Emails in Silent Danger

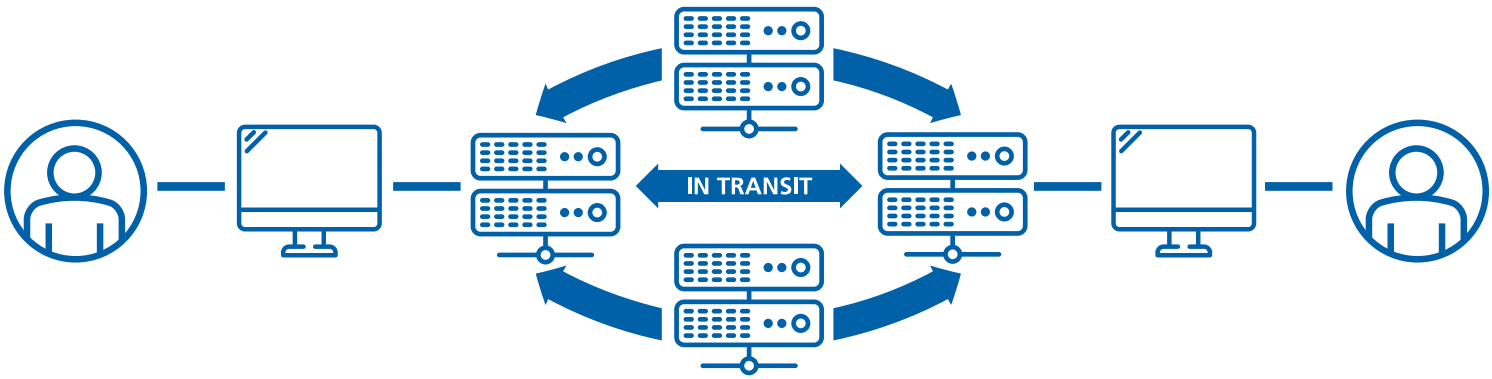
SMTP Proposals Take Aim at Prominent TLS Security Gaps

By: Cathy Kingeter, Senior Product Marketing Manager for Zix Corporation
Published December 2016

Focus on Securing Emails "In-transit"

Email is the heartbeat of business communications with more than 883 million workers worldwide using email for business. But, did you know that email is inherently insecure? When you send an email, your company's and customers' confidential information could be eavesdropped on, potentially intercepted and setup for malicious attack – all without your knowledge. Email breaches often go undetected, and the dangers are not evident until the damage is done. As evidenced by recent compromises experienced by Yahoo!, Democratic National Convention, Hillary Clinton and Colin Powell. In some cases attacks went undetected for years, while attackers lurked waiting for incentives to reveal their spoils.

How do businesses combat threats to email security? A comprehensive approach is required as every email is susceptible to multiple danger points where it can be compromised by an attacker. On the user's machine as a message is composed and stored, between sending email client and sending email server, in-transit as message traverses the internet, and finally as email travels from receiving mail server to recipient users device. Happening in seconds, it can be an extended journey with multiple stops. While security risks are at every stage, the most insecure phase is after the email has left your network and is in-transit over the internet. Here attacks are not visible to your security monitors and tools, leaving email content and attachments vulnerable to attack. Encryption is the answer.



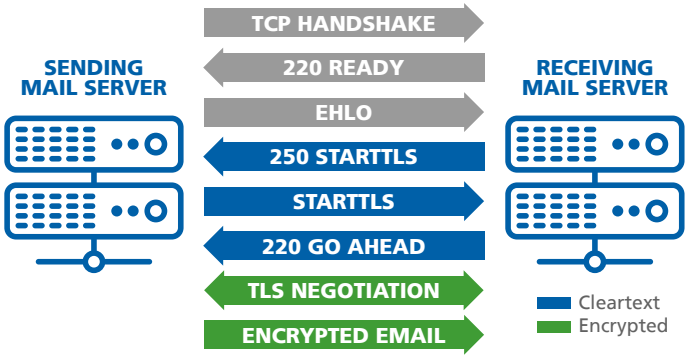
When email is encrypted for transmission "over the wire," email communication is protected against being read and/or altered by attackers. Many organizations and email providers endeavor to reduce risks specifically associated with email in-transit by sending emails over Transport Layer Security (TLS). When successfully negotiated between two mail servers, TLS provides a protective "tunnel" for the email message by encrypting the transportation channel. However in its current form, using TLS for email has its own security vulnerabilities that make it susceptible to man-in-the-middle (MITM) attacks.

