Interested in learning more about security?

# SANS Institute
# InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Vulnerability's of IPSEC: A Discussion of Possible Weaknesses in IPSEC Implementation and Pro

This paper will discuss the protocol suite IPSEC, with a view to analyzing the various weaknesses have been or could be identified within the protocol. The paper will focus on a small set of example exploits across specific implementations or vendor products. The paper will begin with a brief introduction to the fundamentals of IPSEC. IPSEC is a complex and highly mathematical subject, and many of the in depth technical issues will be beyond the scope of this paper, however, an attempt will be made to show the reader t...

Copyright SANS Institute

Author Retains Full Rights

AD

# Vulnerability's of IPSEC:
# A discussion of possible weaknesses in IPSEC implementation and protocols

© SANS Institute 2002, Author retains full rights.

**Name: Daniel Clark**
**Version: 1.3**
**Date: 14 March 2002**

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

**Abstract**

This paper will discuss the protocol suite IPSEC, with a view to analysing the various weaknesses have been or could be identified within the protocol. The paper will focus on a small set of example exploits across specific implementations or vendor products. The paper will begin with a brief introduction to the fundamentals of IPSEC.

IPSEC is a complex and highly mathematical subject, and many of the in depth technical issues will be beyond the scope of this paper, however, an attempt will be made to show the reader the importance of a basic understanding of these underlying operations and tools.

**An Introduction to IPSEC**

IPSEC is not a product in itself, but simply a set of protocols developed by the Internet Engineering Task Force (IETF) as a series of Request for Comment's (RFC's). The RFC's that make up the IPSEC protocol cover the requirements of an implementation of the IPSEC protocols. It should be noted that these RFC's contain parts that are mandatory for compliance and also many areas that are optional. Clearly this can lead to both functionality and security problems between different implementations of the IPSEC protocols.

To begin to understand the nature of IPSEC and how an implementation could work, it is vital to understand a number of basic cryptographic principles. This paper will not go into the specific mathematics of various cryptographic algorithms unless it is vital for the understanding of a specific security weakness.

When dealing with cryptography and security, there are a number of principles that will appear consistently, these principles are:-

- **Confidentiality:** Data cannot be read by anyone other than the person or destination that it was intended for.

- **Integrity:** The data intended for a destination must appear at its destination without being altered.

- **Authentication:** There must be a way for the destination of the data to verify that the source of the data is legitimate. This can also include the requirement to ensure that the source and destination cannot deny that the transaction took place (non-repudiation).

To allow the three requirements above to be met, IPSEC utilises a number of cryptographic tools. These tools often rely on complex mathematics, however, a basic understanding of what each tool does can be gained without needing to understand the deeper mathematics.

Encryption and decryption are the words used for the process of converting data into an unreadable form that can then be converted to its original form using the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

decryption process. The term key is used for a variable that is used in the encryption process.

Cryptographic tools come in a number of different forms, the basic tools available are:-

- **Symmetric Key Encryption:** Works by encrypting data using a single key that can also be used to decrypt that data.

- **Asymmetric Key Encryption:** This is a more complex process where each party has a public and private key. What is encrypted with the public key can only be decrypted with the private key. The public key's are exchanged by both parties and data is encrypted by the source with the destinations public key. The data can then only be read by the destination, or someone with access to the destinations private key.

- **Hashing Function:** A process of encrypting data in a way that is not reversible. This may seem pointless, but the function is usually very fast and the same input will always produce the same fixed length output. This function is very useful for authenticating data.

Some widely used cryptographic algorithms that are mentioned in this paper appear in the list below. The mathematics behind each algorithm can become quite complex and each algorithm has certain strengths and weaknesses. The field of cryptography is one of constant change, as computing power increases and the requirement for stronger and faster encryption methods emerges. The strength or weakness of a cryptographic algorithm relates to how easily it can be broken without the key.

