Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 78 (2000)

Heft: 7-8

Artikel: IPsec VPN : theory and practice

Autor: Ferchichi, Azim

DOI: https://doi.org/10.5169/seals-876460

Exploration Programmes:
Corporate Technology Explores Future Telecommunications

IPsec VPN: Theory and Practice

To meet the growing needs in IP security the IETF community has defined the so-called IPsec standard (IPsec stands for IP security). From theory to practice, this article presents the differences between the intended standard and real-world implementations.

The Exploration Programme Cards & Security
- provides an environment to evaluate, integrate and demonstrate new security technologies and concepts
- contributes to the definition of network and service protection levels by working on scenarios considering the evolution of the threats that Swisscom will be faced with in future
- proposes smart card based solutions to address the security problems arising in a world of short distance wireless communication
- assesses established and emerging biometrics technologies and their impact on Swisscom's business

With its Exploration Programmes, Corporate Technology is exploring telecommunication technologies and new service possibilities with a long-term view of 2–5 years. Further, the expertise built up in the course of this activity enables active support of business innovation projects.

Today, more and more business telecommunication services are deployed across public IP networks like the Internet. On one hand, using public or third party network infrastructure is cost saving, but on the other hand valuable data may be compromised by malicious persons. Likewise, many network operators (even competitors) are interconnecting their networks for better coverage at relative low cost, thereby, however, introducing new security risks.

AZIM FERCHICHI, BERN

Before deploying a VPN using IPsec, critical factors must be carefully addressed such as the VPN network topology and its size, the type of traffic and applications transiting on the VPN, or the legacy system already in place.

This article first describes the basic technology components of IPsec, the standard defined by the IETF community to meet the IP security needs, with a survey of the different security services and explains the limitations and potential flaws. Then it focuses on different possible VPN (Virtual Private Network) scenarios and addresses the main issues that might arise from the interaction between IPsec and other networking technologies. Finally, step-by-step guidelines are described to help deploying an IPsec VPN.

Definitions

We first give a definition of some VPN-related terms:

VPN

A Virtual Private Network is a *logical* network that shares physical resources with other networks giving the impression to users or processes to be inside one *physical* network. When a computer of the VPN communicates with another computer of the same VPN, the underlying shared resources and the interconnection complexity are hidden by the VPN. In its broadest meaning the term "private" may refer to a separate addressing scheme, a simple clear-text tunnelling, or a strong encrypted tunnelling. Frame relay networks, MPLS networks, Dial-up networks and IPsec networks are all examples of VPNs.

Secure VPN

A secure VPN offers a defined set of security services, such as peer authentication, data privacy (or confidentiality), data integrity, secure key management etc. An explanation of basic security services is given in fig. 1.

IPsec VPN

An IPsec VPN is a secure VPN where the security services, functions and algorithms are implemented in compliance with the IPsec standard defined by the IETF.

Basic Description of the IPsec Standard

IPsec is organised to protect the IP packets using two security services: the Authentication Header (AH) service and the Encapsulation Security Payload (ESP) service. In addition, it provides the Internet Key Exchange (IKE) protocol for secure key management and distribution.
AH provides connectionless integrity, data origin authentication using symmet-

Authentication: A security mechanism (or service) that provides the assurance of the identity of the claimed entity

Data origin authentication: A security mechanism (or service) that provides the assurance that the data are really issued from the claimed entity

Integrity of data: A security mechanism (or service) that ensures that any modification to the data are detectable

Confidentiality (or privacy) of data: A security mechanism (or service) that provides the assurance that no data can be read or interpreted by unauthorised entities

Signature (or digital signature): A security tag or mark being used to validate the origin authentication and/or the integrity of the data it is associated with

Secret key algorithm (or symmetric algorithm): A cryptographic function using the same key to encrypt and decrypt the data

Public key algorithm (or asymmetric algorithm): A cryptographic function using a pair of related keys, one being public, the other remaining secret; each key can decrypt what the other encrypts; the authenticity of the public key may be guaranteed by a certificate

Certificate: An electronic document certifying that a public key really belongs to the identity of the entity; Certificates are issued by a so-called Certification Authority (CA)

Fig. 1. Security fundamentals.

ric cryptographic algorithms, and replay protection thanks to a digital signature over a sequence number. It can work in tunnelling or transport mode. For more details concerning AH please consult [1]. Fig. 2 describes the IP packet before and after applying AH.
ESP provides data privacy (or confidentiality) using symmetric cryptographic algorithms, plus all AH security services. For more details concerning ESP please consult [2]. Fig. 2 describes the IP packet before and after applying ESP.
Note that ESP service can be used with null encryption. In this case ESP provides the same security services as AH does and one may wonder why AH exists altogether. In fact there is a subtle difference which occurs only if tunnel mode is selected. In AH tunnel mode the new IP header is included in the authentication calculation, but not in the ESP authentication calculation. However, this has no security implications and does not explain the redundancy between the two services.
IKE describes a framework in which IPsec connections can negotiate authentication, encryption and key management information. It provides key provisioning for AH and/or ESP. For a complete description of IKE please consult [3].
While AH and ESP are quite easy to understand, IKE is complicated. It is divided in two phases: the Main Mode and the Quick Mode (fig. 3). In the Main Mode, an authentication of the IPsec peer entities is made and an IKE Security Association (IKE SA) is defined. IKE SA contains all necessary information for two IPsec entities to secure Quick Mode communication. In Quick Mode, IPsec Security Associations (IPsec SA) are defined in order to provide security information to be used by the AH or ESP service. The content of IPsec SA includes the cryptographic keys and their lifetimes, the selected algorithms, and the source and destination IP address of incoming IP packets on which AH or ESP must be applied.

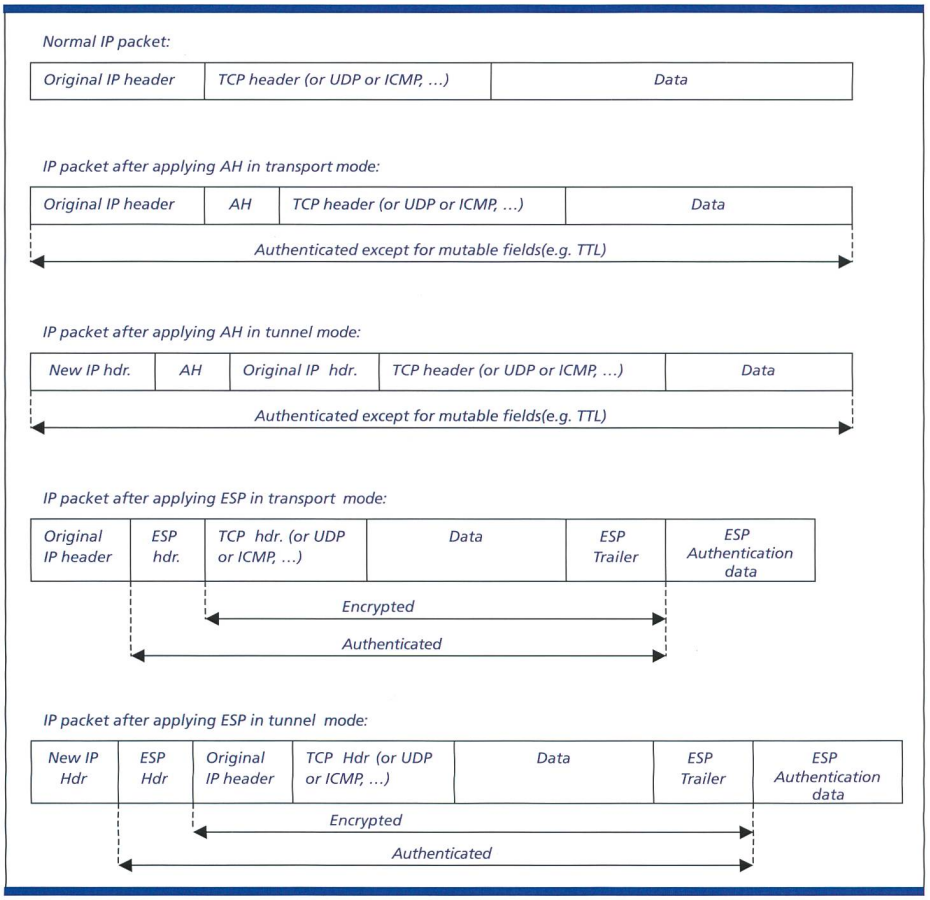

Fig. 2. IP packet with Authentication Header (AH) or Encapsulation Security Payload (ESP) applied.

What is not defined in IPsec

One big imperfection of IPsec is the management. Today no RFC exists that specifies protocols or policies for IPsec management. Therefore, each product tends to have its own management with its own proprietary protocols and policy. The result is that different IPsec VPN products can not be managed the same way with the same management application.
Another issue with IPsec is the Public Key Infrastructure (PKI) integration. For the authentication of IPsec peer entities in IKE, public key algorithms may be used (e.g. DSS, RSA signature etc.). For this, a PKI environment must be defined for the issuance, download and management of certificates. However, there is no RFC that specifies clearly how to integrate a PKI environment within IPsec. In [4], a framework to adapt PKI to the IP world is described. Even if it is stated that PKIX should be used for IPsec, this RFC is not of much help for PKI deployment and integration within an IPsec VPN.
IPsec does not define any VPN-ID included in the ESP or AH header. This would be very useful for management purposes and it could provide an easy means for IPsec entities to distinguish between different types of VPNs with different characteristics (i.e. to accept/reject packets based on their VPN-ID).
Last but not least, IPsec makes no security recommendation. Many security methods or algorithms are possible, as well as key lengths. Furthermore, several interdependencies exist between cryptographic keys (e.g. keys derived from other keys, keys protected by other keys etc.). However, very few statements and no rationale are made to prescribe algorithms and key lengths for a certain security level. If the user has not enough cryptographic knowledge, he might get lost in the cryptographic configuration of his IPsec VPN, and may introduce inconsistencies or weaknesses in the choice of key lengths and key lifetimes. We recommend to refer to [5] and [6] to try to make a good choice of algorithms, key lengths and lifetimes.

IPsec VPN Scenarios

Theoretically, IPsec can be installed on any device that runs a TCP/IP stack, making it possible to have IPsec VPNs with lots of heterogeneous machines. However, most common IPsec VPN deployments are Intranet VPN and Remote Access VPN.

Intranet VPN

Intranet VPN interconnects networks owned by a single company or a single organisational unit (fig. 4). A VPN gate-

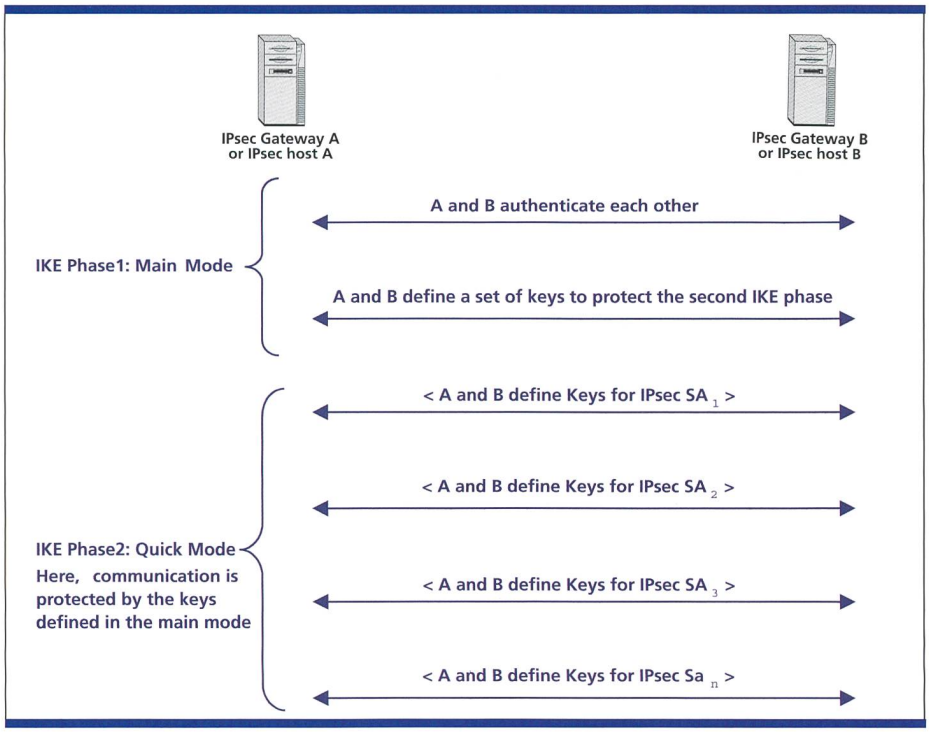

Fig. 3. Internet Key Protocol (IKE) basic description.

way is attached to each site that decrypts incoming traffic and encrypts outgoing traffic. This is the simplest scenario.

Remote Access VPN

Remote Access VPN is suited for mobile users making a dial-in connection to their company's network either directly or through an ISP (Internet Service Provider). Especially in the second case it can be worthwhile to secure the traffic as it crosses Internet. An IPsec software stack is installed on each laptop of mobile users securing the connection up to the IPsec gateway of their company's home network.

Extranet VPN

A new emerging type of VPN is the so-called Extranet VPN. In this scenario, two or more companies have networked access to a limited amount of each other's corporate data. This is a growing need as more and more companies are merging, because it's one of the fastest and less costly ways to interconnect their networks. It may also be a need for joint projects between companies and for companies which have a strong customer-supplier relationship for optimised order and delivery processes. Unlike for Intranet VPN, Extranet VPN assumes a different network and security policy for each interconnected site. This implies that IPsec security services are not sufficient. In addition, the gateway must implement firewall functionality, access list functionality, an application gateway, or any similar tool capable of applying a selection to the transiting traffic. NAT (Network Address Translation) is also generally needed, as conflicts may occur if different companies have overlapping private addressing.

Another possibility is to have a VPN connecting hosts or servers spread over different networks. An example is a distributed database containing sensitive information implemented on several hosts, each one located in a different network. Finally, we can have VPNs mixing all the types we have described above, creating more complex VPN structures (fig. 5).

Platform for IPsec

When IPsec is implemented on end-hosts, up to now it is always a software implementation. This software can be part of the native stack, i.e. directly provided by the OS vendor and integrated in their bundled IP stack. Another possibility is a replacement stack. A third party vendor may write an entire drop-in replacement for the original stack. It is, however, difficult to reproduce the full compatibility with the native OS especially after new OS releases or updates. The most widespread approach is the bump in the stack. Third party vendors insert their IPsec software into the native IP stack by writing to a known API provided by the OS.

When IPsec is implemented on a gateway dedicated to protect a network, different platforms are possible:

- The gateway maybe a computer machine (e.g. a Sun Sparc workstation, or an NT station) with 2 Ethernet cards. The machine has its native operating system running (e.g. Solaris 8, NT 4.0 etc.), on which the IPsec software is installed.
- An another possibility is a dedicated hardware box. Generally it contains special cryptographic processors for fast cryptographic calculations and proprietary OS with more security and very few functionality.
- Finally, the gateway may be a router or a firewall on which an IPsec module has been added.

IPsec and other IP based Services

The two main ugly outcomes of IPsec are the delay introduced by the cryptographic processing and the fact that useful information may be hidden due to encryption.

Cryptographic calculation such as encryption, decryption and signature consume a lot of processing power which may degrade delay-sensitive applications. Triple DES (Data Encryption Standard), for example, requires about 50–100 times more processing power than straight IP routing. Furthermore, experience has proven that today's IPsec products are not optimal for many real-world Voice over IP (VoIP) installations.

