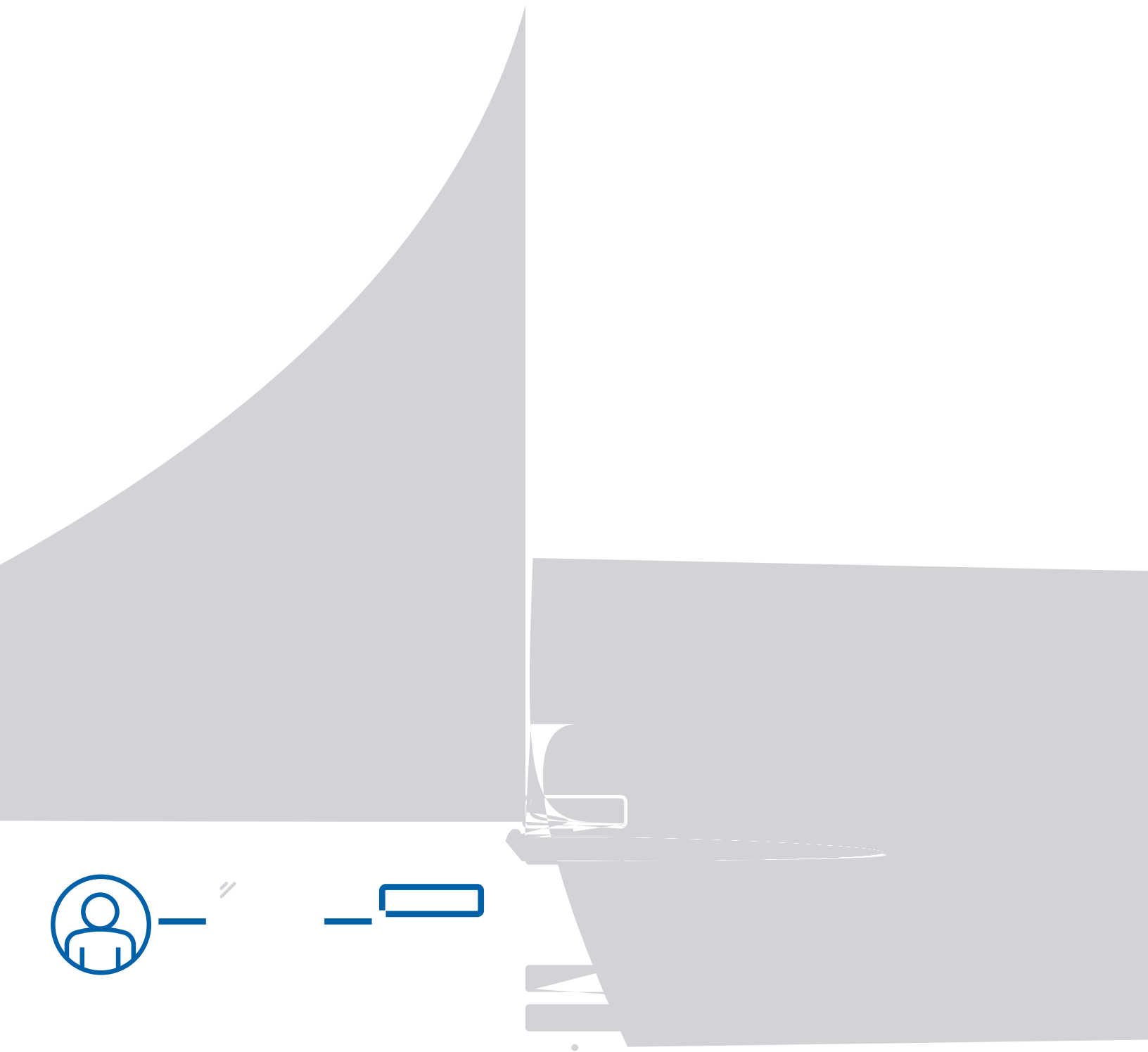

When email is encrypted for transmission "over the wire," email communication is protected against being read and/or altered by attackers. Many organizations and email providers endeavor to reduce risks specifically associated with email in-transit by sending emails over Transport Layer Security (TLS). 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

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

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.

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:

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.

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 r sn c

been t Sewaran for

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