- **Symmetric Algorithms: DES** (Data Encryption Standard), **Triple DES** (temporary replacement for DES), **AES** (Advanced Encryption Standard, replacement for DES), **IDEA** (International Data Encryption Alogrithm)

- **Asymmetric Algorithms: RSA** (River, Shamir, and Adleman), **ECC** (Elliptic Cruve Cryptosystem)

- **Hash Algorithms: MD5** (Message-Digest Algorithm), **SHA** ( Secure Hash Algorithm)

The IPSEC protocols outline ways to utilise these cryptographic algorithms to produce communications that meet some or all of the requirements listed above ie. Confidentiality, Integrity, Authenticity.

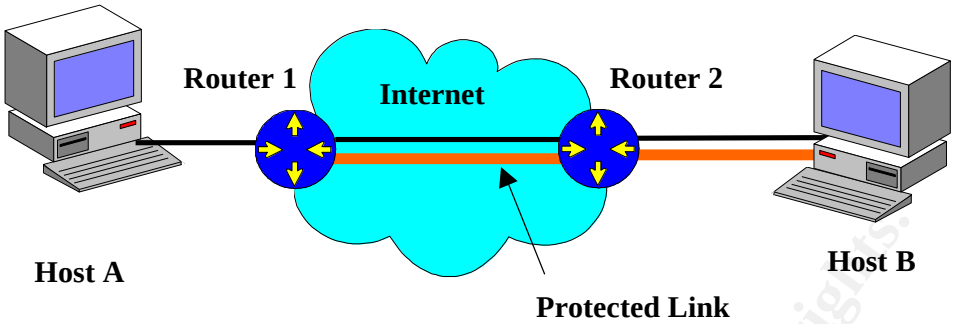
Without going into a technical explanation of each of the algorithm, a summary of how IPSEC uses these algorithms will follow.

### IPSEC Operation

The purpose of IPSEC is to provide various security services to traffic travelling between a source and destination, the destination/source may be a router, or a host. The services may be applied to all packets, or only to specific types of traffic, eg

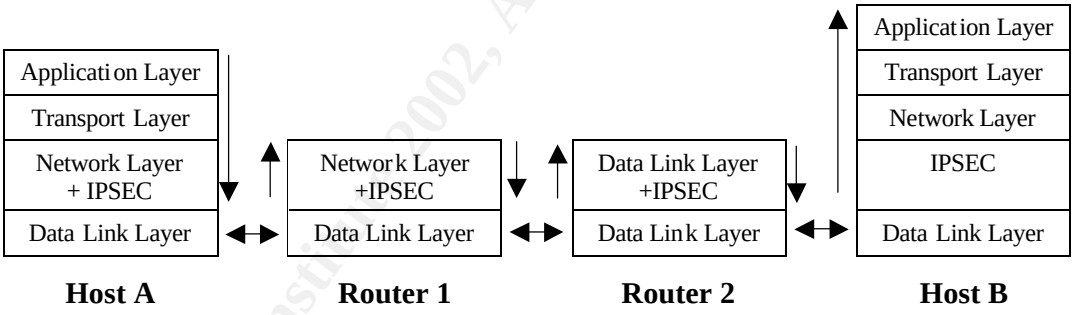
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

telnet or ftp. The diagram below shows conceptually the protection provided by IPSEC between two hosts.




The line in red shows IPSEC implemented on the path between Router 1 and Host B. There are different types of protection provided by IPSEC and there are also different modes for IPSEC to operate in. IPSEC may only operate on certain types of data while other data is transmitted on an unprotected path as shown by the black links. There may be separate IPSEC protected links between the two routers and between Host B and Router 1. It should very quickly become clear that IPSEC can operate in a number of different and complex configurations.

In terms of packet construction and the TCP/IP stack, IPSEC is implemented at the network layer. The diagram below shows the location of the IPSEC protocols in the stack, a basic understanding of the TCP/IP stack will be assumed.




