LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

SSL/TLS Vulnerabilities

02/25/2021

TLP: WHITE, ID# ***202102251030***

Agenda

- About HC3
- Executive Summary
- Background
- Protocols That Use SSL/TLS
- How SSL/TLS Works
- SSL/TLS Vulnerabilities and Threats
- Case Study: The Raccoon Attack
- Mitigating SSL/TLS Vulnerabilities and Threats
- Summary

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

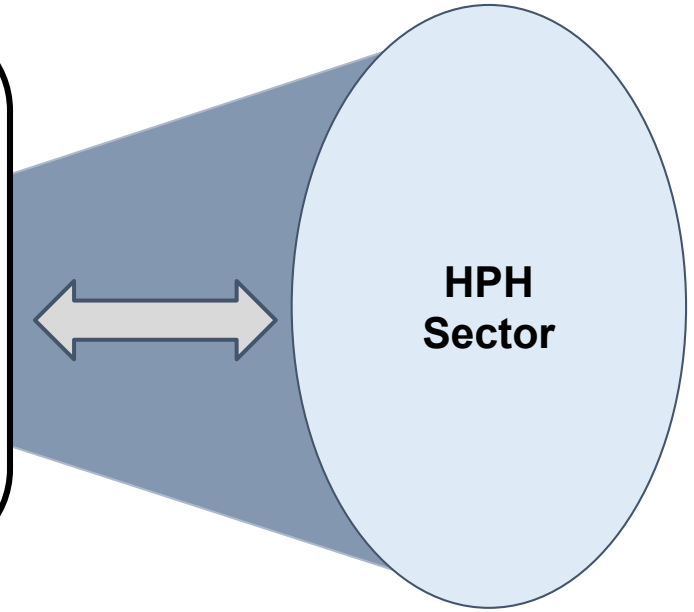
HC3 Mission Statement

To support the defense of the healthcare and public health sector's information technology infrastructure by strengthening coordination and information sharing within the sector and by cultivating cybersecurity resilience, regardless of organizations' technical capacity.

The U.S. Department of Health and Human Services (HHS) created HC3 to help identify, correlate, and communicate cybersecurity information across the healthcare and public health (HPH) sector.

HC3's Role in Helping the Sector

- Ensure cybersecurity information sharing is coordinated with the HPH sector, including within HHS and with government partners.
- Facilitate access to knowledge-based resources necessary to support robust cybersecurity programs and mitigate damage in security breach situations.



HC3 focuses on assisting private sector entities in defending against cybersecurity threats and ultimately reducing risk.

HC3's Authority

- According to Title 6 U.S.C. subsection 1501(3), any non-federal organization that shares cyber threat indicators with an appropriate federal entity is deemed voluntary data sharing, and is exempt from disclosure {Section 552 of Title 5 U.S.C.}.
- This information cannot be used against entities sharing information; as such HC3 does not report to the Office of Civil Rights (OCR) within HHS, nor share data.
- Therefore, HC3 is **separate** from OCR and its reporting requirements, and does **NOT** report on an entity to OCR.

HC3 develops unclassified, knowledge-based resources geared towards promoting and increasing HPH sector cyber knowledge, and hosts a monthly forum (via webinar) to brief active cybersecurity threats for sector-wide participation.

Threat Briefings

Product Overview

Briefing document that highlights relevant cybersecurity topics and raises the HPH sector's situational awareness of current cyber threats, best practices, and mitigation tactics.

Distro Method

- Email
- HC3 Website
- ASPR Sector Newsletter
- Uploaded to CHWG Portal

White Papers

Product Overview

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide recommendations to a wide audience.

Distro Method

- Email
- HC3 Website
- ASPR Sector Newsletter
- Uploaded to CHWG Portal

Threat Briefing Webinar

Forum Overview

Briefing that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Frequency

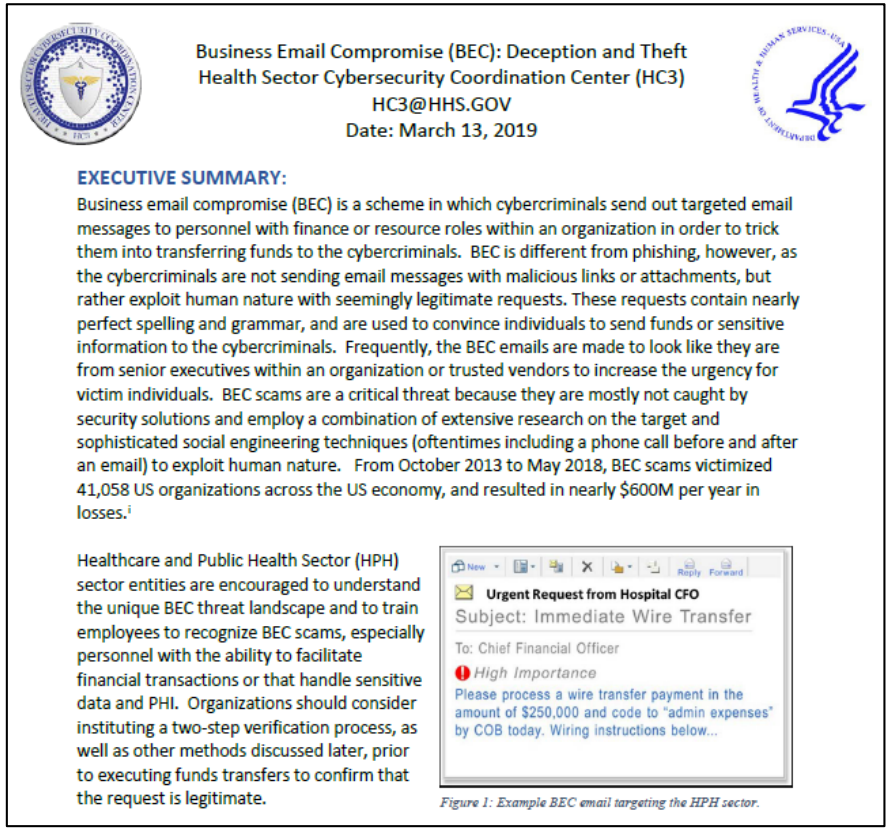
Briefings are hosted on a monthly basis.

Product Example: White Paper

In March 2019, HC3 developed and released a white paper on Business Email Compromise (BEC) with situational background and protection strategies for the sector. The screenshot below is an example of one section of the product.

High-level, situational background information providing context for a non-technical audience

Summarized protection strategies with details in subsequent sections for technical and non-technical audiences



Business Email Compromise (BEC): Deception and Theft
Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV
Date: March 13, 2019

EXECUTIVE SUMMARY:

Business email compromise (BEC) is a scheme in which cybercriminals send out targeted email messages to personnel with finance or resource roles within an organization in order to trick them into transferring funds to the cybercriminals. BEC is different from phishing, however, as the cybercriminals are not sending email messages with malicious links or attachments, but rather exploit human nature with seemingly legitimate requests. These requests contain nearly perfect spelling and grammar, and are used to convince individuals to send funds or sensitive information to the cybercriminals. Frequently, the BEC emails are made to look like they are from senior executives within an organization or trusted vendors to increase the urgency for victim individuals. BEC scams are a critical threat because they are mostly not caught by security solutions and employ a combination of extensive research on the target and sophisticated social engineering techniques (oftentimes including a phone call before and after an email) to exploit human nature. From October 2013 to May 2018, BEC scams victimized 41,058 US organizations across the US economy, and resulted in nearly $600M per year in losses.[i]

Healthcare and Public Health Sector (HPH) sector entities are encouraged to understand the unique BEC threat landscape and to train employees to recognize BEC scams, especially personnel with the ability to facilitate financial transactions or that handle sensitive data and PHI. Organizations should consider instituting a two-step verification process, as well as other methods discussed later, prior to executing funds transfers to confirm that the request is legitimate.

Figure 1: Example BEC email targeting the HPH sector.

HC3's Website

- HHS.gov/HC3
- The one-stop shop for all of HC3 products
  - Products are free to download
- In the "Contact Us" section, we highlight other organizations and programs we work with
- HC3@hhs.gov is the best way to engage us directly

Fostering a Collective and Engaged Sector

HC3's mission and operational focus is to keep the sector apprised of threats and solutions, provide bilateral support, and promote information sharing which is critical to success.

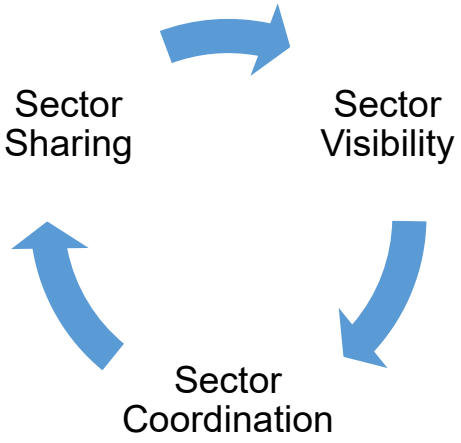
Opportunity Areas for Sector Sharing

- Anomalous Activity
- Defensive Measures
- Indicators of Compromise (IOC)

HC3

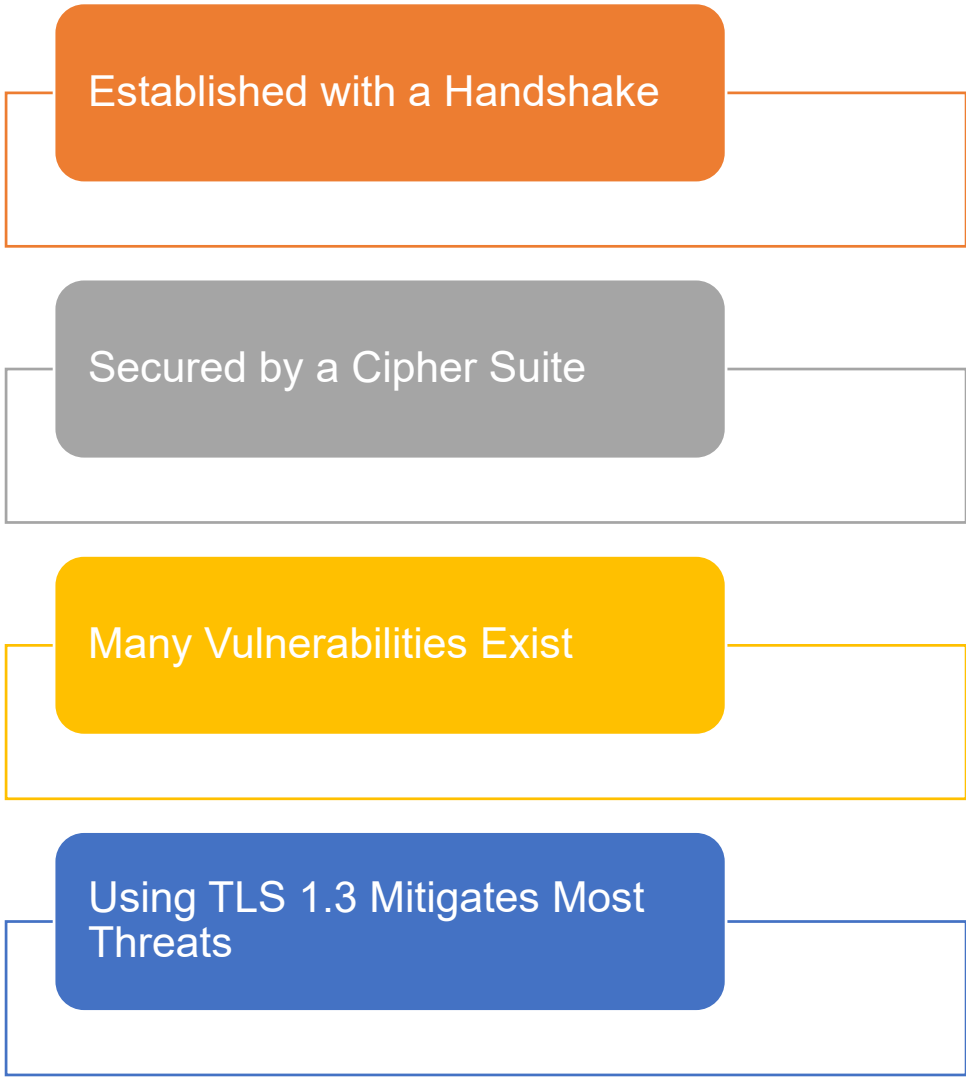
Share info via
HC3@hhs.gov
202-691-2110

HPH Sector Defense



Executive Summary

- SSL/TLS is a secure transport and session protocol designed to provide confidentiality and message integrity to web traffic, using a combination of cryptography and hashing techniques known as a cypher suite.
- Established in the mid-1990s, SSL/TLS has underwent many changes due to vulnerabilities exploited throughout the years.
- SSL/TLS is established with a handshake that determines what cipher suite and master secret can be used, and then uses digital certificates to make a connection between a client and server.
- Using the agreed-upon cipher suite, SSL/TLS uses cryptography to encode data and hashing algorithms in order to maintain message integrity.
- As web traffic increasingly relies upon SSL/TLS, many vulnerabilities have been discovered, and SSL is no longer safe to use.
- Many threats have emerged, with the Raccoon Attack being the most recent.
- To mitigate these attacks when possible, using TLS 1.3 is recommended, and using any version of TLS prior to 1.2 should be avoided.



