



Bringing British
Education to You
www.nccedu.com

Network Security and Cryptography

*Topic 4:
Email Security*



Bringing British
Education to You
www.nccedu.com

Network Security and Cryptography

*Topic 4 – Lecture 1:
Email Security Threats*

Scope and Coverage

This topic will cover:

- Email security threats
- Email security solutions
- PGP
- S/MIME

Learning Outcomes

By the end of this topic students will be able to:

- Describe email security mechanisms
- Digitally sign an email

Importance of Email

- Business has come to rely on email as a means of communication:
 - fast
 - cost-effective
 - easy collaboration and information-sharing
- Email has become the primary method for corresponding with colleagues, customers, and business partners

Email Security Threats

- Viruses can corrupt mission-critical documents and applications
- Hackers will try to obtain confidential information
- Spam can greatly deteriorate the performance of other components within the communications infrastructure
- Threats can stop business systems and mission-critical activities

Viruses

- Viruses are very sophisticated and often appear to be harmless correspondence:
 - personal communication
 - jokes
 - marketing promotions
- Most viruses require recipients to download attachments in order to spread
- Some are designed to launch automatically, with no user action required

Protection from Viruses

- Email security solutions offer highly advanced virus protection:
 - automatically scan all incoming and outgoing messages
 - automatically scan all attachments
 - automatic update capabilities
- New threats emerge all the time and updates offer protection from all the latest threats

Spam

- A large proportion of all corporate email is spam
- Spam costs US business billions of dollars in lost productivity and system slow-downs annually
- Most spam is annoying and slows down the network
- Hackers may sometimes disguise viruses, spyware, and malware as innocent-looking spam

Protection from Spam

- Email security packages usually **contain spam filters** that:
 - Identify **non-relevant communications**
 - Use **key words** and **phrases**
 - May also use **format**, **size**, or **ratio of graphics to text**.
 - Spam is moved to a separate folder or deleted from email server
 - May also **block email addresses** that are known to have sent spam, preventing further disruptive emails

Phishing

- Used for identity theft and fraud
- Posing as authorised emails from trustworthy institutions
- Attempt to get recipients to surrender personal information such as bank account details
- Most are aimed at individuals
- Some have targeted smaller businesses

Protection from Phishing

- Email security packages provide **anti-phishing protection**
- Combination of methods:
 - Authentication
 - Detection
 - Prevention
 - Reporting
- Enables **threat analysis**, **attack prioritisation** and response to minimise risk and impact of phishing

Spyware

- Enables hackers to record activities and data from the infected computer
- Done via a program that dynamically gathers information and transmits it via an Internet connection
- Often bundled in with shareware and freeware programs
- Usually installs and runs without user knowledge

Protection from Spyware

- **Firewalls alone are insufficient**
- Email security packages will scan devices regularly for spyware programs
- Blocks known spyware programs before they can be downloaded and installed

Email Authentication

- Aims to provide enough information to the recipient so that **they know the nature of the email**
- A valid identity on an email is a vital step in stopping spam, forgery, fraud, and other serious crimes
- **SMTP was not designed with security in mind and thus had no formal verification of the sender**
- **Signing emails identifies the origin of a message, but not if it should be trusted**

Authenticating Source IP Address

- TCP allows an email recipient to automatically verify the message sender's IP address
- This does not verify the identity of the sender
- Forged headers can be used to create a spam message that appears to be real
- The sending IP address may belong to a zombie machine under the control of a hacker

Blacklisting IP Addresses

- The IP addresses originating spam and phishing emails can be blacklisted so that future email from them is not received but either quarantined or deleted
- **Many IP addresses are dynamic**
 - Change frequently
 - An organisation has a block of IP addresses
 - IP addresses are allocated when needed
 - May get a new address every time a connection is made
- Therefore, **spammer will not have a permanent IP address**

Controlling Traffic

- Some ISPs use techniques to prevent spamming by their customers:
 - Port 25 can be blocked so that port 587 is used and that requires authentication
 - Limiting the number of received headers in relayed mail
 - Infected computers can be cleaned and patched
 - Outgoing email can be monitored for any sudden increase in flow or in content (a typical spam signature)

Other Email Threats

- So far we have not even mentioned the following issues:
 - Sensitive information **transmitted unencrypted between mail server and client may be intercepted**
 - All popular email communication standards default to **sending usernames, passwords, and email messages unencrypted**
 - Information within email messages **may be altered** at some point between the sender and recipient

Securing Email Content

- The next lecture deals with securing the content of email
- It will include the techniques for:
 - Digitally signing an email
 - Encrypting the content of an email
 - Encrypting the header of an email



Bringing British
Education to You
www.nccedu.com

Network Security and Cryptography

*Topic 4 – Lecture 2:
PGP and S/MIME*

Cryptography in Email Systems

- Cryptography can be used in email to:
 - **Sign an email message** to ensure its integrity and confirm the **identity of its sender**
 - **Encrypt the body of an email message to ensure its confidentiality**
 - **Encrypt the communications between mail servers to protect the confidentiality** of both the message body and message header

Digitally Sign & Encrypt

- **Signing a message and encrypting the body are often used together** to provide authentication and privacy
- When a message needs to be encrypted to protect its confidentiality, it is usually digitally signed
 - so that the recipient can ensure the integrity of the message and also verify the identity of the signer
- Digitally signed messages are usually not encrypted if the confidentiality does not need to be protected