(Diagram Adapted from Doraswamy & Harkins, 1999 p.25)

The arrows show the path of a packet travelling from Host A to Host B. Notice that Host B implements IPSEC as a separate layer, whereas Host A and the Routers include IPSEC as part of the network layer. These are two different types of host implementation known as OS Integrated or Bump in the Stack (BITS). There are drawbacks and advantages for both types of implementation, OS Integration can be difficult for external companies providing solutions to existing networks, however, OS Integration can make use of services in an existing network layer. IPSEC physically interacts with the stack by modifying, encapsulating or inserting data into the IP Packet before it is passed to the Data Link Layer on the way out, and again modifying the Packet before it is passed up to the Network or Transport Layer on the way in.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

IPSEC has two main modes of operation, Tunnel and Transport Mode. IPSEC modifies packets in different ways depending on the Mode in which it is operating. The diagram below shows the packet modifications for the two different modes of operation.

| | | | | | |
|---|---|---|---|---|---|
| **Original IP Packet** | **IP Header** | **TCP Header** | **Data** | | |
| **Transport Mode protected Packet** | **IP Header** | **IPSEC Header** | **TCP Header** | **Data** | |
| **Tunnel Mode Protected Packet** | **IP Header** | **IPSEC Header** | **IP Header** | **TCP Header** | **Data** |

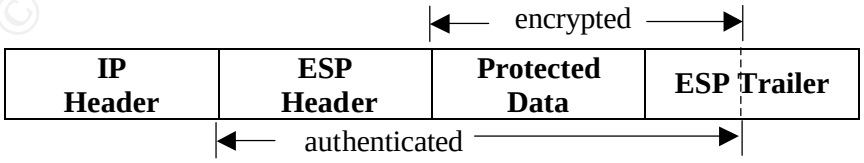
Diagram showing IPSEC packet modification (Doraswamy & Harkins, 1999 p.44)

It can be seen that in transport mode, IPSEC is adding an additional header in between the IP and TCP Headers, while leaving the data in those headers unchanged. In tunnel mode we can see that IPSEC has added a new IP Header as well as the IPSEC Header. In Tunnel mode, the entire packet is protected by the IPSEC protocol, whereas in Transport mode only the TCP Header and Data are protected by the IPSEC Header. Tunnel mode can be used in cases where the packet is travelling between two security gateways, such as routers connected to the Internet, where the destination address of the packet within the destination network needs to be protected. In transport mode, the destination IP address of the packet is transmitted without protection, this mode would need to be used when the destination is a Host IP address. It is possible to wrap modes within each other, ie. a separate IPSEC configuration in transport mode works within a tunnel mode IPSEC configuration.

The IPSEC protocols define operation in two different ways, Authentication Header (AH) and Encapsulated Security Payload (ESP). AH and ESP are quite different in the security that they provide, and operate in different ways.

**Encapsulating Security Payload (ESP)**

The ESP protocol provides data integrity, authentication and confidentiality. The data to be transmitted is encrypted and the entire packet, minus the IP Header and the authentication data is authenticated. The diagram below shows a simplified version of how ESP operates.



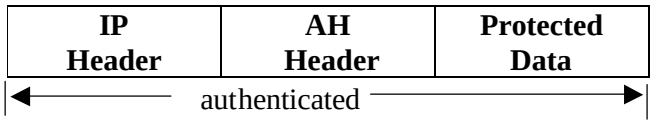

Encapsulated Security Payload (Doraswamy & Harkins, 1999 p.44)

From the diagram we see that the data to be sent is encrypted, thus providing confidentiality. The ESP Header and the encrypted data are also authenticated. This means that a hash algorithm is used to produce a fixed length representation of the authenticated data that is attached to the end of the packet. Only someone who knows

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

that hashing algorithm can check to see that the data which arrives matches the hash attached to the packet. If the two hash results do not match, then it can be assumed that the packet was modified in transit.

**Authentication Header (AH)**




Authentication Header (Doraswamy & Harkins, 1999 p.44)

The Authentication Header is a much simpler protocol when compared with ESP, however it provides much less in terms of packet security. The AH header only authenticates the data and IP Header. This means that there is no confidentiality provided by AH, it only provides integrity and data source authentication. AH is useful when the only concern is protection against modification of the data while in transit. Clearly the processing overhead for AH will be significantly less than that for ESP. Encryption and decryption take much more processing than hashing.

