IPENETRATE

J. Chong (jasc8@u.washington.edu)
Y. Luon (yarun@u.washington.edu)
R. Prins (rprins@u.washington.edu)
A. Trotter (atrotter@u.washington.edu)

INFO 498: Introduction to Computer
Security Incident Response
Autumn 2004
November 22, 2004

iPenetrate

IPENETRATE

IPSEC AND YOU

OUR ONLY JOB IS
TO PENETRATE ONE
THING… YOUR
NETWORK!

INFO498:
AUTUMN 2004

WHAT IS IPSEC?

OBJECTIVE

IPsec is not a single protocol, but rather a suite of protocols designed to protect IP packets as well as provide a defense against network attacks. This is all accomplished by *encrypting* and *authenticating* all IP packets at the Network layer from the OSI model (Layer 3).

For example, IPsec protects packets and networks from *sniffers* by encrypting data, *data modifications* by using cryptography based checksums, *identity spoofing, denial of service, application layer and password based attacks* using mutual authentication, and *man in the middle attacks* using a combination mutual authentication and cryptography based keys.

IPsec is deployable on any platform (windows, unix, mac) and can also be implemented on end hosts, gateways, routers and firewalls.

HISTORY

In November of 1998, the Internet Engineering Task Force (IETF) put out RFC 2401 entitled “Security Architecture for the Internet Protocol” otherwise known as IPsec. Since then, IPsec has grown into 12 RFCs of security measures like MD5, SHA-1, and IKE.

Currently, IPsec is recognized by the IETF as a proposed progressive standard. In order for any RFC to become a proposed standard it must be stable, have resolved design choices, be well understood, have received significant community review, and have community interest. No implementation documentation is required for a progressive standard, but it is highly recommended. IETF does call a progressive standard as an “immature specification.”

The next step for IPsec on the standards tract is for it to become a draft standard before it can become an established standard like SMTP, POP3, TELNET, and FTP. Other progressive standards similar to IPsec are WebDav, IMAP4, and LDAP.

10 out of 10 My Little Pony’s agree that IPsec is vital for your VPN connection!

MECHANICS OF IPSEC

iPenetrate is a group of University of Washington Informatics Students whose interests lie in graduating, girls, eating, and sleeping. When they are not doing the above, they enjoy attending class and learning about all the magical things that higher education has to offer.

We all really enjoy long walks on the beach with a tall drink in our hands. Good company is hard to find, but if you are looking for a friend, then so are we! Don't be afraid to talk to us, we're just that 23 foot 6 inch, 500 pound, 87 year old freak you've been waiting your whole life to meet and confess your deepest sins to.

The beauty of being a piece of wood is that nobody wants to steal your information. We wish we could be that lucky!

AUTHENTICATION HEADER (AH)

The authentication header is one of three ways to secure your data when using IPsec. Using the authentication header provides the user with two types of protection: data integrity, and anti-replay. The authentication header ensures that the data contained in the packet is not modified by signing the packet using a specified hash algorithm. Though the data is readable—the data is not encrypted—the integrity of the data is protected. In addition, the authentication header ensures that middlemen do not send hacked packets by including a sequence number in each packet. If a packet is out of sequence, it will be dropped.

ENCAPSULATING SECURITY PAYLOAD (ESP)

The encapsulating security payload (ESP) is one of the two protocol types that IPsec can use when employed by a host, router, or other deployable device. The major difference between ESP and the Authentication Header (AH) protocol is that ESP provides data confidentiality along with data integrity, data authenticity, and anti-replay service which AH provides. In addition, because ESP provides this data confidentiality, the packet is separated into three parts when being sent from one host to another. This is done because the original IP header is included in the payload portion which is encrypted. The IP header that is visible does not contain the source or destination addresses for the packets. Because of this the IP header is not signed when the ESP protocol is used.

SECURITY ASSOCIATIONS (SA)

Security Associations are the contracts that are created between two computers for the sending and receiving of data. Moreover, a Security Association is a combination of mutually agreed-upon key, security protocol, and SPI which together define the security that will be used to protect the communication from sender to receiver. Each computer has two Security Associations per unique computer; one SA for inbound traffic and another for outbound.

The new Seattle Public Library looks funny and their IP packets have no odor! Strange if you ask us!

EXAMPLES OF USE

When deploying IPsec, some of the most practical implementations are within Virtual Private Network (VPN) connections and dial-up remote access connections to remote servers. With IPv4 itself, there is no guarantee of confidentiality of data or integrity of data, and because of this IPsec is considered an essential component of remote connections. IPsec is most widely deployed where information is critical and must be protected, like a hospital's LAN or businesses that have multiple sites and need remote connections to one another.

IPENETRATE

J. Chong (jasc8@u.washington.edu)
Y. Luon (yarun@u.washington.edu)
R. Prins (rprins@u.washington.edu)
A. Trotter (atrotter@u.washington.edu)

INFO 498: Introduction to Computer Security Incident Response
Autumn 2004
November 22, 2004