Quality of Service (QoS) is also a problem with IPsec, especially if packets are encrypted and tunnelled. With QoS, information may be inserted in the header of the IP packet to be used by routers of the crossed networks. If QoS processing is made before the IPsec processing, the QoS information will be hidden to a router and become unusable. If QoS processing is made after IPsec processing, the QoS gateway will have no information about the original IP packet and will not be able to apply its QoS rules. The solution would be to have an integrated IPsec and QoS gateway able to apply IPsec services and QoS rules at the same time. However, such devices are not yet available on the market.

IPsec VPN Design Criteria

It is important to make a rough *risk analysis* before trying to implement an

IPsec VPN. Remember that IPsec is not easy neither in its conception nor in its practical implementation and the investment in terms of staff cost may be high (education of staff, operational cost etc.). Then a *network topology design* of your VPN must be addressed. It has to show where on the network you intend to put IPsec. You have also to define the type (Intranet, remote access etc.) and the number of VPNs (one flat VPN, two or more separated VPNs, a hierarchy of VPNs etc.) you need.

Once this is done, the *number of sites and hosts* to be interconnected has to be known. This is very important because it will largely influence the choice of your IPsec product. If the number is large (more than 50 machines), the application management is critical and must be well designed in order to easily manage a large volume of machines. In particular, if the same modifications or configuration parameters have to be applied to all machines then one user action should be sufficient. It also needs to have good auditing and alarm tools to help VPN administrators in detecting security problems. Apart from the management application problem, the number of machines will also influence the platform choice. It is better to choose a hardware platform solution in case of large deployment. Imagine you having a hundred machines where you have to harden the OS (i.e. strengthen the configuration of the OS, suppress all unnecessary default running services and apply security patches) and then install the IPsec software one by one: this is a repetitive, cumbersome and time consuming job. The number of machines will also permit you to put a requirement on the IPsec product concerning the maximum number of sessions (or IPsec SA) supported. For example, if you have 100 VPN gateways each protecting 10 machines and 10 subnets then the required number of IPsec SA that must be supported is $2 \times (10 + 10) \times (10 + 10) \times 99 = 79\,200$ sessions at the same time.

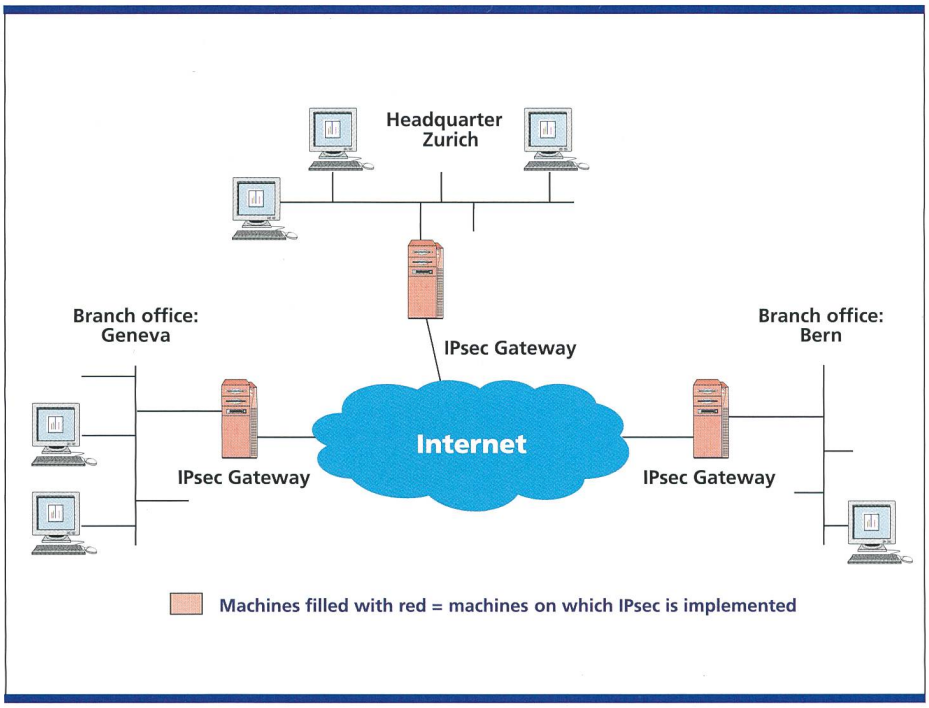

Fig. 4. Intranet IPsec VPN.

Traffic and application analysis is also very important. It permits to identify the shape of the traffic and to set performance requirements for the VPN (delay, throughput etc.). The type of application that will be used over the VPN shall be identified. As described above it appears that some applications do not fit well with IPsec VPN. Anyway, when performance is concerned, hardware-based VPN solutions provide a critical advantage. On the opposite, when data rates are low enough, for example 128 kbit/s or less, then software-based VPN products provide adequate throughput.

The next step is to make your *requirements for the PKI integration* within your IPsec product if you have chosen to use public key algorithms for the authentication of IPsec entities. You have also to establish a complete PKI policy. As this is a huge topic in itself, it will not be further developed here.

The last points before evaluating products are *legacy and inter-operability*. If the number of IPsec VPN elements is small, and if you already have machines where you might be supposed to implement IPsec, it might be worthwhile to look whether they support IPsec. For example, if you want to put few IPsec gateways just where you already have routers, then it could be a good idea to

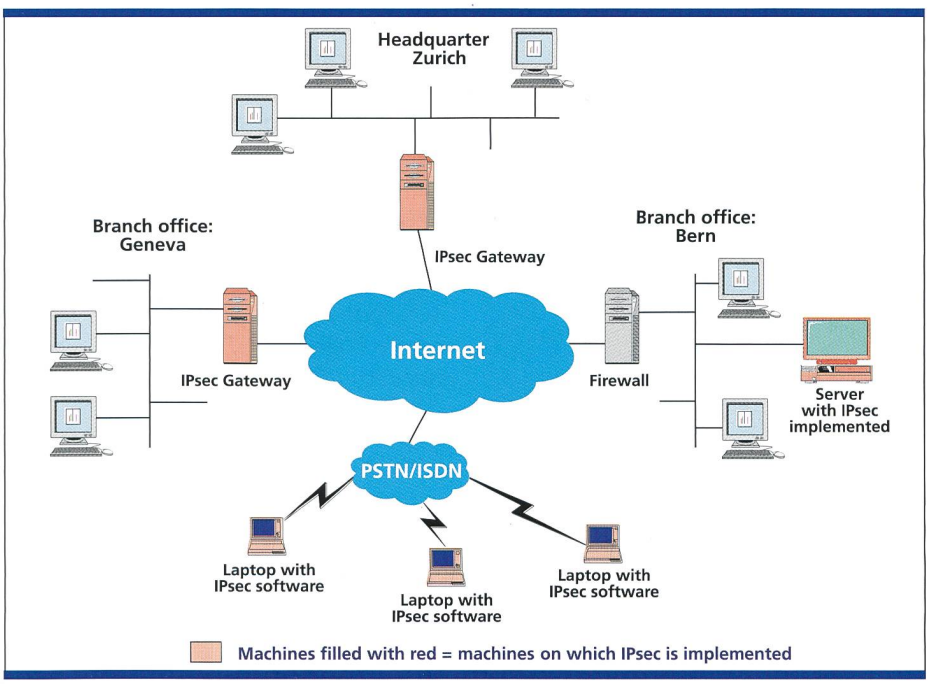

Fig. 5. Mixing different types of VPNs.

enhance the routers with IPsec functionality (e.g. Cisco have add-on IPsec modules for most of their routers). In the same way, you can add an IPsec module on your firewalls (e.g. Checkpoint have an add-on IPsec module for their Firewall-1 product). This has two benefits: first, it is a cheaper solution, and second, it may be managed the same way as the basis system (no need for the administrator to learn and get familiar with a new management tool). Inter-operability may be of concern if you have to connect your new VPN with an existing one. Remember, however, that you will have to manage them separately.
When all the above requirements have been addressed you can select few products to *evaluate and test*. Take time to test them in real-world conditions. Verify the claimed performance of the product by yourself if it's a critical factor for you. Play around with the management application to see potential problems and limitations. Take care of the initialisation and installation of the VPN, and try to calculate the time to set up and run a simple VPN with two machines.
Then extrapolate this time for your real deployment.
Once your choice has been made, you have *to establish processes and define resources* for the VPN installation and maintenance.
Finally, you can *launch and run* your VPN.

Conclusions

IPsec is the first standard offering a rather complete set of security services to protect VPNs at IP level. Beside the cryptographic complexity of the protocol, IPsec may be used for a wide range of IP VPNs like Intranet, Extranet, remote access VPNs or any combination of them. However, before deploying a VPN using IPsec, critical factors must be carefully addressed such as the VPN network topology and its size, the type of traffic and applications transiting on the VPN, the legacy system already in place etc. This is key for a successful IPsec VPN implementation. [9]

Abbreviations

AH:	Authentication Header
DES:	Data Encryption Standard
DSS:	Digital Signature Standard
ESP:	Encapsulation Security Payload
IETF:	Internet Engineering Task Force
IKE:	Internet Key Protocol
IPsec:	IP security
ISP:	Internet Service Provider
MPLS:	Multi-Protocol Label Switching
NAT:	Network Address Translation
OS:	Operating System
PKI:	Public Key Infrastructure
QoS:	Quality of service
RFC:	Request For Comment
RSA:	Rivest, Shamir, Adleman (name of the three investors of the algorithm)
SA:	Security Association
VoIP:	Voice over IP
VPN:	Virtual Private Network

Interesting Links

RFC links:
http://www.ietf.org/rfc.html;
http://www.pmg.lcs.mit.edu/rfc.html

A cryptographic evaluation of IPsec:
http://www.counterpane.com

Selecting cryptographic key size:
http://www.cryptosavy.com/

References

[1] IETF, Authentication Header (AH), RFC 2406, November 1998.

[2] IETF, IP Encapsulating Security Payload (ESP), RFC 2406, November 1998.

[3] IETF, The Internet Key Exchange (IKE), RFC 2409, November 1998.

[4] IETF, Internet X.509 Public Key Infrastructure Certificate and CRL Profile (PKIX), RFC 2459, January 1999.

[5] Bruce Schneier, "Applied cryptography", 1996 Wiley & Sons, Inc.

[6] Arjen K. Lenstra, Eric R. Verheul, Selecting Cryptographic Key Sizes, November 1999.

[7] Elizabeth Kaufman, Andrew Newman, Implementing IPsec, 1999, Wiley & Sons, Inc. (ISBN 0-471-34467-2).

Azim Ferchichi *has a degree in micro-engineering from the Swiss Federal Institute of technology (EPFL) at Lausanne in 1993. He spent the following two years in the telecommunications laboratory of EPFL, specialising in security services for distributed systems. In 1996 he joined today's security group CIT-CT-TPM of Swisscom. He actively participated in numerous projects as IT security and smart-card security consultant.*

Zusammenfassung

IPsec ist der erste Standard, der Sicherheitsdienste anbietet um VPNs auf der IP-Ebene zu schützen. Basierend auf einer ziemlich aufwändigen Implementierung der notwendigen kryptographischen Protokolle, können verschiedene Arten von IP VPNs realisiert werden: Intranets, Extranets, Remote Access VPNs oder jegliche Kombinationen davon. Bei der Spezifikation eines auf IPsec basierenden VPN müssen kritische Faktoren wie Netzwerktopologie und -grösse, Art des Verkehrs und der unterstützten Applikationen sowie bestehende Systeme berücksichtigt werden. Die richtige Behandlung dieser Faktoren bildet den Schlüssel zu einer erfolgreichen IPsec-VPN-Implementierung.

«Informatik-Lehrlinge machen unser Unternehmen ganz schön mobil.»

Jens Alder, CEO, Swisscom AG

IT-AUSBILDUNG. DAS PROGRAMM LÄUFT!

BUNDESAMT FÜR BERUFSBILDUNG UND TECHNOLOGIE BBT
IN ZUSAMMENARBEIT MIT DEN KANTONEN & SOZIALPARTNERN

www.profisurf.ch