Communications, Networking & Security

USING SSL AND VPNs TO PROVIDE SECURITY

HARPARTAP PARMAR

CONTEMPORARY CONTROLS®

May 9, 2017
TOPICS

- Secure Socket Layer (SSL)
- Virtual Private Network (VPN)
- Similarity and Differences between SSL/VPN
WHAT IS SSL?

- Security Protocol for the encryption of data
- Allows secure communication to occur over an unsecure connection between a client and a server
- Provides
  - **Confidentiality** (Encryption)
  - **Data Integrity** (Hash Function/Message Digest)
  - **Authentication** (Digital Signatures/Certificates)
SSL AND TLS VERSIONS?

- **SSL (Secure Sockets Layer)**
  - Version 2.0 and 3.0
- **TLS (Transport Layer Security)**
  - Version 1.0, 1.1 and 1.2
- TLSv1.0 was based on SSLv3
- SSLv2 and SSLv3 have been deprecated because of security flaws (BEAST, POODLE)

### Defined

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL 1.0</td>
<td>n/a</td>
</tr>
<tr>
<td>SSL 2.0</td>
<td>1995</td>
</tr>
<tr>
<td>SSL 3.0</td>
<td>1996</td>
</tr>
<tr>
<td>TLS 1.0</td>
<td>1999</td>
</tr>
<tr>
<td>TLS 1.1</td>
<td>2006</td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>2008</td>
</tr>
<tr>
<td>TLS 1.3</td>
<td>TBD</td>
</tr>
</tbody>
</table>

**Is it SSL or TLS?**

TLS is used in practice but the term SSL has stuck around and is used interchangeable to refer to TLS.
ENCRYPTION — PROTECTION AGAINST EAVESDROPPING

- **Symmetric Key Encryption**
  - Same key for both encryption/decryption
  - Advanced Encryption Standard (AES), BlowFish are popular algorithms

- **Asymmetric Key Encryption**
  - Public Key Encryption (involves both Public/Private Key)
  - One key for encryption and second related key for decryption
  - RSA (Rivest, Shamir & Adleman), Diffie-Hellman

- Asymmetric has high computational cost (takes longer, more CPU)
MESSAGE DIGEST - PROTECTION AGAINST TAMPERING

- Data loss from communication problems or tampering
- Generates a secure hash for the data
- Hash is a fixed length value generated from the data
- Hash value will change if data changes

MD5, Secure Hash Algorithm (SHA-1, SHA-2)

```
SHA1("The quick brown fox jumps over the lazy dog")
gives hexadecimal: 2fd4e1c67a2d28fcad849ee1bb7667391b93eb12

SHA1("The quick brown fox jumps over the lazy dog")
gives hexadecimal: de9f2c7fd5e1b3afad3e85a0bd17d9b100db4b3
```
CERTIFICATES - SSL AUTHENTICATION

- Certificates are digital signatures issued by trusted 3rd parties called Certificate Authorities.
- Multiple CAs
  - Verisign, COMODO, GoDaddy, etc.
- Certificate Issued by CA (send a CSR, install signed certificate on your server)
- Certificates linked to Root CA
MULTIPLE TRUSTED ROOT CERTIFICATE AUTHORITIES
SSL HANDSHAKE

- Protocol Version
- Cryptographic Algorithm
- Authenticate using Certificate
- Generate a shared secret key via asymmetric encryption
- SSL/TLS then uses the shared key for symmetric encryption of messages for the session
SSL HANDSHAKE – WIRESHARK CAPTURE

Encrypted Data over SSL connection

Port 443 HTTP over SSL “HTTPS”
WHAT IS VPN?

- Virtual Private Network
- Involves creating a secure connection, called VPN Tunnel, between computers/networks
- Encrypted Data flows over the VPN Tunnel
- Any type of data can be sent over the VPN tunnel
- Server/Client(s)
USES OF VPN?

- Connect Corporate Networks securely over the internet
- Provide secure access to corporate networks for remote users
- Data privacy while using Open Wi-Fi networks (Panera, Starbucks)
- Commercial VPN services (hide traffic, data collection by ISPs, location based services)
TYPES OF VPN

- PPTP-based VPN
- IPSec-based VPN
- SSL-based VPN
PPTP – POINT-TO-POINT TUNNELING PROTOCOL

- Oldest VPN Protocol
- Uses TCP port 1723 for control channel to setup the connection
- Different channel for Data transport over GRE protocol (port 47)
- PPTP Client is available on most Operating Systems (Windows/Linux/Unix/iOS/Android)
- Considered insecure due to the CHAP authentication.
- Can use Digital certificates with Extensible Authentication Protocol (EAP-TLS)
IPSEC – INTERNET PROTOCOL SECURITY

- Operates on the network layer of the OSI model
- Two Modes of Operation – Tunneling/Transport
- Control Channel (UDP port 500 or 4500)
- Transport channel using Encapsulated Security Payload (ESP) over port 50
- Very flexible and powerful, setup different security policies. Hard to configure/troubleshoot
- Different Vendor implementations
- Kernel Mode
SSL-BASED VPN

- Use SSL/TLS protocol
- Good for access to Web Applications via web browsers
- No client software needs to be installed
- Browser Plugins for enhancements
- Limited Ability
OPENVPN

- Uses SSL/TLS protocol to secure the connection
- Uses a Virtual Network Adapter (tun or tap) to interface between the OpenVPN Software & OS
- Open Source Software
- Runs on Windows/Linux/Unix/Solaris/BSD/ Android/Mac OS/Android/iOS
- User mode /Portable
- OpenVPN software needs to be installed
OPENVPN

- Uses control channel and data channel
- Both channels use the same port (UDP 1194)
- Uses OpenSSL libraries to provide encryption, authentication functions.
- Flexible – use pre-shared key (server/client) or Public key (server/multiple clients)
- Choose cipher, key size or digest
- OpenVPN v1.x, 2.x (up to 2.4)
OPENVPN

- Firewall rules can be applied to the VPN Virtual interface for access control
- Works in NAT’ed or DHCP environments
- Create secure Ethernet bridges using TAP adapter.
- *Tunnel an entire IP subnet or a virtual Ethernet adapter over a single UDP or TCP port*
REMOTE ACCESS VIA FIREWALL/ROUTER

- Port Forwarding
- Different Ports needs to be forwarded for different services.
  - SSH 22, Telnet 23, HTTP 80, HTTPS 443
- A port forward only provides access to one service on a single device
- Opening multiple ports in firewall is not secure
- Data may not be encrypted (Telnet, HTTP)
OPENVPN SETUP

- Routed or Bridged Mode
  - Routed offers better access control and is easier to setup
  - Bridged mode used if handling non-IP protocols, running applications which require broadcasts using single subnet across the tunnel
- Decide on IP address Ranges to use
- Setup a Public Key Infrastructure (PKI) to generate certificates and keys for the server and clients
- Server and Client Configuration Files
PUBLIC KEY INFRASTRUCTURE (PKI)

- Setup your own Certificate Authority (CA)
- Generate master CA certificate and key
- A separate certificate (public key) and private key for the server and each client
- Server/client(s) certificates/keys are signed with the CA key.
# VITAL FILES FOR OPENVPN PKI

<table>
<thead>
<tr>
<th>Filename</th>
<th>Needed By</th>
<th>Purpose</th>
<th>Secret</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca.crt</td>
<td>server + all clients</td>
<td>Root CA certificate</td>
<td>NO</td>
</tr>
<tr>
<td>ca.key</td>
<td>key signing machine only</td>
<td>Root CA key</td>
<td>YES</td>
</tr>
<tr>
<td>dh[n].pem</td>
<td>server only</td>
<td>Diffie Hellman parameters</td>
<td>NO</td>
</tr>
<tr>
<td>server.crt</td>
<td>server only</td>
<td>Server Certificate</td>
<td>NO</td>
</tr>
<tr>
<td>server.key</td>
<td>server only</td>
<td>Server Key</td>
<td>YES</td>
</tr>
<tr>
<td>client1.crt</td>
<td>client1 only</td>
<td>Client1 Certificate</td>
<td>NO</td>
</tr>
<tr>
<td>client1.key</td>
<td>client1 only</td>
<td>Client1 Key</td>
<td>YES</td>
</tr>
<tr>
<td>client2.crt</td>
<td>client2 only</td>
<td>Client2 Certificate</td>
<td>NO</td>
</tr>
<tr>
<td>client2.key</td>
<td>client2 only</td>
<td>Client2 Key</td>
<td>YES</td>
</tr>
<tr>
<td>client3.crt</td>
<td>client3 only</td>
<td>Client3 Certificate</td>
<td>NO</td>
</tr>
<tr>
<td>client3.key</td>
<td>client3 only</td>
<td>Client3 Key</td>
<td>YES</td>
</tr>
</tbody>
</table>
OPENVPN CONFIG FILES

```bash
server 172.16.64.0 255.255.192.0
port 1194
proto udp
dev tun0
comp-lzo
keepalive 50 110
cert ccsiserver.crt
key ccsiserver.key
```

```bash
client
remote www.bascloudvpnserver.com 1194
proto udp
dev tun
comp-lzo
keepalive 50 110
cert ca.crt
key client1.key
cert client1.crt
```
OPENVPN ACCESS PERMISSIONS

- Access permissions are granted based on the configuration files
- Each client has a unique name called its Common Name (also present in certificate)
- Server pushes the routing information to the clients
- Setup client to server or client-to-client access
- Client can be an IP router, thereby providing remote access to LAN side devices securely
OTHER OPENVPN CONSIDERATIONS

● OpenVPN Server should be publicly accessible on the chosen port

● OpenVPN Server can be behind a firewall with Port Forwarding Setup

● If OpenVPN Server IP address assigned via DHCP, Dynamic DNS services required
MEDIATED VPN

- VPN Server is hosted on a server on the internet by a 3rd Party
- Connects clients together to form a VPN tunnel between them
- Provides customers certificates for their client devices and ability to setup access control
- No Server setup, no Public IP requirements, no port forwarding
- OpenVPN client can be a PC or a Router
SSL AND VPN

- **Similarity**
  - Provide Encryption, Authentication, Data Integrity

- **Differences**
  - SSL: useful for HTTPS on servers on the internet, SSL certificate on each device, Memory Constraints, Application Change
  - VPN: Flexible setup (server-client, server-clients, client-client), use a router/gateway device to provide VPN, devices behind the VPN remain hidden to Public Internet, no change in application required to add security
THANKS!

May 9, 2017