Representatives within the Internet Engineering Task Force (IETF) community have published three draft Request for Comment (RFC) proposals designed to augment the current Simple Mail Transfer Protocol (SMTP) Service Extension for Secure SMTP over Transport Layer Security Standard (RFC 3207). The RFC proposals specifically aim to address prominent MITM security gaps associated with sending email over a TLS connection.

This whitepaper explains the inherent email security risks associated with sending email via opportunistic TLS and takes a closer look at the three draft proposals. Readers will gain a better understanding of the individual proposal's area of focus and recommendations, along with awareness for additional functionality needed to secure email in transit

Protecting Email In-Transit with SMTP for TLS

The SMTP over TLS standard was published in February 2002 with the intent of providing private, authenticated email communications over the Internet. The standard introduced the STARTTLS extension, a keyword used to tell the sender's mail server that the receiving mail server is currently able to negotiate the use of TLS. When successfully negotiated, TLS provides a secure communications tunnel between mail servers and message protection from passive eavesdroppers. Below is the typical handshake process for establishing a TLS connection between two mail servers:



1. Communication begins with sender's mail server sending a connection request to the receiving mail server via EHLO command. The receiving mail server sends back a list of options it supports, including support for TLS by returning "250 STARRTTLS" command.

2. If both sides support TLS, the TLS "handshake" begins with receiving mail server sending a TLS certificate to the sending mail server.

3. If the sender trusts the certificate of the receiving mail server, a TLS session encryption key is negotiated.

4. The TLS session starts, and the email message is transmitted.

Encryption in-transit helps to protect emails while they travel between individual email servers. Unfortunately, billions of unencrypted emails are sent and received "in plain text" every day - simply readable and open to attack. Why? Because TLS adoption is voluntary and often misconfigured, and sending methods vary.

TLS Methods

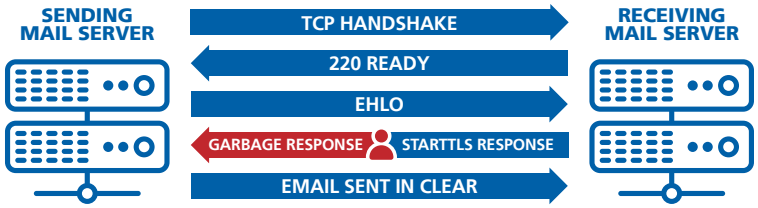
TLS can be implemented through two methods – Mandatory and Opportunistic. Mandatory TLS requires TLS be available before sending an email, otherwise the email is bounced. Mandatory TLS with certificate validation is the safer TLS method but requires TLS be set-up correctly on both mail servers to ensure a successful handshake and secure email delivery. Manual effort to set-up bidirectional TLS with every domain and the associated on-going maintenance can be costly and, for most organizations, is an option reserved only for key customers and partners.

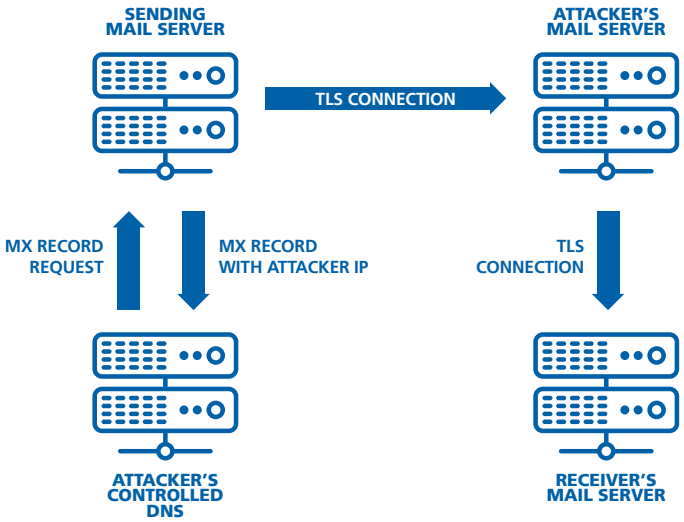
Opportunistic TLS is commonly described as "best effort." If TLS is not available or cannot be successfully negotiated for some reason, the session "fails open," and the email is sent in the clear, making it vulnerable to eavesdroppers. Opposite of mandatory TLS, opportunistic TLS selects message delivery over security, creating a virtual playground for attackers.

Opportunistic TLS Risks Man-In-The-Middle (MITM) Attacks

The "fail open" nature of opportunistic TLS compromises email security risking both passive and active MITM attacks.

Passive MITM attacks for eavesdropping - Since opportunistic TLS is designed to fail open, all a hacker needs to do is compromise the TLS handshake, so email messages are sent in the clear conceding message confidentiality. An attacker can execute a MITM attack by simply intercepting and dropping the STARTTLS command or overwriting with junk, causing the TLS negotiation to fail. With this type of MITM passive downgrade attack, email conversations occur in the open enabling eavesdropping.





Active MITM attacks for redirection – In this scenario, the TLS session is successfully negotiated, but unbeknownst to the sending mail server, the session has been redirected to the attacker's server. This can happen when the attacker spoofs the Domain Name System (DNS) Mail Exchange (MX) records of the recipient domain, causing messages to be redirected to server under the attacker's control. Sender and receiver believe they are communicating over TLS, when in reality they are communicating over TLS to attacker's server. This scenario happens when the SMTP client either does not verify the server's certificate or establishes a TLS connection even when verification fails.

Having such vulnerabilities exposed, compromise data confidentiality and leave organizations at risk. This is why representatives within the IETF community have joined forces to create draft proposals aimed at narrowing these identified MITM and DNS spoofing security risks.

IETF Draft Proposals

There are currently three proposals on the IETF RFC standards track aimed at minimizing MITM "in transit" vulnerabilities associated with email communications over opportunistic TLS.

Let's take a closer look at each draft's individual focus and expected security benefits.

SMTP Mail Transfer Agent ***(MTA) Strict Transport Security (STS)***

Initially released in March 2016 and in its second draft, the SMTP MTA STS proposal is aimed at both passive and active MITM attacks associated with STARTTLS negotiation.

The proposal describes a mechanism for defining and publishing recipient MTA domain policies for inspection and validation by a sending mail server before email is sent. The proposal includes:

- **Policy semantics** – whether senders can expect a server for the receiving domain to support TLS and how to validate the presented TLS certificate.
- **Policy authentication** – described methods for determining the authenticity of a published policy delivered via DNS.
- **Policy application and failure handling** – directions for the sending mail server on what to do when TLS cannot be successfully negotiated. Policy could state email should fail to deliver, meaning email is bounced thereby forcing a TLS session be established prior to message delivery. There is also a new "Report Only" mode. In this mode, sending mail servers can send an aggregated informational report to a designated report address specified in the policy, alerting of failed attempts for optional investigation.

Drafted by top email providers, specifically Google, Microsoft, Yahoo!, Comcast, LinkedIn and others, the SMTP MTA STS proposal is designed to address known STARTTLS vulnerabilities providing a structure under which a mail server can proclaim their ability to receive TLS-secured connections, specify method(s) for certificate validation and request sending mail servers either report on and/or refuse to deliver messages that cannot be securely delivered.

SMTP TLS Reporting

The SMTP TLS Reporting proposal is a companion to the above SMTP MTA STS draft specification, describing a reporting mechanism and format by which sending servers can share statistics and information about potential failures with recipient servers. The goal is to provide transparency into misconfigurations and attempts to intercept or tamper with mail between server systems who support STARTTLS.

Described in the proposal is a reporting schema and report destination information that covers:

- **Successes** – providing a pulse-check to receiving server that all is functioning as anticipate
- **Failures** – providing information on failures due to routing and/or STARTTLS negotiation

The intent is to provide community sharing of STARTTLS connection information, so recipient domains can then use the information to both detect potential attackers and diagnose unintentional misconfigurations.

SMTP Require TLS Option

The goal of the SMTP Require TLS Option is also to improve opportunistic TLS by changing the default "fail open" behavior to "fail close." Currently with opportunistic TLS, if TLS is not available or cannot be successfully negotiated, the session "fails open" by default sending the email message in clear text over a non-secure session. The SMTP Require TLS Option proposal describes a complementary SMTP service extension, REQUIRETLS. The REQUIRETLS SMTP service extension would allow the email client to specify that a given message sent during a particular session must be sent over a TLS protected session with specified security characteristics. The selection mechanism is not defined in the proposal but could be implemented through a user interface selection, in a header field included in the message or based on policy. If selection is made, the message is tagged by the mail server with the REQUIRETLS extension.

Once a message is tagged for secure transmission only, if a STARTTLS session cannot be successfully negotiated for any reason or if the receiving mail server does not advertise support for REQUIRETLS in the EHLO response, the connection is required to "fail close" bouncing the message back to sender as undeliverable. In a non-delivery situation, the proposal describes specific status codes be reported to sending mail server alerting to the failure cause:

- DNSSEC lookup failure
- REQUIRETLS not support by server
- Unable to establish a STARRTLS-protected session

The proposal also defines an optional REQUIRETLS parameter for specifying requirements for server authentication.

Summary of Proposal Focus Areas Addressed

Both the SMTP MTA STS and SMTP Require TLS Option proposals seek to reduce opportunities for both passive and active MITM attacks. The TLS Reporting draft complements the SMTP STS proposal by defining reporting information for both TLS connection successes and failures seeking to standardize the exchange of information between mail servers for both awareness and diagnostic purposes.

Proposal Focus Area	SMTP MTA STS	TLS Reporting	SMTP Require TLS Option
Passive MITM for eavesdropping	✓		✓
Active MITM attacks for redirection caused by tampering with STARRTLS	✓		✓
Active MITM attacks for redirection caused by weakness in server authentication	✓		✓
Reporting for awareness and troubleshooting	✓	✓	
Sender initiated security			✓

Additional TLS Security Gaps Not in the Proposals

Regardless of the sender method, opportunistic or mandatory, TLS by nature has limitations that the draft proposals do not address. Organizations should take an all-encompassing, holistic approach when implementing a solution to secure email "in-transit," including the following considerations:

Multi-hops: SMTP over TLS is single session between two distinct mail servers. Since email uses a store-and-forward protocol, an email may go through several mail servers and needs to be secured with TLS at each point of its journey. For example in a multi-hop scenario of A-to-B, B-to-C and C-to-D, it could be that merely the A-to-B session may have been protected via TLS, leaving the email content and any attachments in the clear for the remaining portion of its email journey.

Reply messages: SMTP over TLS does not guarantee a secure message reply. A message that may have been confidentially delivered over TLS is not guaranteed to be returned securely in a reply message back to the sender. Often the original email is also returned in the reply email body as clear text, so if a TLS session is not successfully negotiated for the reply message, all information that was protected outbound will now be clearly visible in the reply.

Sender and Recipient notification: SMTP over TLS does not provide feedback to the sender that an email actually did/did not transfer securely, nor is recipient notified that email was sent securely so they can treat contents accordingly.

Reporting: SMTP over TLS does not define reporting in support of auditing for compliance and increased visibility. Most mail servers only provide TLS reporting through log files, which are difficult to use for compliance reporting.

What is Next for the RFC Draft Proposals? Approval and Adoption

The IETF develops and promotes voluntary Internet standards, specifically the standards that comprise the Internet Protocol Suite (TCP/IP). The road to approval for an RFC proposal can be lengthy. As an RFC begins as a draft proposal, it can be reviewed and revised within the IETF community many times before being submitted for approval. Only upon approval by designated representatives of the Internet Engineering Steering Group, (IESG), does a proposal become an official RFC. Then adoption of the new RFC can begin. History has shown that it can take years for a new standard to be finalized and implemented throughout the industry.

Zix is thrilled to see the RFC proposals, and we applaud the drive to improve email security. As the standard develops, we plan to enhance our existing superior TLS capabilities in support of the changes. It is positive initiatives like these that motivate quality and specifications that influence the way people design, use and manage internet communications.

Zix – Filling the TLS Security Gaps Today

Zix provides email encryption options that alleviate all of the TLS gaps in securing email content and attachments in transit, but when TLS is the preferred email security method, businesses can rely on Zix to provide superior TLS support. Zix is focused on making email encryption easier for users and, as part of that, supports the responsible use of TLS by enabling customers to define its use in policies and verify the results by way of reporting. We give customers the ability to define and control when the use of TLS is appropriate based on the email content and recipient. Customers can create policies for mandatory TLS or attempt opportunistic TLS and define a fall back to another secure delivery method if TLS is not available – filling the TLS security gaps. Customers can also define the level of encryption and authentication required when establishing a TLS connection.

For compliance officers and administrators, Zix provides an informative dashboard and detailed reports for message level tracking by delivery method. These reports detail how each message was delivered, including TLS encrypted email, along with time stamp, sender and receiver information. Using the Zix reporting dashboard, administrators can easily view both summary and detailed information about their encrypted email traffic.

Exclusive to Zix users, security branding is embedded at the top of every encrypted message providing confidence to your recipients that the email and its sensitive contents were delivered securely. Branding reinforces the importance of protecting sensitive information and reflects the measures your company is taking to protect data privacy and comply with regulations.

This message was sent securely using ZixCorp

Zix Email Encryption is secure, reliable and easy-to-use. If your organization is considering TLS as an additional component to 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			✓

If you would like to learn more about Zix Email Encryption with superior TLS support, review our dedicated TLS datasheet. Have more questions? Simply email us at info@zixcorp.com.

Watch our website for updates on the proposals.