Secure Sockets Layer (SSL)

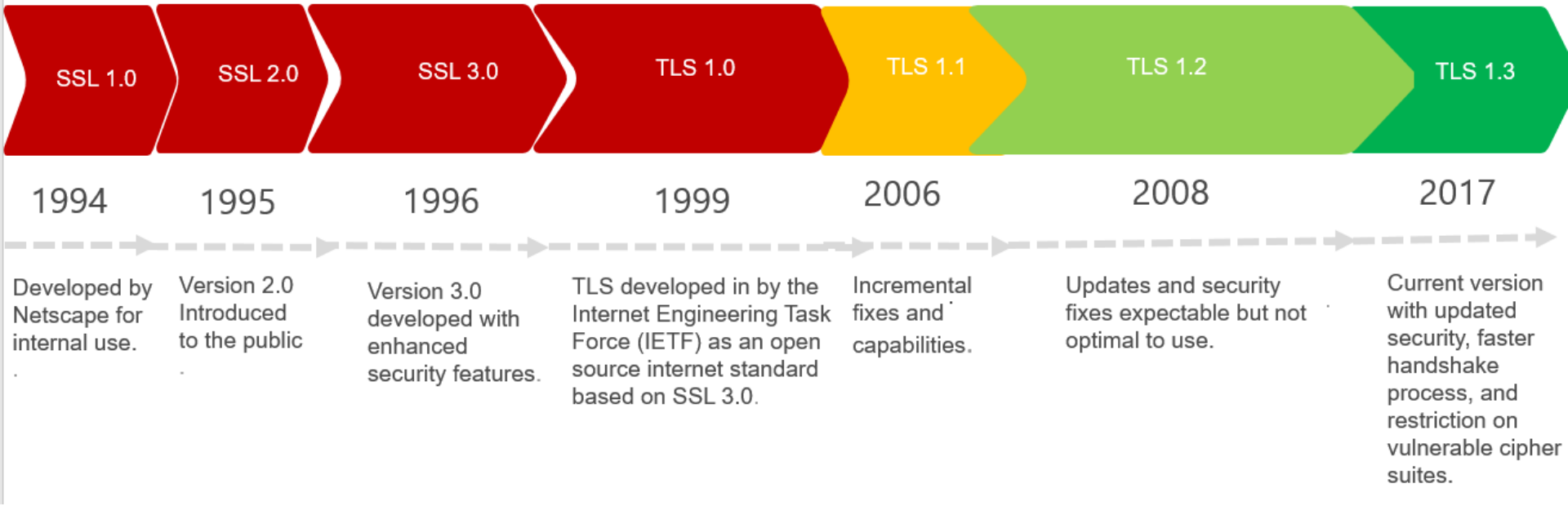
Designed by Netscape to provide:

- Privacy – Data Encryption
- Identity Authentication – Server Authentication and Optional Client Authentication through a handshake process
- Reliability – Message Integrity
- Requires that server and browser are enabled to use SLS
- Protects data in motion but does not protect data at rest
- Works at the Session and Transport Layer of the OSI Model
- Mostly used with HTTP, but also used with other TCP protocols
- Is currently depreciated and should not be used

Transport Layer Security (TLS)

- Designed by IETF as an open-source protocol based on SSL 3.0
- TLS 1.2 and 1.3 are what we should be using. Other versions of TLS and all SSL versions should be avoided, if possible. The most recent version of TLS features:
  - Enhanced security encryption and hashing
  - No backward compatibility
  - HMAC
  - More efficient handshake process
  - Eliminates compromised cipher suites

SSL/TLS Development Timeline



TLS 1.2 and 1.3 provide:

- Confidentiality – Symmetric key encryption for application data. – Typically, Advanced Encryption Standard (AES).
- Integrity – Authenticated Encryption with Additional Data (AEAD). – Usually AES-GCM (Galois/Counter Mode).
- Authentication – X509 certificates signed by a mutually trusted third party. – Typically, server authenticated only.

Protocols That Use TLS

HTTPS

- Hyper Text Transfer Protocol is the most common TCP protocol that uses SSL/TLS

SMTPS

- Simple Mail Transfer Protocol uses SSL/TLS to send secure messages from one mail server to another

POP3S

- Post Office Protocol allows mail to be stored on a server and downloaded to a recipient's email client on demand

IMAPS

- Internet Message Access Protocol allows a user to access email messages remotely

FTPS

- File Transfer Protocol is a network protocol used for the transfer of computer files from a server to a client

SIPS

- Session Initiation Protocol is a signaling protocol used for initiating, maintaining and terminating real-time sessions

Handshake

- Agree on a cipher suite
- Agree on a master secret
- Authentication using certificate(s)

Application Data

- Symmetric key encryption
- AEAD cipher modes
- Typically HTTP

Alerts

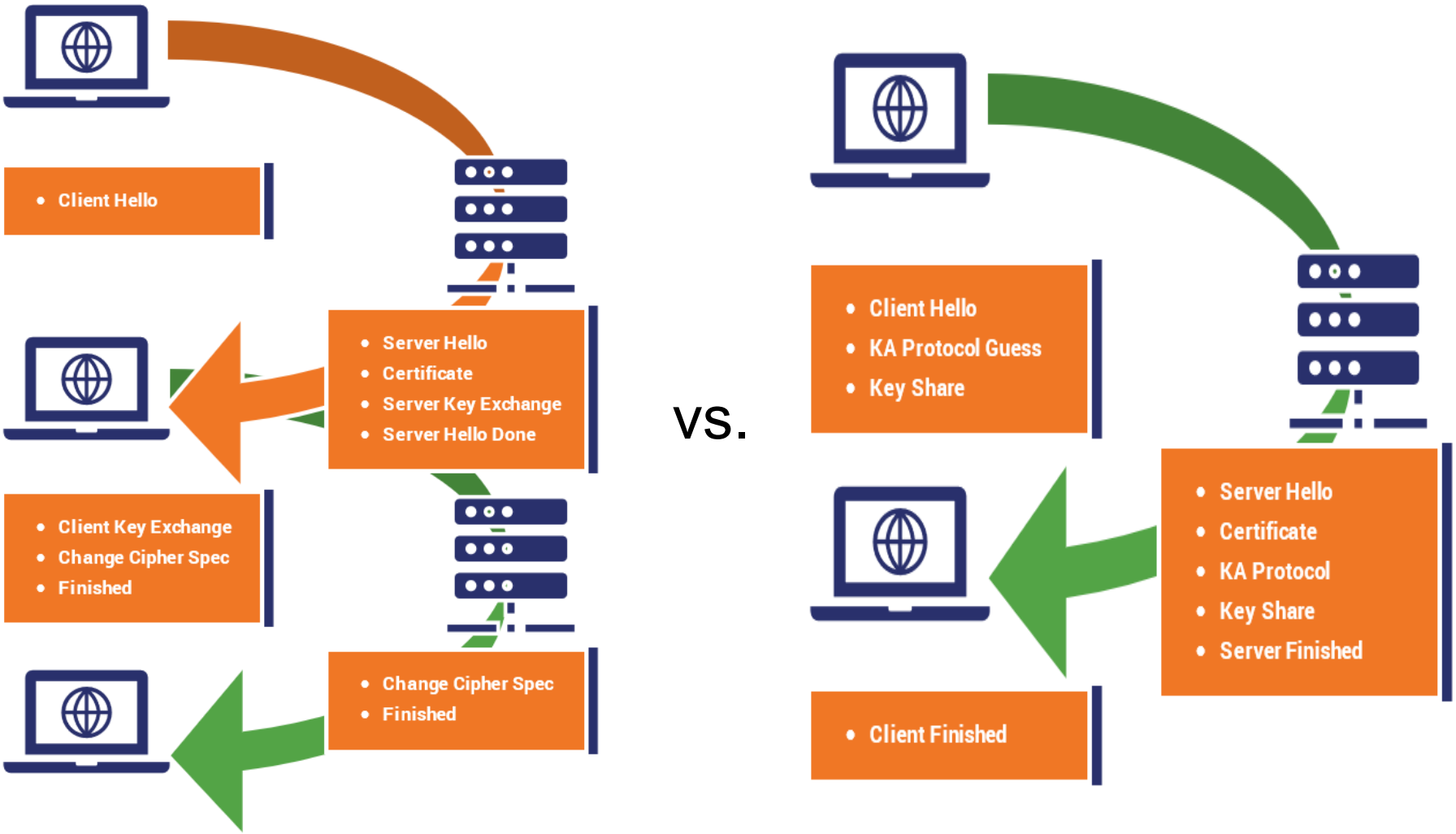
- Graceful closure
- Problem detected

TLS 1.2 and Defunct Handshake

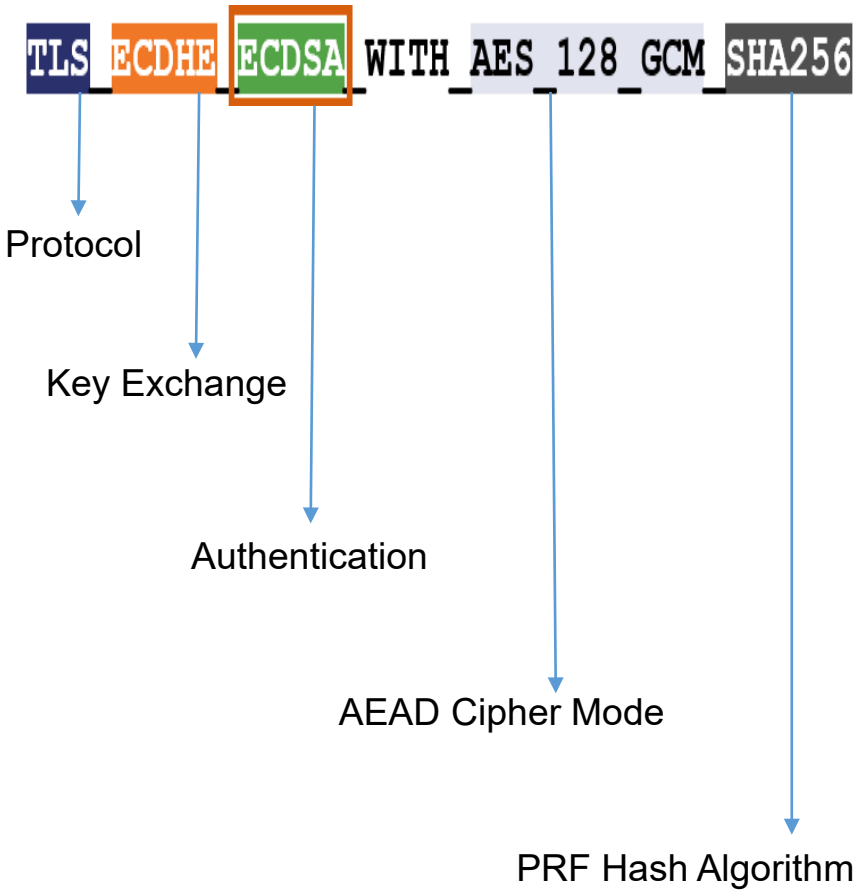
Step	Client	Direction	Message	Direction	Server
1			Client Hello	→	
2		←	Server Hello		
3		←	Certificate		
4		←	Server Key Exchange		
5		←	Server Hello Done		
6			Client Key Exchange	→	
7			Change Cipher Spec	→	
8			Finished	→	
9		←	Change Cipher Spec		
10		←	Finished		

TLS 1.3 Handshake

TLS 1.2 versus 1.3 Handshake



TLS 1.2 Has 37 Cipher Suites; the Following 20 are Recommended

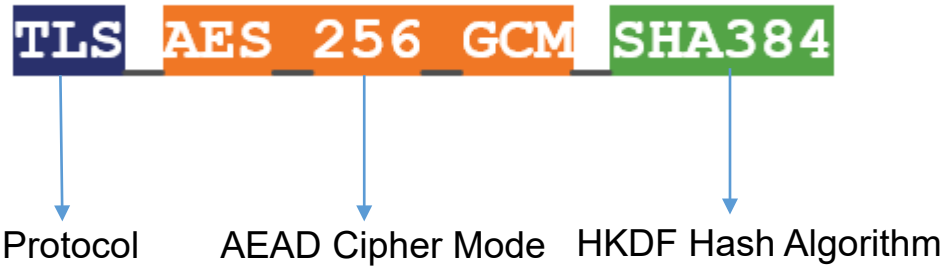


1. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
2. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
3. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
4. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
5. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
6. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
7. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
8. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
9. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
10. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
11. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
12. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
13. TLS_DHE_RSA_WITH_AES_128_CBC_SHA
14. TLS_DHE_RSA_WITH_AES_256_CBC_SHA
15. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
16. TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
17. TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
18. TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
19. TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
20. TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305

TLS 1.3 Reduces the Threat Vector by Limiting Cipher Suites

TLS 1.3 eliminates use of:

- SSL Compression
- Static key exchange functions
- Block ciphers (CBC)
- Non-AEAD ciphers (MAC-then-Encrypt)
- Renegotiation of encryption parameters



It has also dropped support for older, vulnerable SSL ciphers like:

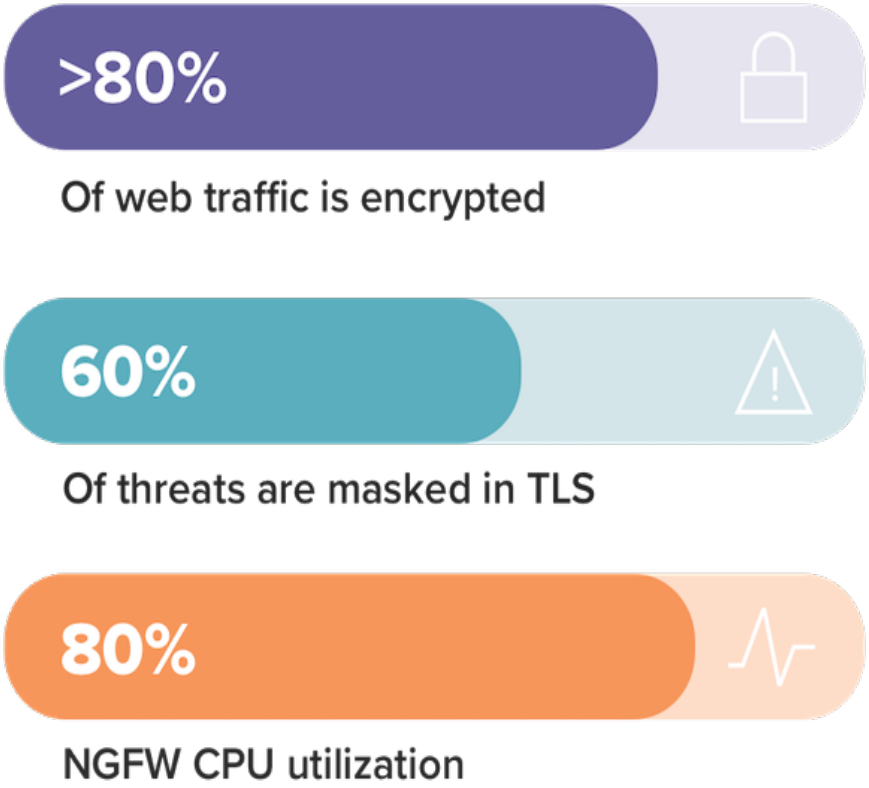
- RC4
- DSA
- MD5
- SHA1
- Weak Elliptic Curves
- RSA Key Exchange
- Static Diffie-Hellman (DH, ECDH)

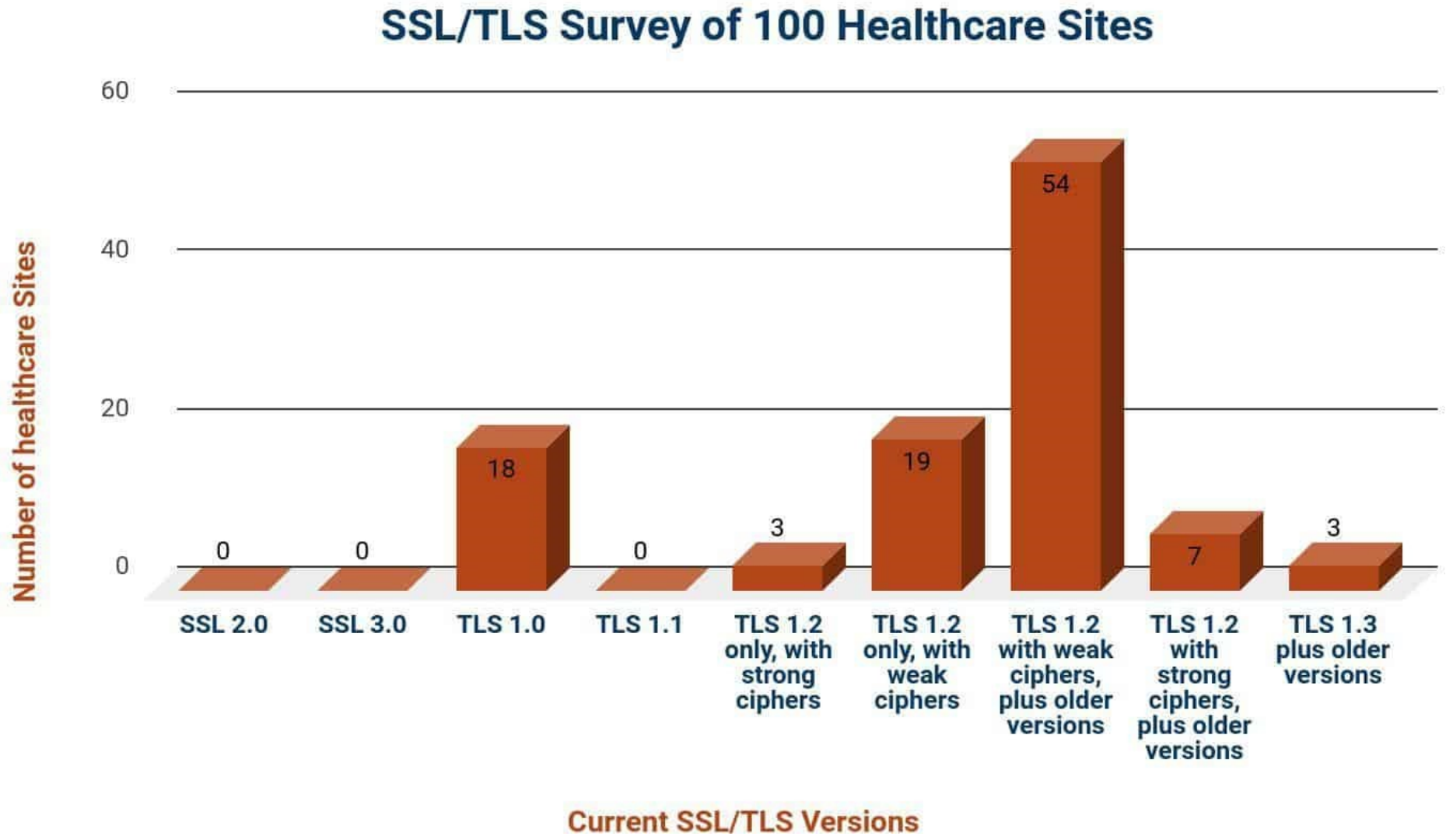
TLS 1.3 uses only the following 5 cipher suites:

1. TLS_AES_256_GCM_SHA384
2. TLS_CHACHA20_POLY1305_SHA256
3. TLS_AES_128_GCM_SHA256
4. TLS_AES_128_CCM_8_SHA256
5. TLS_AES_128_CCM_SHA256

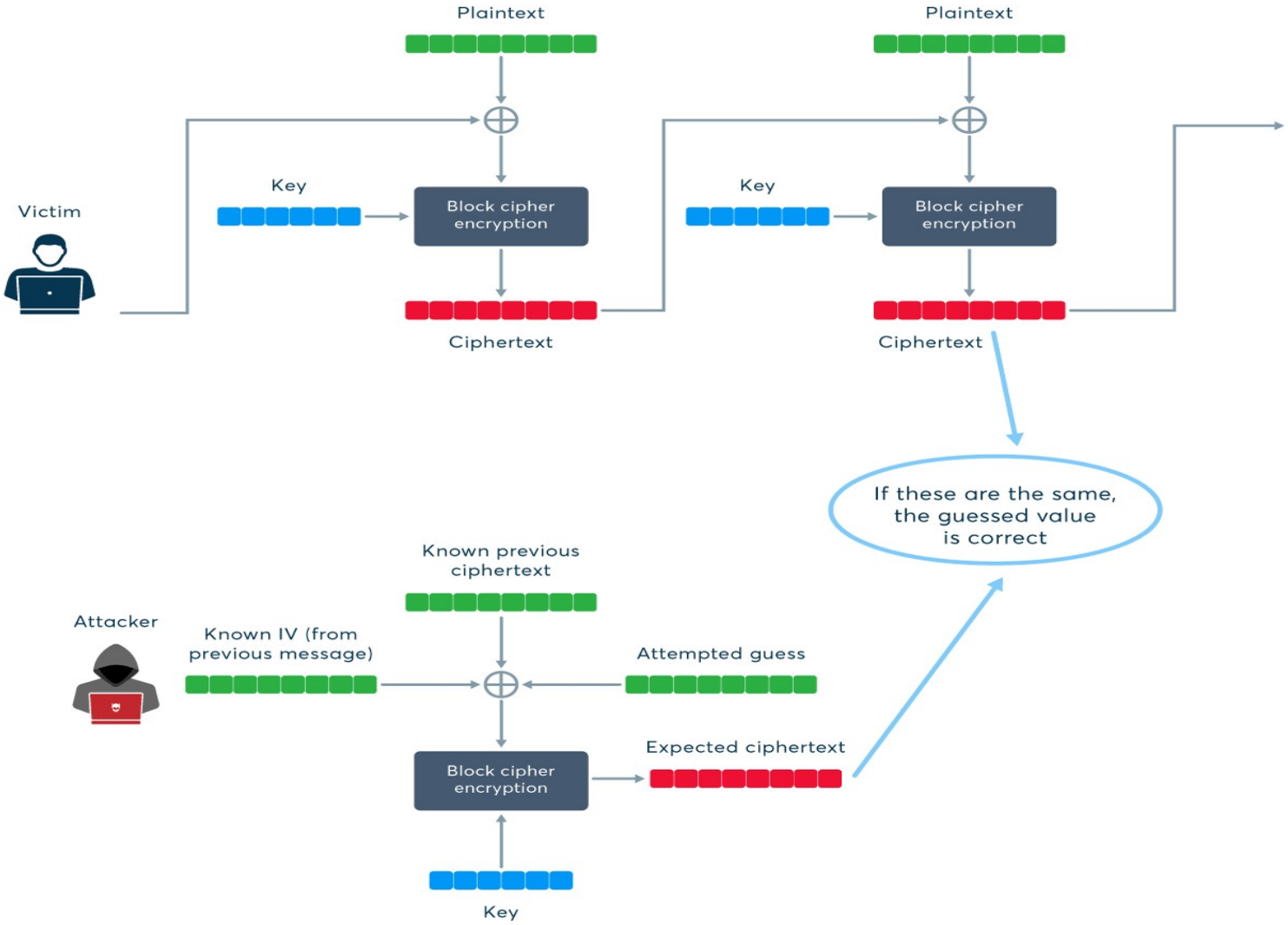
TLS Vulnerabilities and Threats

- SSL/TLS Stripping
- Man-in-the-Middle Attacks
- Self-signed “wildcard” certificates
- Attacker Encrypted Communications
- Unknown, Untrusted, and Forged Certificate Authorities