Now that we have a very brief understanding of the protocols of IPSEC, how is this actually implemented in software or hardware?

The methods through which IPSEC compliant peers establish and operate IPSEC protected links become quite complicated. However, the way that these methods are implemented are vital to understanding the possible vulnerability's in IPSEC.

**Security Associations**

A Security Association (SA) is the term used in IPSEC to describe a negotiated set of parameters between communicating peers. With the wide range of encryption and hashing algorithms available, it is vital that both peers have a way of defining the particular algorithms that will be applied and how they will be applied to each SA. There is also a requirement for clear guidelines to define how the peers initially negotiate these parameters to set up an SA. How does a peer with multiple SA's between various hosts recognise and manage traffic for each SA?

Each peer involved in IPSEC communications must set up an SA Data Base (SADB) to manage its Security Associations. This data base can keep records of which encryption and hashing algorithms the host is capable of using, and which hosts it has permission to communicate and on which ports. It should become clear that this SADB is likely to become the cornerstone of IPSEC operation and if poorly designed it could become the Achilles heel of a secure communications system.

The RFC's produced by the IETF define how an SADB should operate, it also defines the standards through which secure exchanges for setting up SA's must be conducted. The Internet Key Exchange (IKE) is described in a separate RFC and defines how these exchanges take place. IKE is itself based on the Internet Security Association and Key Management Protocol (ISAKMP) which itself implements other protocols developed by cryptographers. Essentially, these protocols are designed to ensure that

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

any implementation of IPSEC or any network security software ie. SSL, are written in a way that has been publicly scrutinised by the community of cryptographers and is considered to be reliable. The dangers of providers who develop in-house cryptography are many, often proprietary algorithms are weak or poorly implemented. These IKE/ISAKMP protocols can ensure that customers can place more trust in an implementation that follows them, assuming the providers are honest. An in-depth look at the operation of IKE is beyond the scope of this paper, however, the referenced text by Doraswamy & Harkins is an excellent resource. Instead, specific areas of IKE or the SA process will be expanded upon when necessary in the next section of the paper.

**Vulnerability's in IPSEC**

The IPSEC protocols are an excellent step in the right direction for internet security. If correctly implemented and configured, the protocols could provide e-business and organisations like defence with the ability to take advantage of the speed and reach of the internet without being as prone to the dangers of attack in an unpoliced environment. Leasing dedicated secure lines from telecommunications providers is prohibitively expensive, whereas dial-up to the internet is relatively cheap.

By incorporating application and transport layer security measures such as Firewalling, SSL and SSH along with IPSEC, it would seem that a highly robust secure network could be created at relatively low cost.

So where could possible vulnerability's in IPSEC lie? IPSEC is built on a structure of numerous cryptographic and networking foundations, IPSEC is also a set of protocols defined by RFCs that can translate into useable vendor products in different ways. The IPSEC RFCs themselves are often strict and clear in many areas, while being slightly ambiguous or unclear in others. As with most security measures, an associated overhead in speed is usually incurred. The article from 'The Austaralian' below shows the problem with the culture of speed over security.

> " E-commerce businesses in Australia were choosing speed over security and did not realise the implications, said Alex van Someren, managing director of encryption specialist nCipher.
>
> Companies could not excuse this situation by saying they were using short keys because longer, more complicated digital keys made connections speeds up to eight times slower…" (Denton, Tessa, March 12 2002)

If money is spent to install an IPSEC system, but low-grade encryption is used, then the strength of the security could be greatly effected. Even worse, if vendors write code that attempts to speed up operation with the result of known or inadvertent weakening in the encryption or hashing algorithm, then clients could be under the perception of high grade security that is in fact easily broken.