Encrypting Transmission

- Encrypting the transmissions between mail servers is used only when two organisations want to protect emails regularly sent between themselves
- **The organisations could establish a virtual private network (VPN)** to encrypt the communications between their mail servers over the Internet
- **A VPN can be used encrypt entire messages including header information**
 - E.g. senders, recipients, subject lines

Individual Emails

- Most email messages are protected individually rather than along a secure VPN
- Each message is protected by **digitally signing** and **optionally encrypting** it
- Widely used standards for signing and encrypting message bodies are:
 - **Open Pretty Good Privacy (OpenPGP)**
 - **Secure/Multipurpose Internet Mail Extensions (S/MIME)**

OpenPGP

- A protocol for encrypting and signing messages and creating certificates using public key cryptography
- Based on an earlier protocol, PGP
- First released in June 1991
- The original PGP protocol used some encryption algorithms with intellectual property restrictions
- OpenPGP was developed as a standard protocol based on PGP Version 5

OpenPGP Algorithms

- A number of OpenPGP based products fully support cryptographic algorithms recommended by NIST including:
 - 3DES and AES for data encryption
 - Digital Signature Algorithm (DSA) and RSA for digital signatures
 - SHA for hashing
- Other implementations of OpenPGP support other encryption schemes

OpenPGP Cryptography

- OpenPGP use **both** public key cryptography and symmetric key cryptography
- **Public key cryptography is used to create digitally signed message digests**
- **Encryption of the message body** is performed using a **symmetric key algorithm**

OpenPGP – Signing & Encrypting - 1

- The plaintext is **compressed**
- A **random session key** is created
- A **digital signature** is generated for the message using the **sender's private key** and then added to the message
- The **message and signature are encrypted** using **the session key and a symmetric algorithm**

OpenPGP – Signing & Encrypting - 2

- The session key is encrypted using the recipient's public key and added to the encrypted message
- The encrypted message is sent to the recipient
- The recipient reverses these steps

Using OpenPGP

- Many popular mail clients require the installation of a plug-in in order to operate OpenPGP, e.g.:
 - Mozilla Thunderbird,
 - Apple Mail
 - Microsoft Outlook
- There are a number of OpenPGP distribution websites that contain instructions on how to use OpenPGP with various mail client applications

MIME

- **Multipurpose Internet Mail Extensions** - an Internet standard that extends the format of email to support:
 - Text that uses character sets other than ASCII
 - Attachments that are not text based
 - Message bodies with multiple parts
 - Header information in non-ASCII character sets

S/MIME

- Secure/MIME is a version of the MIME protocol
- It supports encryption of email messages and their contents via **public-key encryption technology**
- Created in 1995 by a group of software vendors **to prevent interception and forgery of email**
- Builds **on the existing MIME protocol** standard
- Is easily integrated into existing email products

S/MIME Functions

- Provides **cryptographic security services** for electronic messaging applications, including:
 - **Authentication** (via digital signatures)
 - **Message integrity** (via digital signatures)
 - **Non-repudiation of origin** (via digital signatures)
 - **Privacy** (using encryption)
 - **Data security** (using encryption)

S/MIME Interoperability

- Based on **widely supported standards**
 - likely to continue to be widely implemented across a variety of operating systems and email clients
- **Is supported by many email clients** and can be used to securely communicate between them
 - Not always simple
- For example, a Windows operating system user with the Outlook email client can send a secure, digitally signed email to a Unix operating system user without installing any additional software

S/MIME Certificates

- An individual key/certificate must be obtained from a Certificate Authority (CA)
- Accepted best practice is to use **separate private keys for signature and encryption**
 - permits escrow of the encryption key without compromise to the non-repudiation property of the signature key
- Encryption requires having the destination party's certificate stored

S/MIME Process

- S/MIME-enabled mail clients **send messages in a similar way to OpenPGP**
- S/MIME version 3.1 supports **two recommended symmetric key encryption algorithms:**
 - AES
 - 3DES
- AES is considered a stronger algorithm than 3DES

Key Management

- OpenPGP and S/MIME use **digital certificates to manage keys**
- A digital certificate identifies:
 - the **entity that the certificate was issued to**
 - the **public key** of the entity's public key pair
 - other information, such as the **date of expiration**, signed by some trusted party
- There are differences in how the two protocols manage trust

Key Management in OpenPGP

- Uses the **web of trust** which has no central key issuing or approving authority:
 - The web of trust relies on the **personal decisions of users** for management and control
 - Suitable for **individual users and very small organisations**
 - **Unworkable** in **most medium to large organisations**
 - Some organisations deploy **keyservers** that users can access to get others' keys and store their own keys

Key Management in S/MIME

- Has a **hierarchical structure**:
 - Typically, there is a **master registration and approving authority**, the root Certificate Authority (CA), that issues a public key certificate for itself and any subordinate CAs
 - Subordinate CAs normally issue certificates to **users and also to any other subordinate CAs**
 - They in turn sanction to users and their subordinate CAs, forming a hierarchy
 - This public key infrastructure can be used to establish a chain of trust between two users holding valid certificates

Third Party Services

- Third-party services are available that allow organisations to exchange encrypted email
- Removes the need to establish trust relationships
- No worries about mail application compatibility
- But the use of such services means placing sensitive messages on third-party servers
 - This is also a security concern

References

- Stallings, W. (2010). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
- NIST (2007). *Guidelines on Electronic Mail Security*. NIST.

Topic 4 – Email Security

Any Questions?



Bringing British
Education to You
www.nccedu.com