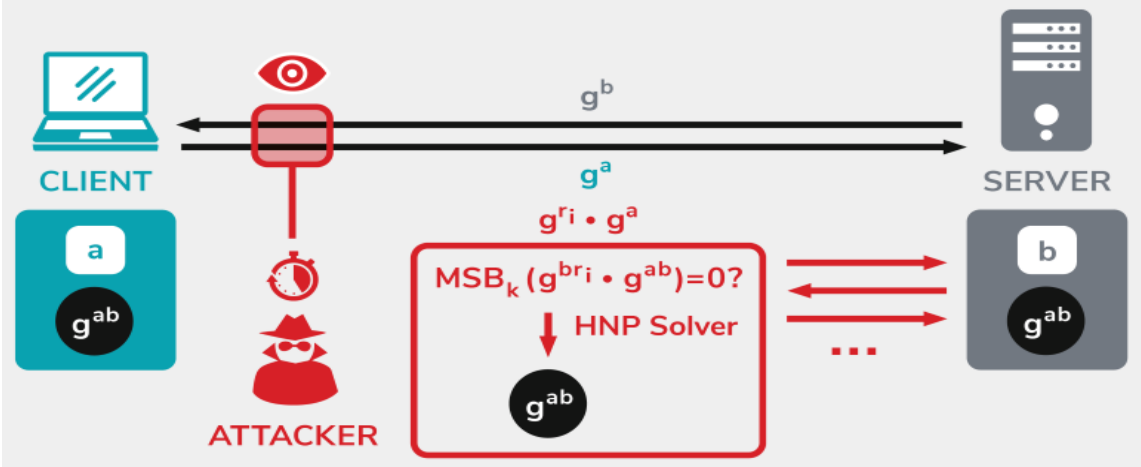



SSL/TLS Survey of 100 Healthcare Sites
Number of healthcare Sites
60
40
20
0
0
0
18
0
3
19
54
7
3
SSL 2.0
SSL 3.0
TLS 1.0
TLS 1.1
TLS 1.2 only, with strong ciphers
TLS 1.2 only, with weak ciphers
TLS 1.2 with weak ciphers, plus older versions
TLS 1.2 with strong ciphers, plus older versions
TLS 1.3 plus older versions
Current SSL/TLS Versions

TLS Vulnerabilities and Threats: The Beast Attack used on TLS 1.0



- "Raccoon" is a sophisticated attack on TLS 1.2 and prior versions.
- Raccoon attacks the Diffie-Hellman key exchange process and retrieves the premaster secret to complete the handshake.
- This is a difficult attack and would require certain circumstances to align:
  - The server would have to use a cipher suite that contains the Diffie-Hellman Ephemeral key
  - The server would have to require the reuse of public keys in the handshake process, and
  - The attacker would have to have perfect timing to execute the attack.
- If successful in decrypting the connection, an attacker using Raccoon can extract sensitive documents, emails, passwords, and credit card numbers.
- Using TLS 1.3 would eliminate the risk of the Raccoon attack due to the elimination of DHE in the cipher suites.



Examples of Known Threats to TLS/SLS

Name of Attack	Description	Protocol(s) Impacted	Mitigation	CVE
C.R.I.M.E. (Compression Ratio Info-Leak Made Easy)	CRIME works by leveraging a property of compression functions, and noting how the length of the compressed data changes. This allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses, in which a string in an HTTP request potentially matches an unknown string in an HTTP header.	HTTPS that use TLS 1.2 and below	Upgrade to TLS 1.3	2012-4929
P.O.O.D.L.E. (Padding Oracle On Downgraded Legacy Encryption)	Downgrades the handshake SSL 3.0 and exploits weakness in RC4 and CBC to allow attacker to gain access to sensitive data passed within the encrypted web session, such as passwords, cookies and other authentication tokens.	HTTPS that allows downgrades SSL 3.0	Do not allow the use of SSL 3.0, RC4 or CBC	2014-3566

Examples of Known Threats to TLS/SLS, Part 2

Name of Attack	Description	Protocol(s) Impacted	Mitigation	CVE
Triple Handshake	TLS client connects to a malicious server and presents a client credential. An attacker can then impersonate the client at any other server that accepts the same credential. The attacker performs a man-in-the-middle attack on three successive handshakes between the client and server, and succeeds in impersonating the client on the third handshake. RSA and DHE key exchanges have vulnerabilities that allow an attacker to create two different sessions with different identities sharing the same master secret.	HTTPS that allow the use of DHE and RSA Key Exchange	Ensure that all certificates received over a connection are valid for the current server endpoint, and abort the handshake if they are not. In some usages, it may be simplest to refuse any change of certificates during renegotiation.	CVE 2016 - 6112
D.R.O.W.N. (Decrypting RSA with Obsolete and Weakened eNcryption)	If one connection allows SSL V2, connections attacker can use SSL V2 RSA vulnerability to attack updated versions of TLS, facilitating a man-in-the-middle attack.	HTTPS	Do not allow connections with SSL or Cipher Suites that use RSA	CVE 2016 - 0800

Examples of Known Threats to TLS/SLS, Part 3

Name of Attack	Description	Protocol(s) Impacted	Mitigation	CVE
SHAttered	Jeopardizes message integrity by using SHA-1 Hash Collisions	HTTPS Use SHA 3	Discontinue Cipher Suites that use SHA-1 and replace with cipher suites that use SHA 3	CVE-2005-4900
NoMore	Exploits weakness in RC4	HTTPS	Stop using RC4	CVE-2015-2808
Sweet 32	Birthday Attack on 64 Bit Triple DES Block Cipher	HTTPS	Stop using 64 Bit Block Ciphers	CVE 2016-2183

SSL/TLS Vulnerability Mitigation

- Upgrading to TLS 1.3 would eliminate all known vulnerabilities
- Deactivate all versions of SSL, as well as TLS 1.0 and 1.1, and activate only strong cipher suites in TLS 1.2
- Turn off header compression
- Turn off the RC4 stream cipher (Rivest Cipher 4, also known as ARC4 or ARCFOUR, short for Alleged RC4)
- Disallow renegotiation with clients
- Get rid of export-grade ciphers
- Disallow insecure padding modes in TLS 1.2 (such as RSA PKCS#1 v1.5)
- Disable vulnerable CBC MAC-then-Encrypt modes
- Activate support for TLS_FALLBACK_SCSV, a protocol extension that prevents MITM attackers from forcing a protocol downgrade

TLS 1.3 eliminates the use of:

- Support for outmoded algorithms and ciphers
- RSA key exchange (and mandates Perfect Forward Secrecy)
- Reduces the number of negotiations in the handshake
- Reduces the number of algorithms in a cipher suite to 2
- Block mode ciphers and mandates AEAD bulk encryption
- Uses HKDF cryptographic extraction and key derivation
- Offers 1-RTT mode and Zero Round Trip Resumption
- Signs the entire handshake, an improvement of TLS 1.2
- Supports additional elliptic curves