The DES algorithm is clear evidence that encryption algorithms do have a finite lifetime, as computing power increases and smart cracking software become more easily available, it is essential that encryption algorithms grow and change to meet the threat. The IPSEC protocols make allowances for this, with options to specify

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

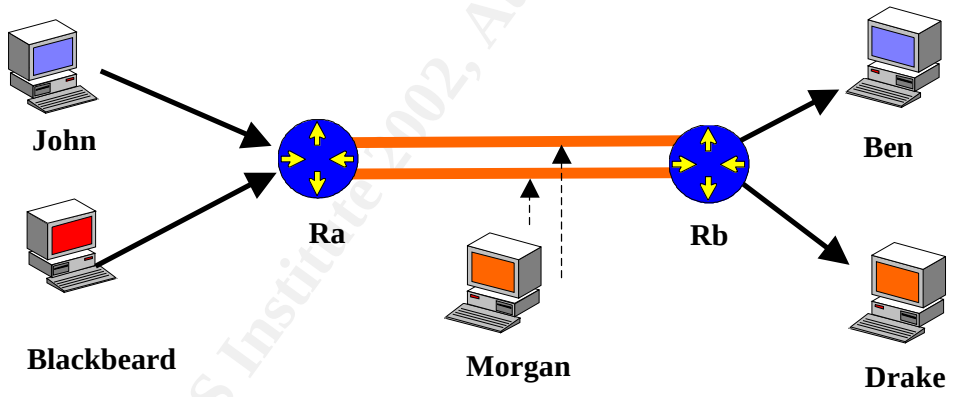
mandatory algorithms for certain SA's. However, implementation of this requirement is the responsibility of the vendor, and consumers should be very clear on the way that their IPSEC product, and the product of their peer, operates.

An organisation called TruSecure Corporation has a division ISCALabs (www.icsalabs.com) that focuses on certifying vendor IPSEC implementations as compliant with the RFCS for IPSEC. As IPSEC is a relatively new technology, it is vital that an organisation like this can develop credibility and the ability to satisfy consumers that products labelled as certified do actually comply with current versions of the IETF RFCs. As with most networking specifications, there is often difficulty in getting implementations from different, competing vendors to talk to each other. This can often be due to ambiguities in the specifications at the time of development, or also an intention to limit customers to systems built only on the vendors product.

We can now break down vulnerability's into a few categories, those inherit to the IPSEC protocols, those related to the underlying cryptography, and those relating to poor vendor implementation. A small selection of these will now be discussed.

**Vulnerabilties in IPSEC protocols**

There are numerous speculations and scenarios in which the protocols defined for operation of IPSEC can be challenged. Some of these may be so abstract as to be considered unfeasible in a real world situation. Here are two attacks considered by Vesselin Tzvetkov from Bochum university in Germany:-




(Diagram adapted from Tzvetkov, VPN Attacks)

**Cut-And-Past Attack:**
This attack will only be possible on two networks that use IPSEC as a tunnel between the two routers that link the networks. There is also a requirement that the attacker has access to a second machine in each of the two networks.

The attack works by Morgan sniffing a legitimate encrypted packet from John to Ben. Morgan also sniffs a planned packet sent from Blackbeard to Drake. Morgan copies encrypted data from John's packet into a packet from Blackbeard to Drake. Router B is tricked into decrypting Johns packet for Ben and sending it to Drake. This exploit is not as straightforward as it may appear, as there are some other requirements relating to the sequence numbers used in IPSEC packets and ensuring that John's genuine

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

packets don't reach Router B before the false packets do. IPSEC includes various replay-attack protection methods that would make this attack a little more difficult to successfully carry out in a real world situation.

**Session Hijacking:**
Similar to the previous attack, Blackbeard could have created packets that are intended to arrive at Ben as if they were sent from John. Instead of stealing Johns packet and asking Router b to decrypt it for Drake, Morgan now pastes Blackbeards data into John's packet and it is decrypted by Rb and sent to Ben as though it came from John.

These attacks are much more complicated to conduct in practice, as sequence numbers and other authentication issues must be overcome. Despite this, the attacks appear feasible.

**Vulnerability's in underlying Protocols or Host**

The IPSEC protocols rely on a number of underlying technologies to achieve encryption and authentication. The initial establishment of SA's is also completed using Key Exchange methods defined by other protocols.

These Key Exchanges and communications designed to set up the parameters of an SA are themselves reliant on various forms of encryption and authentication.

There is a requirement for the storage of keys and certificates on the local system. Algorithms such as Diffe-Helman are used to establish shared secrets between two hosts over an untrusted link. Weakness or vulnerability's in the specific methods for key exchange, in hashing or encryption algorithms could easily affect the security of IPSEC.

It is now widely accepted that the DES encryption algorithm is now susceptible to brute-force attacks (brute force attacks try to decrypt data by simply trying every possible key value) using readily available software and hardware. If the protection surrounding the SADB is broken, then every key and IPSEC links set up using that database is easily obtainable.

Even if there is a secure tunnel between hosts for a specific type of traffic, if the hosts itself is compromised from a separate unprotected connection, then all protected data will be available to the attacker. The sensible placement and monitoring of secure links created with IPSEC is critical. IPSEC is simply a tool and must be combined with other security measures such as Host Intrusion Detection Systems (HIDS), good key management, well configured firewalls and many others.

**Vulnerable Implementations**

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

A number of articles on the bugtraq mailing list, Dec 2001 discussed the discovery of a Denial of Service (DOS) attack that could be launched on Windows 2000 machines that use IPSEC.

The discovery showed that sending UDP traffic to port 500 of a Windows 2000 machine could raise the processor usage up to 99% on a high-end machine and render it incapable of communication. The advisory suggested that firewalling port 500 off would be an effective solution, however

> 'If you are actively making usage of IPSEC at your site, then an immediate fix to this problem might not be available'
> (c0redump@ackers.org.uk 11 Dec 2001, Bugtraq List)

It was interesting to note that similar test were conducted on NetBSD machines and the attack was not able to render the machine incapable of communicating.

The listings also noted that most VPN configurations implement a packet filter that only accepts connections on port 500 from known clients and would not be susceptible to this attack.

As with many Microsoft products, the 'out of the box' configurations and default settings are often very insecure. For an enterprise to successfully use the IPSec implementation provided by Microsoft for Windows 2000, it is extremely important that a high level of knowledge and training is held by the system administrators who configure IPSec. Simply clicking 'next' through the default wizards will most likely leave a network vulnerable to the simplest of attacks. The knowledge required to develop local specific policies that require the right level of encryption and hash algorithm comes with training, training costs money, and money is not always easily parted with by management. Especially when the company has already spent large amounts on the software required to use IPSec. It is vital to understand the core concepts behind IPSec and how they integrate with a specific implementation to achieve reliable security.

Numerous vendors are providing IPSEC equipment, both OS manufacturers such as Microsoft and also hardware manufactures like CISCO. It is certainly a good idea for consumers to visit the www.icsalabs.com site to check the details of the compliance and compatibility of various vendor solutions before spending large amounts of money. Thought must also be given to the fact that expensive and powerful equipment can be rendered useless through poor configuration, the training and expertise required to set-up and monitor good IPSEC solutions must be factored in to purchase plans.

**Summary & Conclusions**

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

IPSEC is an excellent set of protocols, developed out of significant work and collaboration from within the networking security community. IPSEC can be viewed as another piece of the security arsenal, and if used correctly in conjunction with numerous other technologies it could ensure a much greater degree of security on computer networks.

One of the most important lessons that was gained from the study of IPSEC, is the requirement for customers to understand the implementation of their specific vendor or OS provider. Some vendors produce products that are not fully compliant with the IPSEC protocols, and could be seriously flawed in the security that they provide.

As exploits and vulnerability constantly surface, it is essential that any implementation of IPSEC has the ability to grow and change to meet new threats or fix new vulnerability's. This paper has only scratched the surface of the technical aspects of IPSEC, and any company or system administrator considering an implementation should research widely before committing to a particular product.

**References:**


c0redump@ackers.org.uk "Re: UDP DoS attack in Win2k vi IKE" 11 Dec 2001, Bugtraq List URL: http://securityfocus.com (12 March 2002)

Denton, Tessa. "E-commerce sites 'easily cracked'" The Australian IT, 12 March 2002 URL: http://australianIT.com.au/ (13 March 2002)

Doraswamy, Naganand & Harkins, Dan. IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks. New Jersey: Prentice Hall, Inc, 1999.

IBM eNetwork Software Library, "Using IPSec to Construct Virtual Private Networks",
URL: http://www-3.ibm.com/software/network/library/whitepapers/vpn/remsec.html
(12 March 2002)

ICSALABS URL: http://www.icsalabs.com/ (13 March 2002)

Jappila, P.& Poyhonen P., "The Internet Security"
URL: http://keskus.hut.fi/opetus/s38130/s98/security/secfinal.pdf
(13 March 2002)

Netlock "Protecting Modern Enterprise Networks"
URL: http://www.netlock.com/security-protect.html
(12 March 2002)

Paladugu, V. Cherukuru, N. & Pandula S. "Comparison of Security Protocols for Wireless Communications"
URL: http://ece.gmu.edu/courses/ECE543/reportsF01/pachpa.pdf
(12 March 2002)


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

SANS Institute 1.4 SANS Security Essentials IV: Encryption and Exploits, 2002

Sharick, Paula. "Use IPSec to Protect Your LAN Resources", October 2000, Security Administrator URL:http://www.ntsecurity.net (12 March 2002)

Szalay, Mate, "A Special Attack Against IPSec", Helsinki University of Technology, March 2000. URL: http://www.hut.fi/~mszalay/essay.html (12 March 2002)

Tzvetkov, Vesselin, "Way of using for VPN.Attacks and vulnerabilities of IPSec. Part II" URL: http://homepage.ruhr-uni-bochum.de/vesselin.tzvetkov/pro/AttIPsec.pdf (13 March 2002)

© SANS Institute 2002, Author retains full rights.

Last Updated: May 24th, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Malaysia @ MCMC 2013 | Cyberjaya, MY | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| SANS Pen Test Berlin 2013 | Berlin, DE | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| Industial Control Systems Security Training - Houston | Houston, TXUS | Jun 10, 2013 - Jun 15, 2013 | Live Event |
| Security Impact of IPv6 Summit 2013 | Washington, DCUS | Jun 14, 2013 - Jun 16, 2013 | Live Event |
| SANSFIRE 2013 | Washington, DCUS | Jun 14, 2013 - Jun 22, 2013 | Live Event |
| SANS Canberra 2013 | Canberra, AU | Jul 01, 2013 - Jul 13, 2013 | Live Event |
| Digital Forensics & Incident Response Summit 2013 | Austin, TXUS | Jul 09, 2013 - Jul 16, 2013 | Live Event |
| SANS London Summer 2013 | London, GB | Jul 09, 2013 - Jul 16, 2013 | Live Event |
| SANS Rocky Mountain 2013 | Denver, COUS | Jul 14, 2013 - Jul 20, 2013 | Live Event |
| SANS Mumbai 2013 | Mumbai, IN | Jul 22, 2013 - Jul 27, 2013 | Live Event |
| SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification | Washington, DCUS | Jul 22, 2013 - Jul 26, 2013 | Live Event |
| SANS San Francisco 2013 | San Francisco, CAUS | Jul 29, 2013 - Aug 03, 2013 | Live Event |
| SANS SEC 560: Network Penetration Testing @ Bangalore 2013 | Bangalore, IN | Aug 05, 2013 - Aug 10, 2013 | Live Event |
| SANS Boston 2013 | Boston, MAUS | Aug 05, 2013 - Aug 10, 2013 | Live Event |
| Critical Security Controls Summit | Washington, DCUS | Aug 12, 2013 - Aug 18, 2013 | Live Event |
| Industrial Control Systems Security Training - DC | Washington, DCUS | Aug 12, 2013 - Aug 16, 2013 | Live Event |
| SANS Thailand 2013 | Bangkok, TH | Aug 19, 2013 - Aug 31, 2013 | Live Event |
| SANS Virginia Beach 2013 | Virginia Beach, VAUS | Aug 19, 2013 - Aug 30, 2013 | Live Event |
| Mobile Device Security Summit 2013 | OnlineCAUS | May 30, 2013 - Jun 06, 2013 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |