TLS and DANE

EXPERT ADVICE ON GETTING STARTED, BEST PRACTICES, AND PIT FALLS TO AVOID

This is the 5th episode in the Zimbra webinar series that aims to demystify modern email authentication and email encryption for practical, everyday use.

A Brief Introduction

Randy Leiker

President and CEO of Skyway Networks

- 26 Years Of IT industry experience
- 23 Of Those Years at Skyway Networks
- Long history with Zimbra, dating back to Zimbra 5.0

Skyway Networks℠

Email Security Webinar Series

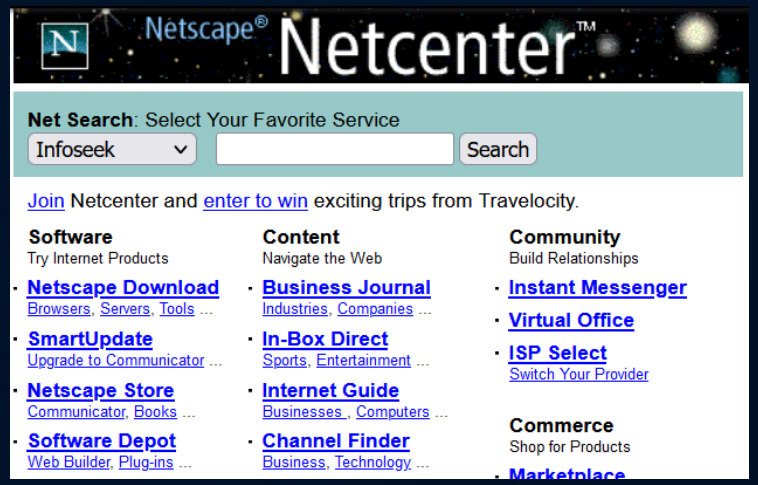
- **Topics Covered In Earlier Episodes**
  - SPF & DKIM: these form the foundation on which modern email authentication operates and are the first key steps to protecting your outbound email and domain name's reputation.
  - DMARC: supercharges SPF & DKIM by providing enforcement of your email policies, with a powerful feedback mechanism.
  - MTA-STS, TLS-RPT, BIMI: advertise to email senders that you prefer strong encryption and gain important insights into any delivery failures. Also, enable your organization's logo to appear in email recipient Inboxes for improved brand trust.
  - DNSSEC: prevent your DNS infrastructure from being the weakest link in the security chain and defend yourself from a variety of spoofing and man-in-the-middle attacks.

Overview Of Today's Webinar

- TLS
  - Cryptography History
  - TLS Concepts
  - Using Strong Protocols & Cipher Suites in Zimbra
  - TLS Best Practices
  - TLS Q&A
- DANE
  - Introduction to DANE
  - What's Wrong With the CAs
  - How To Set Up DANE
  - DANE Best Practices
  - DANE Q&A
  - Key Take Aways

This webinar is being recorded and will be posted on the Zimbra YouTube Channel at https://www.youtube.com/c/zimbra

Cryptography History



- SSL: Secure Sockets Layer
- TLS: Transport Layer Security

- SSL 1.0 to 3.0 created by Netscape Corporation in mid-1990s for securing only HTTP, FTP, and SMTP data in transit on the Internet.

- IETF (Internet Engineering Task Force) released TLS 1.0 in 1999, a successor to SSL 3.0. It secures data for any TCP-based protocol.

- Follow-up releases: TLS 1.1 in 2006, TLS 1.2 in 2008, and TLS 1.3 in 2018.

- Use of all SSL versions and TLS 1.0 to 1.1 is discouraged due to vulnerabilities.

TLS Concepts: Symmetric Encryption

TLS Concepts: Symmetric Encryption

Message To Encrypt: “flight leaves tonight”
Secret Key: 2

TLS Concepts: Symmetric Encryption

Message To Encrypt: “flight leaves tonight”
Secret Key: 2

Plain-text: “flight leaves tonight”
Encrypted: “hnijv ngcxgu vqpkijv”

TLS Concepts: Symmetric Encryption

Message To Encrypt: “flight leaves tonight”
Secret Key: 2

Plain-text: “flight leaves tonight”
Encrypted: “hnijv ngcxgu vqpkijv”

a b c d e f g h i j

Secret Key: 2

Encrypted: “hnijv ngcxgu vqpkijv”
Plain-text: “flight leaves tonight”

a b c d e f g h i j

Secret Key: 2

TLS Concepts: Symmetric Encryption

- Requires a sender and recipient to exchange a pre-shared key in advance.
- Offers the fastest encryption and decryption performance.
- It is primarily responsible for why web sites using HTTPS have the appearance of being nearly as fast as their HTTP counterparts.

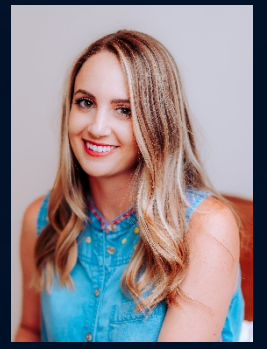
TLS Concepts: Asymmetric Encryption

- There is no pre-shared key between two parties in advance.
- Has much slower encryption/decryption performance compared to Symmetric Encryption.
- Asymmetric Encryption is used only at the very beginning of a TLS connection between two parties, that then switch over as soon as possible to Symmetric Encryption.

TLS Concepts: Asymmetric Encryption

Jill

1. Jill creates a keypair: matching private & public keys.
2. Jill creates a certificate signing request (CSR) containing her public key.
3. The CSR is provided to Jill's Certificate Authority (CA), Let's Encrypt.
4. The CA signs Jill's public key and sends back a modified version to her to install in Zimbra.

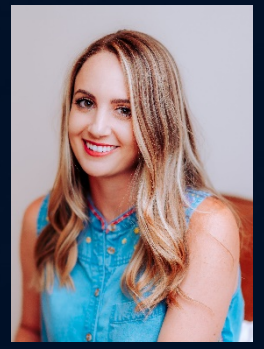


Katie

TLS Concepts: Asymmetric Encryption

Jill

5. Jill composes & sends an email to Katie.
6. Jill's Zimbra server connects to Katie's email server and they exchange public keys.
7. Katie checks Jill's public key expiration date and the CA that signed it (Let's Encrypt in this example). Jill does the same for Katie's public key.
8. A mutually agreed one-time use session key is created & shared between Jill & Katie for Symmetric Encryption of the email message.
9. Katie's server uses Symmetric Encryption to decrypt Jill's email and delivers it to her Inbox.



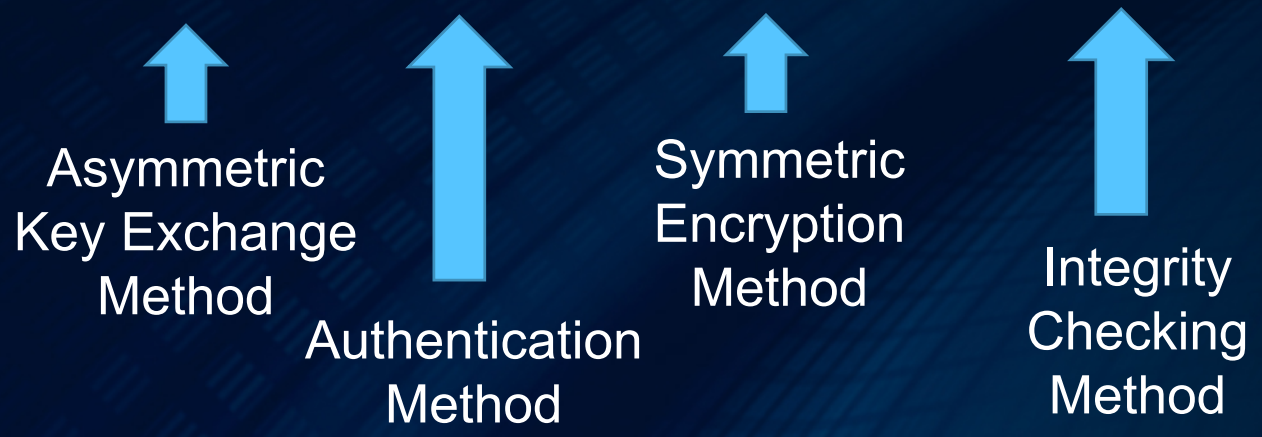
Katie

TLS Concepts: Protocols & Cipher Suites

- Protocols:
  - ~~SSL 1.0, 2.0, 3.0~~
  - TLS 1.0, 1.1, 1.2, 1.3
- Cipher Suites
  - ECDHE-ECDSA-AES128-GCM-SHA256

TLS Concepts: Protocols & Cipher Suites

- Protocols:
  - ~~SSL 1.0, 2.0, 3.0~~
  - TLS 1.0, 1.1, 1.2, 1.3
- Cipher Suites
  - ECDHE-ECDSA-AES128-GCM-SHA256



Using Strong Protocols & Cipher Suites In Zimbra

- Refer to: https://wiki.zimbra.com/wiki/Cipher_suites
- Viewing Available TLS Protocols and Cipher Suites In Zimbra:
  - su - zimbra (or) sudo su - zimbra
  - ~/common/bin/openssl ciphers -v

Fixing A Broken Certificate Chain Of Trust

- How-To Article: https://wiki.zimbra.com/wiki/Certificate_Chain
- Video: https://blog.zimbra.com/2022/05/zimbra-skillz-how-to-create-the-certificate-chain

- Certificate Authority: Root Certificate

  - Intermediate Certificate

    - Your SSL Certificate (Public Key)

TLS Best Practices

- **Best Practice # 1:** Backup your current Zimbra TLS settings
  - Before making changes, first make a copy of the current settings so you can easily rollback. For example, before using:
    - zmprov -l mcf zimbraReverseProxySSLCiphers…
  - Run the following to make a copy of the current setting:
    - zmprov gcf zimbraReverseProxySSLCiphers

TLS Best Practices

- **Best Practice # 2:** Avoid changing many TLS settings in Zimbra simultaneously
  - Changing many TLS settings all at once will make it difficult to determine which setting change created a problem.
  - Focus on a single component in Zimbra, for example, Nginx or Postfix, make setting changes, then observe for at least a few days to a week.

TLS Best Practices

- **Best Practice # 3:** Use an incremental approach to disable older protocols and cipher suites.
  - Start by disabling TLS 1.0, then if no complaints, disable TLS 1.1.
  - Use this same method for incrementally disabling older cipher suites too.

TLS Best Practices

- **Best Practice # 4:** Use wildcard SSL certificates with care.
  - Wildcard certificates offer convenience (*.domain.example) but a breach of one server risks the TLS encrypted traffic from all servers using the same keypair.
  - If using wildcard certificates, consider using multiple wildcard certificates that are partitioned by functional purpose. Examples: One certificate for a web server farm and another certificate for a Zimbra cluster.

TLS Questions

Up Next: DANE

Introducing DANE

- DANE: DNS-based Authentication of Named Entities
- Purposes:
  - Enables domain name owners to publicly specify the SSL certificate that is legitimate for a domain name by publishing a DNS record.
  - Designed to prevent an adversary from obtaining an SSL certificate from a Certificate Authority (CA) under false pretenses.
  - Makes the option available to later transition away from relying on Certificate Authorities & trusted root certificates in OS’es and apps.

What's Wrong With The Certificate Authorities?

- Certificate Authorities (CAs) have always been expressly trusted to validate who may obtain an SSL certificate for a domain name.
- Multiple incidents in the past involving fraud and compromises of CAs have proven this trust is misplaced.
- The DANE standard was developed to address this broken system.

How To Setup DANE

- For Domain Name Owners:

  1. A domain name owner obtains an SSL certificate from a Certificate Authority (CA) as normal.

  2. The domain name owner generates a SHA-256 hash of all or just part of their SSL certificate.

  3. The hash is published in DNS as a TLSA (Transport Layer Security Authentication) record.

_25._tcp.mail.domain.example. IN TLSA 3 1 1 0820307308201efa003020102020

How To Setup DANE

_25._tcp.mail.domain.example. IN TLSA 3 1 1 0820307308201efa003020102020

- _25: Port number of the service using the SSL certificate

How To Setup DANE

_25._tcp.mail.domain.example. IN TLSA 3 1 1 0820307308201efa003020102020

- _25: Port number of the service using the SSL certificate
- _tcp: Protocol of the service using the SSL certificate

How To Setup DANE

_25._tcp.mail.domain.example. IN TLSA 3 1 1 0820307308201efa003020102020

- _25: Port number of the service using the SSL certificate
- _tcp: Protocol of the service using the SSL certificate
- mail.domain.example: the domain or sub-domain for the SSL certificate

How To Setup DANE

_25._tcp.mail.domain.example. IN TLSA 3 1 1 0820307308201efa003020102020

- _25: Port number of the service using the SSL certificate
- _tcp: Protocol of the service using the SSL certificate
- mail.domain.example: the domain or sub-domain for the SSL certificate
- 3: Certificate Usage: indicates this is a domain issued certificate

How To Setup DANE

_25._tcp.mail.domain.example. IN TLSA 3 1 1 0820307308201efa003020102020

- _25: Port number of the service using the SSL certificate
- _tcp: Protocol of the service using the SSL certificate
- mail.domain.example: the domain or sub-domain for the SSL certificate
- 3: Certificate Usage: indicates this is a domain issued certificate
- 1: Selector: indicates that only the public key portion of the SSL certificate is included in the hash

How To Setup DANE

_25._tcp.mail.domain.example. IN TLSA 3 1 1 0820307308201efa003020102020

- _25: Port number of the service using the SSL certificate
- _tcp: Protocol of the service using the SSL certificate
- mail.domain.example: the domain or sub-domain for the SSL certificate
- 3: Certificate Usage: indicates this is a domain issued certificate
- 1: Selector: indicates that only the public key portion of the SSL certificate is included in the hash
- 1: Matching Type: indicates that the hash value is a SHA-256 hash

How To Setup DANE

_25._tcp.mail.domain.example. IN TLSA 3 1 1 0820307308201efa003020102020

- _25: Port number of the service using the SSL certificate
- _tcp: Protocol of the service using the SSL certificate
- mail.domain.example: the domain or sub-domain for the SSL certificate
- 3: Certificate Usage: indicates this is a domain issued certificate
- 1: Selector: indicates that only the public key portion of the SSL certificate is included in the hash
- 1: Matching Type: indicates that the hash value is a SHA-256 hash
- 08203073…: the hash value of the certificate

How To Setup DANE

- Getting Started:
  - DANE for Incoming Zimbra Email: https://blog.zimbra.com/2022/04/zimbra-skillz-enable-dane-verification-for-incoming-email-in-zimbra
  - DANE for Outgoing Zimbra Email:
    - https://blog.zimbra.com/2022/03/zimbra-skillz-enable-dane-verification-for-outgoing-email-in-zimbra/

DANE Best Practices

- **Best Practice # 1:** Before using DANE, you must ensure your domain name has been setup with DNSSEC first, and that you have a working DNSSEC resolver.
    - The most recent Zimbra 8.8.15 and 9.0 Patch versions upgraded the included dnscache service to enable DNSSEC by default.

DANE Questions

Up Next: Key Take Aways

Key Take Aways

- Carefully consider the TLS protocols and cipher suites to support. User hardware will determine the older protocols and cipher suites you can safely disable on your Zimbra server.
- Gradually transition to a secure TLS configuration by disabling just one protocol or cipher suite at a time, then monitoring for a period of time for user feedback on any connection issues.
- TLS continues to evolve and there will be newer protocol versions and cipher suites released, so plan to periodically re-evaluate.
- DANE requires both a DNSSEC capable DNS resolver and for your domain name to be DNSSEC signed.

Thank You For Attending Today's Webinar!

- Helpful Links
  - **TLS**
    - https://wiki.zimbra.com/wiki/Cipher_suites
    - https://wiki.zimbra.com/wiki/Certificate_Chain
    - https://www.ssllabs.com/ssltest
  - **DANE**
    - https://blog.zimbra.com/2022/04/zimbra-skillz-enable-dane-verification-for-incoming-email-in-zimbra
    - https://blog.zimbra.com/2022/03/zimbra-skillz-enable-dane-verification-for-outgoing-email-in-zimbra/

Speaker's Contact Information

Randy Leiker
Skyway Networks
randy@skywaynetworks.com
https://skywaynetworks.com