TLS 1.3 Mitigates Several Attacks

Eliminated in TLS 1.3	Threat Eliminated
RC4	• Roos's Bias 1995 • Fluhrer, Martin & Shamir 2001 • Klein 2005 • Combinatorial Problem 2001 • Royal Holloway 2013 • Bar-mitzvah 2015 • NOMORE 2015
MD5 & SHA1	• SLOTH 2016 • SHAttered 2017
AES-CBC	• Vaudenay 2002 • Boneh/Brumley 2003 • BEAST 2011 • Lucky13 2013 • POODLE 2014 • Lucky Microseconds 2015
3DES	• Sweet32
RSA PKCS#1 v1.5	• Bleichenbacher 1998 • Jager 2015 • DROWN 2016
Compression	• CRIME 2012
Renegotiation	• Marsh Ray Attack 2009 • Renegotiation DoS 2011 • Triple Handshake 2014

NSA Reported in January 2021 on Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations

Attackers can exploit outdated transport layer security (TLS) protocol configurations to gain access to sensitive data with very few skills required. The graphic below depicts network traffic flows with various configurations, in an abstract manner. Updating TLS configurations to use strong encryption and authentication will help provide organizations with the cryptographic agility to stay ahead of malicious actors' capabilities and protect important information.

Network Traffic Encryption Types

- **Data at risk** Obsolete TLS
- **Data may be at risk** Authorized TLS with weak cipher suite
- **Data may be at risk** Authorized TLS with compliant cipher suite
- **Data protected** Authorized TLS with compliant cipher suite and strong key exchange methods

Data at Risk: Common types of data sent over TLS

- Proprietary information
- Network sensitive files
- Web traffic using HTTPS
- Social security numbers
- Passwords
- Travel information
- Online payment information
- Other sensitive files

Conclusion

SSL/TLS is a secure transport and session protocol designed to provide confidentiality and message integrity to web traffic.

SSL/TLS is established with a handshake that decides which cipher suite and master secret can be used.

SSL/TLS uses cryptography to encode data and hashing algorithms to maintain message integrity.

Many vulnerabilities have been discovered, and SSL and any version of TLS prior to 1.2 should not be used.

To mitigate known attacks, use TLS 1.3 when possible.

Reference Materials

References

- Mathy Vanhoef and Frank Piessens, iMinds-DistriNet, KU Leuven. 2015. " Numerous Occurrence MOnitoring & Recovery Exploit." *RC4 NOMORE.* Accessed November 2020. https://www.rc4nomore.com/.
- Brodie, Andy. 2017. "Overview of TLS 1.3." *OWASP The Open Web Application Security Project.* Accessed November 24, 2020. https://owasp.org/www-pdf-archive/TLS_v1.3_Overview_OWASP_Final.pdf.
- Cloudinsidr.com. 2018. *Known-attack-vectors-against-tls-implementation-vulnerabilities.* May 21. Accessed November 25, 2020. https://www.cloudinsidr.com/content/known-attack-vectors-against-tls-implementation-vulnerabilities/.
- Cybersecurity and Infrastructure Security Agency. 2014. "Alert (TA14-290A) SSL 3.0 Protocol Vulnerability and POODLE Attack." *CISA.* September. Accessed November 2020. https://us-cert.cisa.gov/ncas/alerts/TA14-290A.
- Hiwarale, Uday. 2020. "A brief overview of the TCP/IP model, SSL/TLS/HTTPS protocols and SSL certificates." *Medium.com.* February 1. Accessed November 25, 2020. https://medium.com/jspoint/a-brief-overview-of-the-tcp-ip-model-ssl-tls-https-protocols-and-ssl-certificates-d5a6269fe29e.
- Kerry McKay (NIST), David Cooper (NIST). 2019. *SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.* Government, Gaithersburg, Maryland: National Institute of Standards and Technology.
- Microsoft Research. 2014. "Triple Handshakes Considered Harmful:." *miTLS.* May. Accessed November 24, 2020. https://mitls.org/pages/attacks/3SHAKE.
- National Institute of Standards and Technology. 2020. *National Vulnerability Database.* November. Accessed November 2020. https://nvd.nist.gov/vuln/search

References

- Nohe, Pattrick. 2019. "Taking a Closer Look at the SSL/TLS Handshake." *hashedout by the SSL Store.* April 30. Accessed November 2020. https://www.thesslstore.com/blog/explaining-ssl-handshake/.
- Ritter, Tom. 2014. "Details on the Crime Attack." *NCCGROUP.* September 14. Accessed November 23, 2020. https://www.nccgroup.com/us/about-us/newsroom-and-events/blog/2012/september/details-on-the-crime-attack/.
- Robert Merget, Marcus Brinkmann, Nimrod Aviram,Juraj Somorovsky, Johannes Mittmann, Jörg. 2020. "Raccoon Attack: Finding and Exploiting Most-Significant-Bit-Oracles in TLS-DH(E)." *30th USENIX Security Symposium .* Vancoover, BC, Canada.
- The MITRE Corporation. 2020. *Common Vulnerabilities and Exposures.* November. Accessed November 2020. https://cve.mitre.org/cve/search_cve_list.html.
- Lehane, John. 2019. *Gigamon Blog.* April 30. Accessed November 24, 2020. https://blog.gigamon.com/2019/04/30/tls-by-the-numbers/.
- referralmd. 2019. "The Impact of Weak Protocols & Ciphers on Healthcare Servers." *referralmd.* Accessed January 29, 2021. https://getreferralmd.com/2019/11/impact-of-weak-protocols-ciphers-on-healthcare-servers/.
- National Security Agency. 2021. "NSA Cybersecurity Advisory: Eliminating Obsolete TLS Protocol Configurations." *National Security Agency Central Security Service.* January 5. Accessed January 29, 2021. https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2462345/nsa-releases-eliminating-obsolete-transport-layer-security-tls-protocol-configu/
- Zbigniew Banach. 2020. "How the BEAST Attack Works." *Netsparker.com.* January 17. Accessed February 4, 2021. https://www.netsparker.com/blog/web-security/how-the-beast-attack-works/.

Questions

Upcoming Briefs

- Next briefing

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm (EST), at **(202) 691-2110.**

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or call us Monday-Friday between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV