000 active IPSec clients. Firewall rated at 1 Gbps clear-text throughput.
Nortel Services Edge Router 5500 [13]	SW, BITS, HW accel.	1655, 1771, 1828, 1829, 2328, 2385, 2401, 2403, 2404- 2409, 2702, 2858, 3031, 3032, 3036, 3037, 3209, 3270, 3602, 3664, 3630, 3702	RFC 2764-based ("A Framework for IP Based Virtual Private Networks")	Flow and Class -based accounting. Services event logging and accounting	375 Mbps 3DES, 450 Mbps AES (Services Edge Router 5500)
Cisco IOS (Internetwork Operating System) [14]	Combination; accel. - ESA – public key math and RNG; BITS	IKE, DES (explicit IV) RFCs 1994, 2138, 2401-2411, 2451	Policy entry via command line.	Nesting of IPSec traffic to multiple peers	Up to 2 Gbps 3DES IPSec VPN with up to 8000 tunnels. (Catalyst 6506)
IBM [15], z/OS, releases 1.4, 1.5, 1.6, and 1.7, running on System z9 and zSeries servers.	SW, BITS, coprocessors	3947, 3948, 2401-2410, 2451	Yes	Logging	3DES: 3,143 kbps (SW), 5,159 kbps (HW - IBM 4758-2 Cryptographic Coprocessor PCI card)
WindRiver WindNet [16]	SW, BITS, HW accel. interface.	2401-2404, 2406-2410, 2451	API (Application Programming Interface) to set up SAs manually, only. MKM (Manual Key Manager)	Cryptographic Provider interface - support for the complete line of Motorola security processors.	Figures not supplied.
Microsoft Windows XP, 2003, 2000 [17]	SW, BITS	Not AES yet. RFCs 2401- 2409.	Policy Management. SAs viewable.	DoS counter: SAs limited. Oakley logging and IKE monitoring	Max. of 19.4 SAs/sec. est. (993 MHz PC)
Solaris [18] OS 8 and later (to 10)	SW, BITS. HW accel.	2401, 2402, 2406, 2409, 2412	Policy table configuration	None found.	800 Mbps (3DES – Sun Crypto Accelerator 4000 TM)
AT&T Moat [19]	SW – Free S/WAN [20]; BITW	Free S/WAN complete set – scalability features added – tunnels can be dynamically configured.	A simple database lists all the moat customers – Shell scripts do configuration.	SSH used instead of IKE and both sides configure their own SAs.	6.9 Mbps

3DES = Triple DES, accel. = accelerator, AES = Advanced Encryption Standard, BITS = Bump In The Stack, BITW = Bump In The Wire, bps = bits per second, DDoS = Distributed DoS, DES = Data Encryption Standard, DoS = Denial Of Service, ESA = Encryption Service Adapter, FTP = File Transfer Protocol, IKE = Internet Key Exchange, IP = Internet Protocol, IPSec = Secure IP, IV = Initialization Vector, MD = Message Digest (a cryptographic hash), PCI = Peripheral Component Interconnect, RFC = Request For Comment, RNG = Random Number Generator, SA = Security Association, SHA = Secure Hash Algorithm, SSH = Secure Shell (application), S/WAN = Secure Wide-Area Network, VLAN = Virtual Local Area Network, VPN = Virtual Private Network.

Prime number generation, Modular arithmetic, Encryption and Hashing [23]. There is no formal access control module in IPSec, contributing to availability problems; neither is there a formal availability control module, and moreover the defacto availability protection is weak in IKE.

A. Availability Problems in IKE

There are severe availability problems associated with IKE, the protocol used to establish SAs (Security Associations) between peers.

The Key Exchange protocol is rather susceptible to a Denial of Service attack due to the acceptance of Diffie-Hellman (DH) values; the initiator (or client) can have the responder (or server) doing modular exponentiation for nothing. Even though cookies are used, a Distributed Denial of Service (DDoS) attack is a threat ([24] pg. 3, RFC 2522 pg. 18).

Aggressive Mode eliminates the cookie exchange entirely, making it even more non-recommended for use. It doesn't provide identity protection, but it is intended for mobile users, who most need that, due to the ease of eavesdropping on wireless links ([24] pg. 5). Quick Mode opens the door to a DoS-Replay attack in which an attacker simply replays the Quick Mode packets and the responder uses all of its resources decrypting the packets only to find that the nonces used are the same ([24] pg. 6).

Several papers provided suggestions to improve key exchange by suggesting new and different protocols.

Ref. [25] suggested a pair of protocols, called JFKi and JFKr, for "Just Fast Keying", "initiator" and "responder", respectively; the former was designed to provide identity protection for the initiator in the key exchange and the latter to provide it for the responder. These protocols combat DoS attacks against the responder by not requiring

the responder to perform modular computation until the initiator has first done so, and established round-trip communication.

Another proposal ([26] pg. 329), involves "client puzzles" in which the server requires a client to solve a puzzle before the responder will create state or do its own computations. The server sends a hash containing its nonce, along with a partial solution to the hash. The client has to find the nonce and return it before the server will authenticate it, while the server only has to store the nonce for each client. The client's workload increases rapidly with the number of requests it makes, whereas storage and work at the server increases slowly ([27] pg. 7). The server can vary the difficulty of its puzzles in relation to its load.

It is hoped that the debate process within the IETF will adopt these and/or other suggestions for improving the present easily-attackable state of IKE/ISAKMP.

V. Applications

IPSec, being a lower-level protocol, is useful in many situations, such as securing wireless communications, a technology that has been notorious for using a weak security standard.

Ref. [28] used IPSec to secure a wireless gateway. The Microsoft Windows 2000 implementation of IPSec was used. Throughput was 604 kBps (Bytes per sec.) unencrypted, 458 kBps using 40-bit WEP, 355 kBps using IPSec with DES and MD5 and 209 kBps using IPSec with 3DES and SHA. This is credible in terms of the roughly 30 Mbps maximum throughput possible using software implementations of IPSec.

Acknowledgments

J. H. Wiebe thanks his advisor, Dr. S. Erfani, for his advice and encouragement, and his fellow student, N. Bayan, MASc, for assistance with publication.

References

[1] D. Trček, "An Integral Framework for Information Systems Security Management," *Computers & Security*, May 2003, Vol. 22, No. 4, Elsevier Ltd., pp.337-360.

[2] S. Duflos, B. Kervella, and E. Horlait, "An Architecture for Policy-based Security Management for Distributed Multimedia Services," *Proc. of the Tenth ACM Int'l Conf. on Multimedia*, Dec. 2002, ACM, pp. 653-655.

[3] W. Park, J. Nah, and S. Sohn, "A Study of Security Association Management Oriented to IP Security," *Lecture Notes in Computer Science*, 2002, Vol. 2344, Springer-Verlag GmbH, pp. 381-388.

[4] A. Ferrante, V. Piuri, and F. Castanier, "A QoS-enabled Packet Scheduling Algorithm for IPSec Multi-Accelerator Based Systems," *Proc. of the 2nd Conf. on Computing Frontiers*, May 2005, ACM, pp. 221-229.

[5] M. Li, "Policy-Based IPsec Management," *IEEE Network*, Nov/Dec 2003, IEEE, pp. 36-43.

[6] D. Nayak, D. Phatak, and V. Gulati, "Modeling and Evaluation of Security Architecture for Wireless Local Area Networks by Indexing Method: A Novel Approach," *Lecture Notes in Computer Science*, Vol. 3439, 2005, Springer-Verlag GmbH, pp. 25-35.

[7] A. Keromytis, J. Ioannidis, and J. Smith, "Implementing IPsec," *Global Telecom. Conf.*, Nov. 1997, Vol. 3, IEEE, pp.1948-1952.

[8] A. Dandalis, V. Prasanna, and J. Rolim, "An Adaptive Cryptographic Engine for IPSec Architectures," *2000 IEEE Symp. on Field-Programmable Custom Computing Machines*, 17-19 April, 2000 pp.132-141.

[9] T. Wollinger, J. Guajardo, and C. Paar, "Security on FPGAs: State-of-the-Art Implementations and Attacks," *ACM Trans. on Embedded Computing Systems*, Aug 2004, Vol. 3, No. 3, pp. 534-574.

[10] P. Schaumont, H. Kuo, and I. Verbauwhede, "Unlocking the Design Secrets of a 2.29 Gb/s Rijndael Processor," *Proc. of the 39th Conf. on Design Auto.*, Jun 10-14, 2002.

[11] O. Cheung, and P. Leong, "Implementation of an FPGA Based Accelerator for Virtual Private Networks," *Proc., 2002 IEEE Int'l Conf. on Field-Programmable Tech.*, 16-18 Dec., 2002, pp. 34-41.

[12] N. Raghavan, R. Gopal, S. Annaluru, S. Kura, "Virtual Private Networks and Their Role in e-Business," Bell Labs Technical Journal, Vol. 6 No. 2, 2002, pp. 99-115.

[13] Nortel, Nortel Services Edge Router. (2006). Available: http://www.nortel.com.

[14] Cisco, (2006), "Cisco Catalyst 6500 Series Security and IPSec VPN Systems". Available: http://www.cisco.com.

[15] IBM, (2006), z/OS IPSec. Available: http://www.ibm.com.

[16] WindRiver, WindNet, (2006), "WindNet IPSec and IKE". Available: http://www.windriver.com/products/device_technologies/middleware/windnet_ipsec/windnet_ipsec.pdf.

[17] Microsoft, (2006), IPSec, Available: http://www.microsoft.com/technet/itsolutions/network/ipsec/default.mspx.

[18] Sun, Solaris, (2006), IPSec, Available: http://www.sun.com.

[19] J.S. Denker, S.M. Bellovin, H. Daniel, N.L. Mintz, T. Killian, and M.A. Plotnick, "[AT&T] Moat: a virtual private network appliance and services platform," *Proc. of the 13th Large Installation System Administration Conference (LISA '99)*, November 7-12, 1999, Seattle, Washington, USA. pp. 251-260. Available: http://www.usenix.org/events/lisa99/full_papers/denker/denker_html

[20] Free S/WAN project. Available: http://www.freeswan.org/.

[21] IETF, RFCs (Requests For Comment). Available: http://www.ietf.org/rfc/rfcNNNN.txt, where NNNN is the RFC number.

[22] N. Ferguson, and B. Schneier, "A Cryptographic Evaluation of IPSec," Counterpane Internet Security Inc., San Jose, CA, 1999. Available: http://www.schneier.com/paper-ipsec.pdf.

[23] M. Fahandezh, "A Framework for IPSec Functional Architecture," MASc Thesis, ECE, Faculty of Grad. Studies and Research, U. Windsor, 2005.

[24] W. Simpson, "IKE/ISAKMP considered harmful," USENIX, 1999. Available: http://www.usenix.org/publications/login/1999-12/features/harmful.html.

[25] W. Aiello, S. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A. Keromytis, and O. Reingold, "Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols," *Proc. of the 9th ACM Conf. on Computer and Communications Security*, Nov. 2002, pp. 48-58.

[26] M. Choi, D. Kwak, and S. Moon, "A Proposal for DoS-Defensive Internet Key Exchange," *Lecture Notes in Computer Science*, Vol. 2668, 2003, Springer-Verlag GmbH, pp. 328-337.

[27] J. Leiwo, T. Aura, and P. Nikander, "Towards Network Denial of Service Resistant Protocols," *Proc. of the 15th Int'l Information Security Conf. (IFIP/SEC 2000)*, Beijing, China, August 2000.

[28] A. Godber, and P. Dasgupta, "Secure wireless gateway," *Proc. of the 3rd ACM workshop on Wireless security*, Sept. 2002, ACM, pp. 41-46.