Global Information Assurance Certification Paper

Adam Hansen
September 25, 2000

Overview

Recently, an enormous amount of attention has been directed at information security. This trend is due in part to a number of high profile web sites that have been compromised by hackers via the Internet. Accordingly, a great deal of attention has been placed on the gateway that stands between the corporate network and the Internet, the firewall. The question then becomes, is this enough?

Numerous studies, conducted by many reliable sources, have concluded that the majority of hacks are conducted from within as opposed to outside the confines of a corporations information system. According to Security Magazine (www.scmagazine.com), an estimated sixty percent (60%) of all hacks come from within. However, in many instances, businesses have a false sense of security, feeling that their firewall will protect them from being hacked, glossing over the statistics.

This paper will focus on describing the IPSec functionality built into Windows 2000. Specifically, it will show what IPSec is and how Microsoft implemented IPSec in Windows 2000.

What is IPSec

As the size of computer networks continue to grow, especially the Internet, more and more sensitive information is transmitted. As a result, the need for a method of securing sensitive information has become the focus of a working group affiliated with the Internet Engineering Task Force (IETF). The IETF determined the need for a standard, which would provide for the necessary security to be applied to internetworking traffic, yet allow for the inner-operability of varying types of host. The development of an RFC is currently underway as the working group has not completed the final draft. However, significant progress has been made in the forms of working drafts of this new standard. This work-in-progress has been made available at http://www.ietf.org/html.charters/ipsec-charter.html

Oversimplified, IPSec is a protocol, which applies to the OSI model. Specifically, it describes how information is manipulated at the network layer of the OSI model to include the ability to secure both the header and payload. The current draft of the standard accounts for IP Authentication Header (AH) and IP Encapsulating Security Payload (ESP).

The current working document outlines a protocol, which would allow for a variety of cryptographic algorithms to be used to secure the data.

This standard also calls for the development of protocols and cryptography techniques for the management of the keys used to secure the network layer. This, in part, has been realized by a protocol called Internet Key Management Protocol (IKMP), which will facilitate the management of the aforementioned keys from the application layer.

How Windows 2000 IPSec Works

Microsoft has made a commitment to developing a secure operating system in Windows 2000. As such, the developers of this operating system identified IPSec as the emerging standard with the most potential, thus Microsoft has attempted to comply with the current draft of IPSec.

The implementation of IPSec included with Windows 2000, does a fairly good job of complying with the current IPSec draft. The remainder of this section will discuss the technologies used by Microsoft in the shipping implementation of IPSec in Windows 2000.

IP Authentication Header

IP Authentication Header (AH) has been implemented in Windows 2000. AH is used to prevent anyone from re-playing the transmitted packet sequence at a later time. It also adds integrity to the mix by computing a hash of each packet before it leaves. It finally keys the message so only the intended recipient can de-encrypt the packet.

AH works by computing the hash value of each packet passed from the transport layer of the OSI model with its sequence number. Once the hash has been computed, the packet is encrypted using a key, then transmitted.

Microsoft has implemented the above using the Diffie-Hellman public key cryptography algorithm. The algorithm used in this technique is an open source standard, thus theoretically compliant with any other Diffie-Hellman implementation.

Hash Message Authentication Code (HMAC) has been implemented as the private key cryptography algorithm. Once again, this is an open source technology, which is used to handle the private key for this encryption of the header.

Diffie-Hellman and the selected version of HMAC combine to compute the hash of the packet including the sequence information to prevent

anyone from replaying the communication. This technology complies with the IETF draft as it implements packet integrity, anti-replay, authentication and non-repudiation.

IP Encapsulating Security Payload (ESP)
The IETF working draft calls for IP Encapsulating Security Payload (ESP). This has been implemented in Windows 2000 to add the required confidentiality as well as to secure the packet payload.

Data Encryption Standard – Cipher block chaining (DES-CBC) has been implemented in the shipping version of Windows 2000 to secure the packet payload. DES-CBC is a secret key algorithm used to encrypt the packet payload pre-transmission. The actual encryption technique works by combining a random number and the secret key before passing the packet payload onto the network.

Microsoft has used DES-CBC to meet the ESP requirement of the IPSec working draft. This approach to the ESP requirement works well because it offers a high level of security based on an open standard.

Enhancements
The aforementioned techniques implemented to meet the requirements of IPSec have been exceeded in the current version of IPSec implemented in Windows 2000. This has been accomplished via the addition of key management schemes.

Microsoft has added the Internet Security Association and Key Management Protocol (ISAKMP) with the Oakley key determination scheme (Oakley) to offer an enhanced key management support scheme. This package simplifies the management of the many keys used in the IPSec process, such that it can be managed.

Furthermore, leveraging Kerberos technology, a centralized key management scheme can be easily implemented within Windows 2000. Not to mention both ISAKMP/OAKLEY and Kerberos are referenced as either technologies, which IPSec is based on or support goals for the standard.

Conclusion
In today's economy, the exchange of information can be considered as important as the pen was in the 70's. The computer is an essential tool for in corporate America today, and internetworking has allowed for the exchange of information such that the worker of today can work smarter and more efficiently than ever before.

However, as with most things, with the good comes the bad. Statistics have shown that the majority of the information, which has been compromised, was done so by the people on the inside. This paper has described one feature included with all versions of Windows 2000, which can make it much more difficult for information to be compromised, regardless of where it comes from and where it is going.

IETF IPSec Working Group
http://www.ietf.org/html.charters/ipsec-charter.html

Armstrong, Illena, "Beating the Bad Guys, Designing Secure Systems", July 2000, InfoSecurity Magazine, URL:
http://www.scmagazine.com/index2.html

"Windows 2000 Security Services Features", 1999, Microsoft, URL:
http://www.microsoft.com/WINDOWS2000/guide/server/features/security.asp

"IP Security for Windows 2000 Server", 1999, Microsoft, URL:
http://www.microsoft.com/windows2000/library/howitworks/security/ip_security.asp

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS