Practical No. 14

Problem Definition: To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).

Learning Objectives:

1. Understand the concept and working of Encrypted mails

Theory

MIME (Secure/Multipurpose Internet Mail Extensions)

S/MIME allows users to send encrypted and digitally signed emails . This protocol allows recipients of the email to be certain the email they receive is the exact message that began with the sender. It also helps ensure that a message going to an outbound recipient is from a specific sender and not someone assuming a false identity.

How does S/MIME work?

S/MIME provides cryptographic-based security services like authentication, message integrity, and digital signatures. All these elements work together to enhance privacy and security for both the sender and recipient of an email.

S/MIME also works with other technologies such as Transport Layer Security (TLS) which encrypts the path between two email servers. The protocol is also compatible with Secure Sockets Layer (SSL) which masks the connection between email messages and Office 365 (a common email service) servers.

In addition, BitLocker works in conjunction with S/MIME protocol, which encrypts data on a hard drive in a data center so if a hacker gets access, he or she won't be able to interpret the information.

Benefits of encrypted email

1. Safeguards sensitive data

If you're sending information like your Social Security number over email, it's important that it's not easily stolen by hackers.

2. Economical

Instead of purchasing security equipment, you can simply rely on email encryption that's integrated directly on the server.

3. Timesaving

Instead of wasting time using several programs to make sure a connection is secure, you can rely on email encryption to do most of the work for you.

4. Regulation compliance

If you work in the healthcare industry, for example, and you haven't taken the right steps to secure medical data, you could be in violation of HIPAA laws [6]. Encryption helps you avoid those missteps.

5. Protects against malware

Malicious emails sometimes contain viruses masked as innocent email attachments. If you or someone else send an attachment using encrypted email, the email has a digital signature to prove its authenticity.

How does email encryption work?

If you don't want anyone but the receiver to see the contents of a message, encryption is vital. To the outsider, an encrypted email will have a bunch of random letters, digits, or symbols

instead of readable text. The person with the private key to decrypt it, typically the receiver, will be able to read the email as usual.

There are generally three encryption types available:

- S/MIME encryption works as long as both the sender and recipient have mailboxes that support it. Windows Outlook is the most popular version that works with this method. Gmail uses it as well.
- Office 365 Message Encryption is best for users with valid Microsoft Office licenses who can use this tool to encrypt the information and files sent via email. It's also a top choice for Outlook users
- PGP/MIME is a more affordable and popular option that other email clients may prefer to use. It's reliable and integrated into many of the apps we use today

Other email products may have their own brand of encryption, but the science behind it is the same. Only senders and recipients who have exchanged keys or digital signatures can communicate within the encrypted network.

How to send encrypted email in Outlook

Encrypting email may sound complicated, but it's not. Microsoft has a reputation for providing its users with simple ways to encrypt data, from files to folders to emails, too. It makes sense that they would include built-in tools for Outlook, their proprietary email

system. You don't need a separate software tool or plug-in to start sending secure messages. Just follow these steps to begin.

1. Create a digital certificate

For Outlook users, encrypting a single email is simple. First, you must have a digital signature. To create a digital signature:

1. Start in your Outlook window and click on the File tab
2. Select Options, then Trust Center, then Trust Center Settings
3. Select Email Security, Get a Digital ID
4. You'll be asked to choose a certification authority. This is entirely up to you as most are rated the same
5. You'll receive an email with your digital certificate/ID included
6. Go back into Outlook and select Options and the Security tab
7. In the Security Settings Name field, type in a name of your choosing
8. Ensure that S/MIME is selected from the Secure Message Format box and that Default Security Settings is checked as well
9. Go to Certificates and Algorithms, select Signing Certificate, and click Choose
10. Make sure the box is checked next to Secure Email Certificate, and check the box next to "Send These Certificates with Signed Messages"
11. Click OK to save your settings and start using Outlook

2. Use your digital signature

Now that you have a digital ID, you need to start using it:

1. Open a new message to access the Tools tab
2. Click that, then Customize, and finally the Commands tab
3. From Categories, select Standard
4. From Categories, select Digitally Sign Message

3. Encrypt Outlook messages

You can now send encrypted messages to a recipient with the next steps.

1. Open the window to compose a new message and select the Options tab, then More Options
2. Click the dialog box (triangle with arrow pointing down) in the lower-right corner
3. Choose Security Settings and check the box next to Encrypt message contents and attachments
4. Write your message as normal and send

After you've sent and received a message that you've both signed and encrypted, you don't have to sign it again. Outlook will remember your signature.

4. Encrypt all Outlook messages

You can encrypt each one, or you can use the steps below to encrypt all outgoing messages in Outlook:

Open the File tab in Outlook

Select Options, then Trust Center, and Trust Center Settings

From the Email Security tab, select Encrypted email

Check the box next to Encrypt content and attachments for outgoing messages

Use Settings to customize additional options, including certificates

How to Send Encrypted Email

Have you ever wondered about the security of your private email conversations? Whether at work, school, or home, sending emails comes with a bit of a risk. There's one thing you can do to discourage data breaches and attacks on your sensitive data, however. Use encrypted email. Learn how to practice this common-sense method for communicating in

our step-by-step guide. But first, let's look at why you should embrace encryption for your email correspondence.

How to Encrypt Email and Send Secure Messages

Emails sent over an open network can be intercepted and malicious actors can see email contents, attachments, or even take over your account.

To drive home the importance of email security, take a look at some alarming statistics that show the widespread cybersecurity issues that may have affected you in the past and still pose a threat today:

In 2016, 3 billion Yahoo accounts were hacked

According to research by cyber security company, Symantec, emails with a malicious URL make up a total of 12.3% of all emails

As these numbers illustrate, emails are a point of vulnerability for many unsuspecting users. However, it's not all doom and gloom, there are ways to protect yourself and your information.

To help safeguard against hackers and ensure your privacy is maintained, you can use encryption. Encryption ensures that your emails remain unreadable, even if they fall into the wrong hands.

Conclusion: Thus we have studied the steps for implementation of S/MIME protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).

Signature with date