Virtual Private Networks and Secure Protocols

Cryptography FourB

Ed Crowley

Fall '08

Topics

- Secure Protocols &VPNs
  - HTTPS
  - SSL
  - IPSEC
  - PPTP

Secure Protocols and VPNs

- In the real world, secure communications depends on multiple services. Specifically:
  - Authentication (Validate communicators)
  - Key Agreement/Exchange
  - Confidential Communications (Encrypted message exchange)
  - Integrity (Assurance message not modified)
  - Nonrepudiation (Assurance that one party can't deny the communication.)
- Secure email implements all of the above services, SSL and IPSec implement them all except nonrepudiation.

E-mail

- While many e-mail programs have cryptographic protection built in, you can also install your own cryptographic programs.
- For example, Microsoft Outlook Express comes with S/MIME (Secure/Multipurpose Internet Mail Extension) support. But because some copies of Outlook Express S/MIME support only 512 bit public keys, some users might want to add PGP, which supports longer public keys.

Virtual Private Network

- A virtual network is built on top of an existing physical network that provides a secure communications mechanism for data and control information transmitted between networks.
  - Most often utilized to protect communications carried over public networks such as the Internet.
- Can provide several types of data protection, including:
  - Confidentiality
  - Integrity
  - Authentication
  - Replay protection
  - Access control

Three VPN Architecture Models

- Gateway-to-gateway
  - Protects communications between two specific networks
- Host-to-gateway
  - Protects communications between one or more individual hosts and a specific network belonging to an organization.
- Host-to-host
  - Protects communication between two specific computers.

