7 most popular email security protocols today

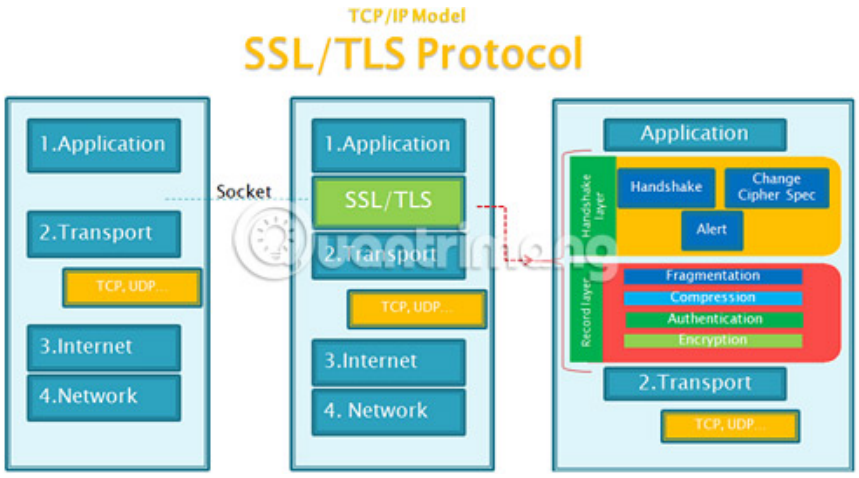
Email security protocols are structures that protect a user's email from outside interference. Email requires additional security protocols for a reason: Simple Mail Transfer Protocol (SMTP) does not have integrated security.

Email security protocols are structures that protect a user's email from outside interference. Email requires additional security protocols for a reason: Simple Mail Transfer Protocol (SMTP) does not have integrated security. A shocking news, right?

Many security protocols work with SMTP. Here are those protocols and how they protect your email.

Learn about email security protocols

1. How SSL / TLS keeps email safe



Secure Sockets Layer (SSL) and 'successor', Transport Layer Security (TLS), are the most popular email security protocols to protect email when it travels over the Internet.

SSL and TLS are application layer protocols. In Internet communications networks, the application layer normalizes communication for end-user services. In this case, the application layer provides a security framework (a set of rules) that works with SMTP (also the application layer protocol) to secure the user's email communications.

This part of the article will only discuss TLS because its precursor, SSL, has been discontinued since 2015.

TLS provides more privacy and security to 'communicate' with computer programs. In this case, TLS provides security for SMTP.

When the user's email application sends and receives mail, it will use Transmission Control Protocol (TCP - part of the transport layer and the email client using it to connect to the email server) to initialize 'handshake' with email server.

Handshake is a series of steps in which the email client and the email server confirm security and encryption settings, then start sending email. At the basic level, handshake works as follows:

1. Client sends 'hello' message, encryption types and TLS version compatible to Email Server (email server).

2. The server responds with TLS Digital Certificate and the server's public encryption key.

3. Client application verifies certification information.

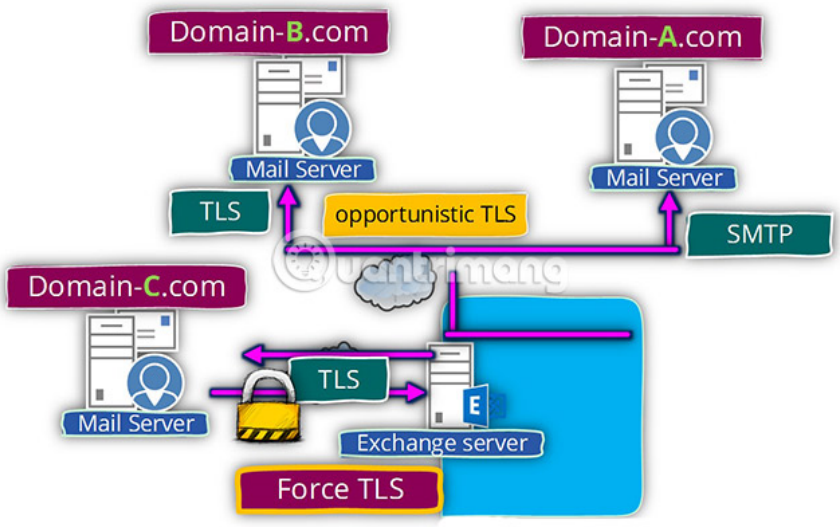
4. The client application creates Shared Secret Key (also known as Pre-Master Key) with the server's public key and sends it to the server.

5. The server decrypts the Secret Shared Key.

6. At this time, the client and server can use the Secret Shared Key to encrypt the data transmission, in this case the user's email.

TLS is very important because most email servers and email clients use it to provide basic encryption for users' email.

Opportunistic TLS and Forced TLS



Opportunistic TLS is a protocol command that informs an email server that a client email application wants to turn an existing connection into a secure TLS connection.

