Security Protocols

S/MIME

S/MIME is the Secure/Multipurpose Internet Mail Extensions, also known as S/MIME. It's a standard that provides cryptographic security for electronic messaging, things like email. Now, when we talk about S/MIME, it is built into most email clients you're going to use. So, if you're using Apple Mail or Microsoft Outlook or even Gmail, it has the capability to support S/MIME. S/MIME is going to use separate session keys for each email message that's being sent or received. We can use digital IDs within Outlook or digital signatures within many different programs to give our emails authentication, integrity, and non-repudiation through S/MIME.

Now, S/MIME is a way that we can encrypt our emails and their content. The problem with that is it also encrypts all of their contents, including malware. So, if I wanted to send you an email and I was going to encrypt the content, and I put a piece of malware in there and encrypted it and sent it to you, guess what? Your boundaries may not detect it. Your filter may not detect it because it's going through encrypted, and if they don't have access to your private key to decrypt it, they're not going to be able to see it and protect you from it. So, how do you overcome this? Well, a lot of email gateways will actually load up the user's private key so, they can decrypt the emails, look at the contents, make sure they're safe, and then pass them on to the user. Again, though, if you're giving up your private key, that can reduce the security of the system.

SSL/TLS

Well, SSL stands for the Secure Socket Layer and TLS stands for Transport Layer Security. These are cryptographic protocols that provide secure Internet communications for web browsing, instant messaging, email, VoIP, and many other services. I know we talk a lot about it in web browsing, but it can be used for all of these other things, too. Now, when we talk about SSL and TLS, let's start with SSL because it's the older protocol. SSL was what was created first. It was a way to start securing the web as we wanted to start doing ecommerce. The last time SSL was updated, though, was 1996 with SSL version three. It's really old. You shouldn't use SSL. Instead, it's been replaced by TLS, Transport Layer Security. Now, everyone watching this should be using TLS version 1.3, which is the latest and greatest right now as of this filming. Now, often you're going to hear people call it SSL even if it's

TLS that you're using. This is just something that people call incorrectly because it's a creature of habit.

Downgrade Attack

A downgrade attack is when a protocol is tricked into using a lower quality version instead of using the higher quality version that it was supposed to.

SSH

SSH or Secure Shell is another protocol that we often use to tunnel other protocols through. Secure Shell is a protocol that we can create a secure channel between two computers or network devices and this allows one device to actually take control over another device. So, if I wanted to connect my laptop to a server so that I can do remote execution of commands as a system administrator, I would use Secure Shell to do that. Basically, Secure Shell was designed as a replacement for Telnet because Telnet, we've already said, is bad. Telnet sends everything in the clear and unencrypted. SSH, on the other-hand, allows us to have this nice encrypted tunnel that protects our data. SSH was originally used in Unix and Linux, but now, you're finding it in Windows, as well. It is very heavily used as a text-based remote control method for anything that you need to be able to get into and do remote control of, things like routers and switches, you Telnet into them to get to their command line and be able to set up commands.

The earlier versions, version 1 and 1.5, had issues with unauthorized insertion of content, improper forwarding of those secure connections to other servers, and integer overflow issues. But all of that was fixed, thankfully, in SSH version 2. Version 2 also added Diffie-Hellman for secure key exchanges and the use of MACs, which are Message Authentication Codes, and this provides us integrity checking of the data as it's being transferred over the network. This makes SSH a great tool for us and something that we heavily, heavily use as security administrators and network administrators.

VPN Protocols

PPTP

This is a protocol that encapsulates PPP packets and ultimately sends data out as encrypted traffic. Now, what is PPP? PPP is the Point-to-Point Protocol, and it was originally used for dial-up connections, but it's used in combination with the PPTP protocol over Port 1723 to allow servers and devices to connect over a wide area network like the Internet. Now, PPTP uses CHAP-based authentication, and that makes it vulnerable to attack. If you're going to use PPTP for your VPNs, you should always require a strong authentication mechanism be used, instead, something like EAP-TLS, like we've talked about before. This is going to rely on PKI and digital certificates for stronger authentication. Otherwise, you should look at something like L2TP or IPSec.

L2TP

L2TP is the Layer 2 Tunneling Protocol. This is going to give you a connection between two or more computers or devices that aren't on the same private network. Notice, here I didn't use the word secure. That is because L2TP is not secure on its own and it provides no encryption and no confidentiality by itself. Instead, we usually are going to pair it with IPSec to provide that security. IPSec is going to provide us with the encryption and confidentiality while we're using L2TP, and this is going to enable us to use things like PKI with L2TP if we're using Windows Servers as part of that authentication process. L2TP is used over Port 1701 as you may have remembered from our Ports and Protocol lesson.

IPSec

Now, IPSec is a TCP protocol that authenticates and encrypts IP packets effectively, securing those communications between computers and devices using the protocol. This is going to create a nice secure tunnel for us that we can send our traffic and create our VPNs across. This is what we use heavily inside of VPNs. Now, when we talk about IPSec, IPSec is going to provide us confidentiality by giving us encryption. It's going to provide integrity for us by using hashing and it's going to give us authentication by performing a key exchange.
When we talk about that key exchange, it's known as IKE, the Internet Key Exchange. This is a method that's used by IPSec to create a secure tunnel by encrypting the connection between authenticated peers. This can occur in one of three ways. A Main mode, an Aggressive mode, or a Quick mode.

1. In Main mode, there are three separate exchanges that are going to occur.

2. When we use Aggressive mode, the key exchange is going to happen more quickly, but it still achieves basically the same result as Main mode but it only uses three packets.
3. If we decide to use Quick mode, only the negotiated parameters of the IPSec session are going to be handled. This key exchange occurs during the establishment of an IPSec tunnel in two different phases. So, let's take a look at how this happens.

SA

Well, a Security Association, or an SA, is an establishment of secure connections and shared security information using certificates or cryptographic keys. So, basically, it's you trust me and I trust you, we've shared information and now, we know each other and we've verified our identities.

AH

Now, the next thing we have to talk about is this concept of an Authentication Header, this is because the Authentication Header is a protocol using IPSec to provide integrity and authentication. The Authentication Header is actually hashed to provide that integrity and it's often used with an Encapsulating Security Payload known as an ESP.

ESP

An ESP is going to provide you integrity, confidentiality, and authentication for the packets by encapsulating them and encrypting them.

So, by using just the Authentication Header, we're going to get integrity and authenticity. But, if we use ESP as well, we’re going to get integrity, confidentiality, and authenticity. So, a lot of times we'll use both of them to get us a more secure tunnel.

Modes

When we talk about Transport mode, this is where there's a Host-to-Host transport mode using only encryption of the payload of an IP packet but not its header. And Tunnel mode is going to create an end-to-end network tunnel that's created, that's going to encrypt the entire IP packet, the payload, and the header.