Gateway to Gateway VPN

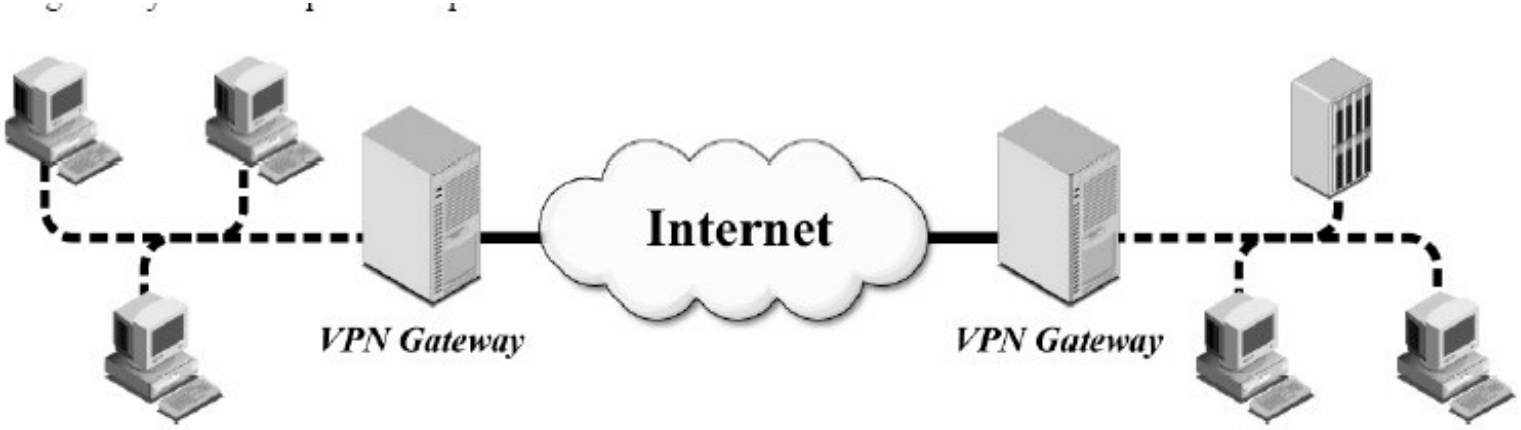

Figure 2-2. Gateway-to-Gateway Architecture Example

- *This, and following images from NIST SP 800-77*

Host to Gatway VPN

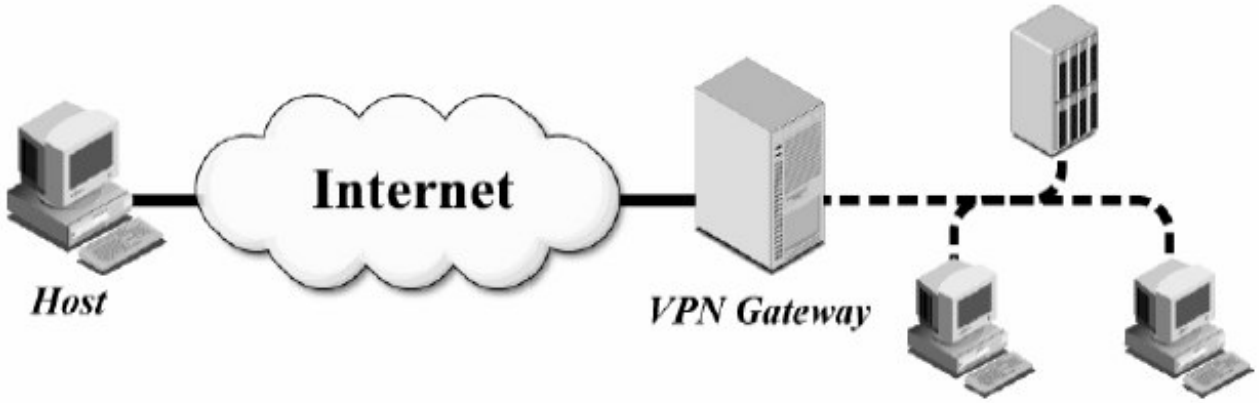

Figure 2-3. Host-to-Gateway Architecture Example

Host to Host VPN

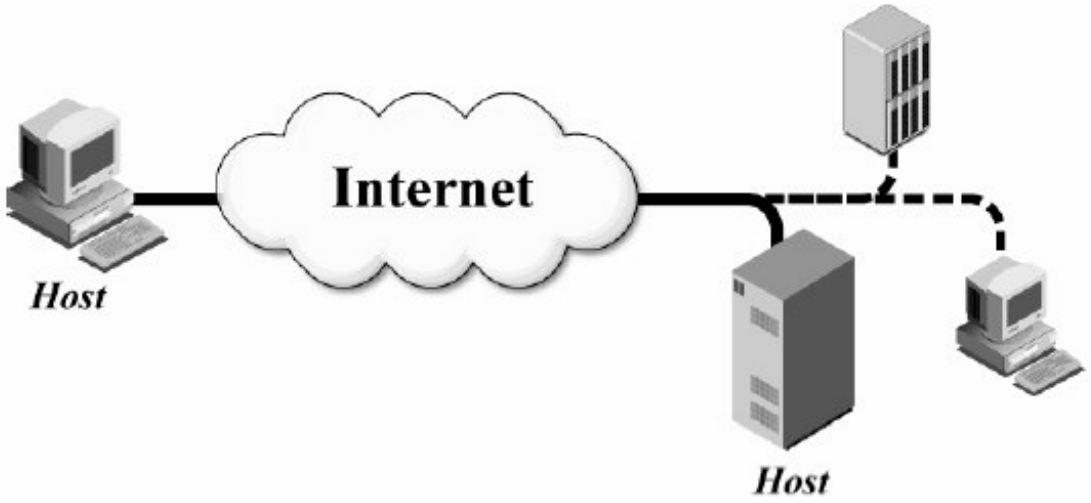

Figure 2-4. Host-to-Host Architecture Example

VPN Comparison

Table 2-1. Comparison of VPN Architecture Models

Feature	Gateway-to-gateway	Host-to-gateway	Host-to-host
Provides protection between client and local gateway	No	N/A (client is VPN endpoint)	N/A (client is VPN endpoint)
Provides protection between VPN endpoints	Yes	Yes	Yes
Provides protection between remote gateway and remote server (behind gateway)	No	No	N/A (server is VPN endpoint)
Transparent to users	Yes	No	No
Transparent to users' systems	Yes	No	No
Transparent to servers	Yes	Yes	No

TCP/IP Layer Review

Application Layer. This layer sends and receives data for particular applications, such as Domain Name System (DNS), HyperText Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).
Transport Layer. This layer provides connection-oriented or connectionless services for transporting application layer services between networks. The transport layer can optionally assure the reliability of communications. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are commonly used transport layer protocols.
Network Layer. This layer routes packets across networks. Internet Protocol (IP) is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP).
Data Link Layer. This layer handles communications on the physical network components. The best-known data link layer protocol is Ethernet.

Figure 2-1. TCP/IP Layers

Secure Protocols by TCP Layer

- HTTPS, SSH – Application level security
- SSL/TSL – Security at the transport level.
- IPSEC – Security at the network level.
- PPTP – Security at the data link layer.
- Link encryption – Security at the data link and physical levels.

SSL/TLS

- Netscape developed SSL to secure Internet transactions (’94).
- SSL is a data communication protocol that implements three cryptographic services
  - Authentication
  - Confidentiality
  - Message integrity.
- By default, authenticates server to client.
- Does not provide MIM attack protection

SSL/TLS

- SSL evolving into TLS
  - An IETF open standard.
    - Only minor differences between SSL V3 and TLS V1
  - Can use a variety of technologies including: 3DES or RC4, MD5 or SHA1, with RSA and Diffie Hellman and X.509 certificates for authentication.
- Provides secure key exchange an Internet browser and an Internet server.
- Does not offer nonrepudiation.

SSL/TLS Handshake

Phases

- Hello
  - Client and server negotiate crypto algorithms, compression methods, and a session ID value
- Server sends certificate
  - Server may request client certificate (rare)
- Key Agreement (Exchange)
- Authentication
  - Client verifies server cert
  - If requested, sends its cert
  - Finished handshake messages
- Bringing up primary crypto
  - Change cipher.
  - Finish handshake.

SSL/TLS Encryption Options

- RC4, 40 bit or 128 bit
- DES – 56 bit
- 3DES – 168 bit
- RC2 – 40 bit
- Utilization depends upon client/server negotiation.
  - Impacted by browser configuration

SSL Rollback Attack

- SSL 3 and TLS 1 are similar and are considered secure
- SSL 2 is vulnerable to a rollback attack
  - SSL 2 can use 40 bit encryption
- In browsers that offer it as an option, SSL 2 should be manually turned off

IPSec

IETF standard that can provide OSI Network Level:

- Confidentiality
- Authentication
- Access control
- Integrity

Supported IPSec communication architectures:

- Host to host
- Network to network
- Host to network

IPSec

- An IPSec enabled computer automatically protects any electronic communications between itself and another IPsec enabled computer including:
  - Email
  - Web browsing
  - File transfers
- IPSec automatically negotiates cryptographic protections with another IPSec enabled computer that has acceptable credentials.
- In contrast to SSL, that negotiates ciphers in plain text, IPSec hides its negotiations.

IPSec

IPSec Components

- Security Association (SA)
- Internet Key Exchange (IKE)
- Secure Protocols
  - Authentication Header (AH) provides
    - Integrity
    - Authentication
    - Nonrepudiation.
  - Encapsulation Security Header (ESH) provides
    - Confidentiality.

IPSec Three Phases

1. Key agreement and authentication
2. Negotiation of VPN parameters (Setting up Bulk Exchange Parameters)
3. Data Protection

IPSec policy

- Defines a minimum set of communication parameters to be used when securing an IPSec connection.

IPSec Security Association (SA)

- When a VPN connection is established, the negotiated entries are saved to the Security Association Database.
  - The index value is called the Security Parameter Index or SPI
  - The SPI gets recorded within the header of each IPSec packet

Three Security Association components

- SPI
- Destination IP address
- Security protocol identifier (AH or ESP)

Two Security Association Types

1. Transport
   - Facilitates communications between two hosts
   - During transport, source and destination IP addresses in plain text.
   - Usually, only authenticates payload
2. Tunnel mode
   - When either end of a security association is a security gateway, the SA must be tunnel mode
   - Encrypts ultimate destination as well as source IP addresses

- Hosts must support both transport and tunnel mode

Internet Key Exchange

- Hybrid of ISAKMP and Oakley methods
- Allows two IPSec nodes to decide which algorithms they will use for authentication and encryption, as well as how long this will last

Negotiated issues include

- Authentication method
- Protocols (ESP or AH)
- Algorithms
- Keys

IPSec Issues

- AH breaks many NAT implementations
- IKE expect source and destination ports to be UDP 500
- Because of encryption, may be difficult to troubleshoot

SET

- Secure Electronic Transaction
  - Because it uses certificates, considered a PKI application
  - Level 7 protocol
    - Developed by a consortium including Cybercash, MasterCard and Visa.
- Provides confidentiality for purchases by encrypting the payment information.
- Covers end to end transactions.

Questions?

References One:

http://cis.gsu.edu/~rbaskerv/cis8680/Lessons/crypto/index.html

http://www.simonsingh.net/Crypto_Corner.html

http://www.schneier.com/

http://www-106.ibm.com/developerworks/library/s-pads.html

http://www.math.temple.edu/~renault/cryptology/affine.html

References Two

https://www.isc2.org/cgi-bin/request_studyguide_form.cgi?AG=6042

http://www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/distsys/part2/dsgch14.mspx

http://www.fas.org/irp/nsa/rainbow.htm