Transport Layer Security:

Its History, Limitations and How You Improve It and Email Security with Zix

By ZixCorp
www.zixcorp.com

The Vulnerability of Email

Email is core to daily business life. It enables efficient, real-time communication, unites businesses through a ubiquitous platform and improves collaboration with colleagues and business partners. Email continues to dominate business communication, with more than 883 million workers worldwide using email for business.

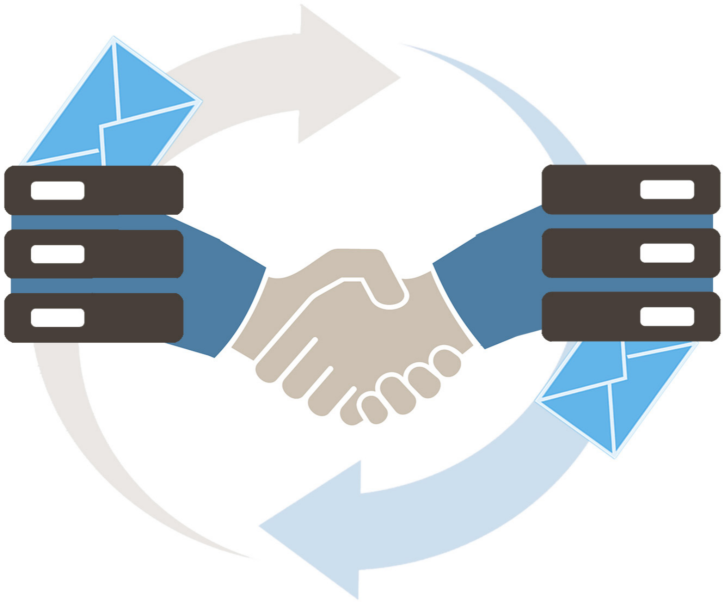
While email or simple mail transfer protocol (SMTP) traffic presents many benefits, it also introduces security and compliance challenges. Email is as unsecure as a postcard traveling through the mail service. Without the proper security measures in place, it's easy for an unauthorized person to capture data in email as it travels across the Internet. A simple method of managing the risks associated with sensitive email is to implement email encryption. Encryption makes the contents of every email, both the message text and any attachments, indecipherable to unauthorized individuals. Encryption uses complex algorithms to convert the original email content into an information package that cannot be read until the intended recipient unlocks the message. As a practical matter, if an unauthorized individual intercepts a copy of an encrypted email while it is moving across the Internet, they simply will not be able to read it.

Without the proper security measures in place, it's easy for an unauthorized person to capture data in email as it travels across the Internet.

As an alternative, many organizations try to reduce the risks of email by turning to a technology known as transport layer security (TLS). TLS is a protocol that's designed to provide privacy for email and is an effective technology when used for point-to-point communication. When a sender organization's server and the recipient organization's server communicate, TLS can (if implemented correctly) ensure that no third party may eavesdrop or tamper with any message.

HOW TLS WORKS

To initiate a secure connection, the TLS "handshake" protocol allows the sender and recipient servers to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. The steps to implement this protocol include:



1. Each company's email gateway is configured to enable TLS communication for email traffic
2. When the sender's server connects to the recipient's server, the sender checks whether TLS services are offered
3. If the recipient has TLS enabled, it initiates a TLS "handshake" by sending its TLS certificate to the sender
4. If the sender trusts the certificate of the recipient, a TLS session encryption key is negotiated
5. The TLS session starts, and the email message is transmitted.

TLS can offer the sender's organization some security, however this alternative has limitations and risks.

METHODS AND IMPACT

Traditionally, TLS is implemented through two methods – Mandatory and Opportunistic. Mandatory TLS requires a TLS connection be present before sending an email. If a TLS connection cannot be ensured on the recipient end, then the email is bounced. To establish reliable connections, security administrators at both ends of each desired connection must commit to correctly establishing security settings, managing encryption certificates and maintaining the ongoing health of those components through adds, changes and upgrades. Mandatory TLS is the safer method of the traditional two options. However, the commitment is cumbersome, costly and time consuming.

Opportunistic TLS, or unmanaged TLS, does not have the time or resource costs of Mandatory TLS. However, it introduces significant security and compliance risks. In Opportunistic TLS, servers are configured to try to send the email via TLS, but if TLS is not available, the email messages are still sent in the clear, allowing anyone to intercept the sensitive information contained in the message. Also, most opportunistic TLS will accept any level of authentication and encryption, including self-signed certificates and 64-bit encryption.

Mandatory TLS is cumbersome, costly and time consuming. Opportunistic TLS introduces significant security and compliance risks.

Regardless of the sender methods used in Opportunistic TLS or Mandatory TLS, neither option can ensure secure reply. It's not always possible for the sending organization to ensure the receiving organization has forced TLS for the response to a message. In fact, in many cases, the reply to a secure message is sent in the clear and includes the content of the original message - thereby defeating the purpose of secure email.

In addition, TLS is a point-to-point transport technology that is unable to span multiple SMTP hops between two points. This is due to the fact that the security is at the SMTP Transport level and not at the Mail Application Level, creating workflow issues when securing an email exchange with multiple organizations.