Sometimes, the user's email application will use pure text connection instead of following the above handshake process to create a secure connection. Opportunistic TLS will try to start the TLS handshake to create a 'tunnel'. However, if the handshake process fails, Opportunistic TLS will return to the plain text connection and send the email without encryption.

Forced TLS is a protocol configuration that forces all email 'transactions' to use secure TLS standards. If the email cannot be transferred from the email client application to the email server, then the email recipient will not be sent.

2. Digital Certificate

Digital Certificate is an encryption tool that can be used to secure email by password. Digital Certificate is a type of public key encryption.

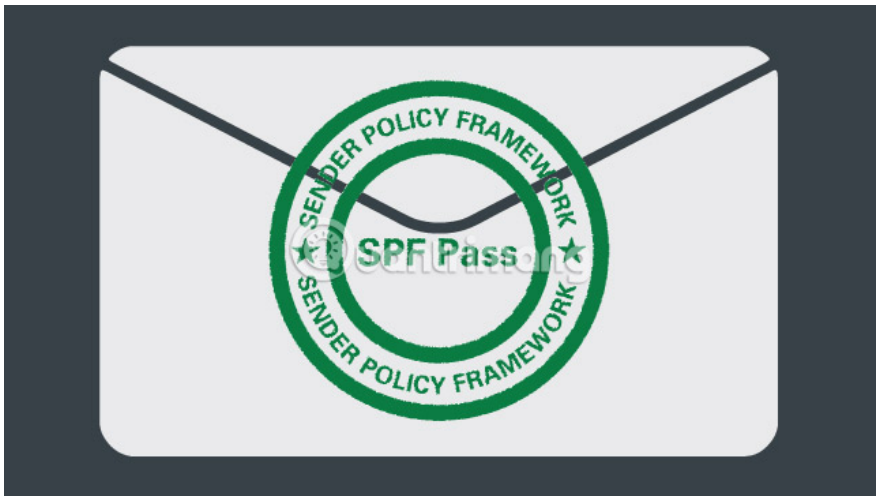
Authentication allows people to send you encrypted emails with predefined public encryption keys, as well as encrypting messages you send to others. Then, the Digital Certificate acts like a passport, bound to online

identity and the main use is to authenticate that identity.

When there is a Digital Certificate, the public key is available to anyone who wants to send encrypted messages to you. They encrypt their documents with your public key and you decrypt it with your private key.

Digital Certificate can be used for individuals, businesses, government organizations, email servers and almost every other digital entity to authenticate online identity.

3. Domain tampering with Sender Policy Framework



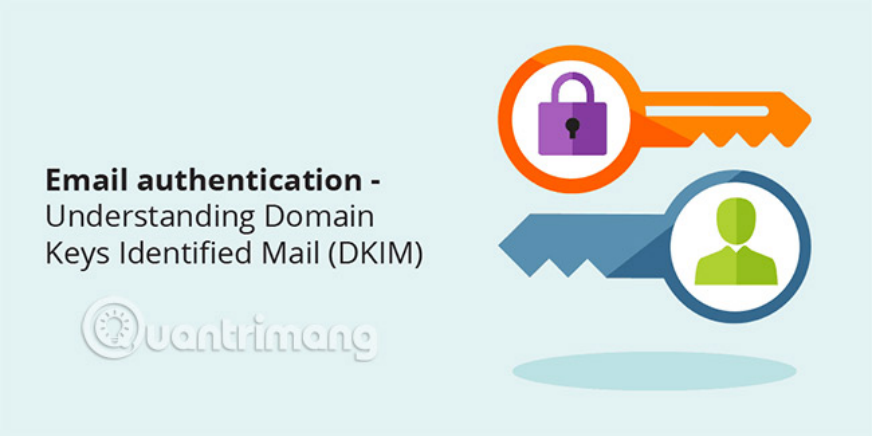
Sender Policy Framework (SPF) is a theoretical authentication protocol that protects against domain spoofing.

The SPF introduces additional security checks that allow the server to determine whether the message originated from the domain, or whether someone is using the domain to hide their true identity. Domains are part of the Internet with a unique name. For example, TipsMake.com is a domain.

Hackers and spammers often hide their domain when trying to invade the system or scam users, since the domain can trace the location and owner or at least see if the domain is in the list. black By spoofing a malicious email as a 'healthy' active domain, it is likely that users will not suspect when clicking or opening malicious attachments.

Sender Policy Framework has three core elements: Framework, authentication method and specialized email header for information transmission.

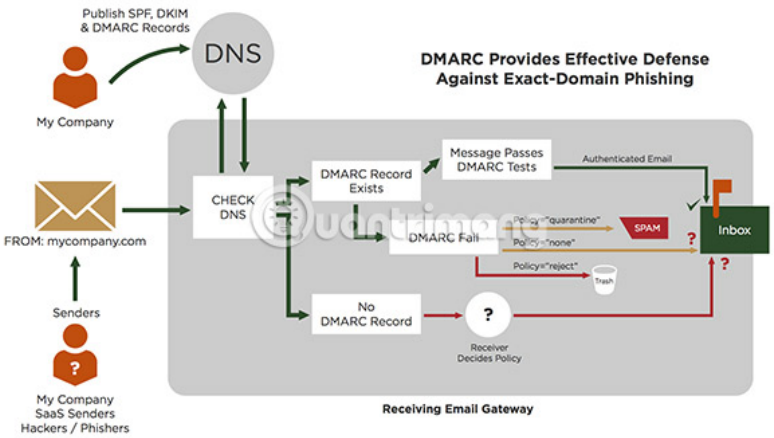
4. How DKIM keeps your email secure



DomainKeys Identified Mail (DKIM) is an anti-phishing protocol to ensure that sent messages are safe during transmission. DKIM uses digital signatures to check email sent by a specific domain. Moreover, it also checks whether the domain allows email. DKIM is an extension of SPF.

In fact, DKIM makes it easier to develop 'blacklists' and 'whitelists'.

5. What is DMARC?



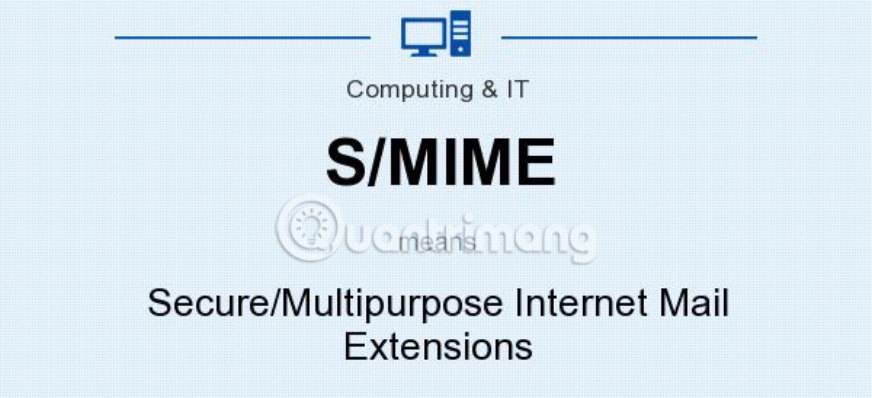
The next email security protocol is Domain-Based Message Authentication, Reporting & Conformance (DMARC). DMARC is an authentication system, validating SPF and DKIM standards to protect against fraudulent actions originating from a domain. DMARC is an important feature in the fight against domain fraud. However, the relatively low acceptance rate means that the fake status is still rampant.

DMARC works by preventing title spoofing from the user's address. It does this by:

1. Match the 'header from' domain to the 'envelope from' domain. Envelope from 'domain name is determined during SPF inspection.
2. Match the domain envelope from 'd = domain name' found in the DKIM signature.

DMARC guides an email provider on how to handle any incoming email. If the email does not meet the SPF test standard and validates DKIM, it will be rejected. DMARC is a technology that allows domains of all sizes to protect their domain names from tampering.

6. Terminal encoding with S / MIME



Secure / Multipurpose Internet Mail Extensions (S / MIME) is an age-old end-to-end encryption protocol. S / MIME encrypts the email content before it is sent, except for senders, recipients, or other parts of the email header. Only the recipient can decrypt the sender's mail.

S / MIME is deployed by the email application but requires Digital Certificate. Most modern email applications support S / MIME, but users will still have to check for specific support for their application and email provider.

7. What is PGP / OpenPGP?

Pretty Good Privacy (PGP) is another older end-to-end encryption protocol. However, more likely users have encountered and used its open source copy, OpenPGP.

OpenPGP is the open source version of the PGP encryption protocol. It gets updated regularly and users will find it in many modern applications and services. Like S / MIME, third parties can still access email metadata, such as sender and email recipients.

Users can add OpenPGP to their email security settings using one of the following applications:

1. Windows: Windows users should consider Gpg4Win.org.
2. macOS: MacOS users should check Gpgtools.org.

3. Linux: Linux users should choose GnuPG.org.
4. Android: Android users should check OpenKeychain.org.
5. iOS: iOS users choose PGP Everywhere. (pgpeverywhere.com)

OpenPGP implementation in each program is slightly different. Each program has a different developer who sets the OpenPGP protocol to use email encryption. However, it is all reliable encryption programs that users can trust to send their data.

OpenPGP is one of the easiest ways to add encryption on many different platforms.

Email security protocols are extremely important because they add a layer of security for users' email. Basically, email is very vulnerable to attack. SMTP has no security available and sends email in plain text (ie, without any protection and anyone who blocks it can read the content) is very risky, especially if It contains sensitive information.

Wish you find the right choice!

See more:

1. 7 tips to help secure email
2. 4 simple ways to secure Email
3. 8 best secure email services ensure your privacy