ENHANCING TLS

When TLS is the preferred email security method, Zix provides you with superior TLS support. By integrating it directly into ZixGateway® encryption policies and the Zix Best Method of Delivery® you benefit from exclusive enhancements, including:

- ## Secure, bidirectional transparency

  The Zix Best Method of Delivery chooses the most secure and transparent delivery method available for each message. Zix S/MIME provides high security and bidirectional transparency, enabling the decryption of the message at the gateway and delivering it to the recipient without need for a password or extra steps. If S/MIME is not available, TLS can be configured as an alternative transparent delivery method.

- ## Simplified set-up of mandatory TLS

  By making TLS a part of the email encryption policies, TLS can be added as a delivery method by simply checking a box. By replacing the need for individual TLS configurations, ZixGateway allows your organization to skip the cost and time typically associated with each connection.

- ## Increased delivery control

  No longer is TLS an all-or-nothing method. By making TLS a part of the ZixGateway policies, TLS is used only where appropriate. If a TLS connection breaks, Zix also provides a fallback secure delivery method.

- ## Reporting capabilities

  ZixGateway offers superior visibility for compliance officers by providing reports that log how each message was delivered, including TLS encrypted email, and to whom it was delivered.

- ## Security Branding

  Embedded at the top of each TLS message is a “Secured by Zix” banner, providing confidence to your recipients that the email and its sensitive content were delivered securely.

No competing solution can provide the security, simplicity, control, transparency, visibility and branding that is delivered through Zix.

WHY IS ZIX BETTER?

When an email is sent, the message is scanned for sensitive content with the robust and customizable content filters available in ZixGateway. When security is required, the Zix Best Method of Delivery ensures that email messages containing private or sensitive information are delivered in the most secure, easiest manner for the recipient, beginning with S/MIME delivery. When a TLS encryption option is indicated and supported, the email is delivered securely through the TLS delivery method.

For recipients who do not support S/MIME or TLS delivery, Zix offers two different delivery methods – ZixPort® and ZixDirect™. ZixPort is a pull technology that provides a mobile-friendly, secure Web portal for delivering sensitive information to customers and partners. It can be branded and integrated into your corporate portal and also supports secure compose so customers and partners can initiate and securely send a new inbound message. ZixDirect is a push technology that delivers encrypted email directly to user inboxes.

No competing solution can provide the security, simplicity, control, transparency, visibility and branding that is delivered through Zix.

THE ADVANTAGES OF ZIX EMAIL ENCRYPTON

TLS is second in the Zix Best Method of Delivery, because S/MIME through the Zix Encryption Network provides you with broader value and is fundamentally more secure, private and reliable than a collection of independent TLS connections.

Zix Encrypted Network is the industry's largest shared community of email encryption users and includes more than 14,000 business customers. By connecting Zix users in one community, we deliver unrivaled email security with:

- **Reliable Send and Return Path Protection**
  Both the forward and return paths between every pair of ZixGateway endpoints are encrypted, fully protecting network members' replies. Through automatic encryption and decryption at ZixGateway endpoints, 100 percent of messages are encrypted between organizations in the Zix Encryption Network, adding greater peace of mind for management without impact at the user level.

- **Setting and Certificate Automation**
  All protective endpoint settings and encryption certificates are actively maintained as part of the continuous operation of the Zix Encryption Network. Adds, changes and removals of other members is managed by Zix, enabling customers to reallocate resources to other business objectives.

- **Flexible Policy Controls**
  Under policy control, other encryption-based private delivery mechanisms like push, pull or TLS (for recipients outside the Zix Encryption Network) can be included into each customers' private communications framework to meet custom delivery needs based on message contents or destination characteristics. In addition, if TLS breaks, Zix can compensate by enabling fallback to an alternative secure delivery method. .

- **Security Branding**
  The technology that delivers security branding for TLS messages also offers branding for encrypted messages delivered through the Zix Encryption Network, providing continued confidence that the sensitive information they received was properly protected.

- **Reporting**
  The encryption decisions and visibility of the cryptographic processes exist at the application level. As a result, ZixReporting accurately tracks encryption type for every message, providing management feedback and a protection audit trail with an appealing graphic interface and no requirements to search or scrape logs.

- **Monitoring**
  In the event that something is irregular or goes wrong and may interfere with a transmission path or logic flow in the Zix Encryption Network, alarms are triggered and automatic maintenance immediately drives correction.

A RELIABLE EMAIL SECURITY STRATEGY

Within the strategic plan to protect your organization from a data breach, Zix Email Encryption is the most secure, reliable and easy-to-use solution. It eliminates the inherent risks of email and avoids limitations and risks of TLS. If your organization is considering TLS as an additional component of your email security strategy, reduce the disadvantages of mandatory and opportunistic TLS by leveraging the unrivaled benefits of superior TLS with Zix.

	Mandatory TLS	Opportunistic TLS	TLS with Zix
Simple configuration & maintenance		✓	✓
Secure delivery	✓		✓
Increased delivery control			✓
Reporting for increased visibility & compliance			✓
Security branding for peace of mind			✓