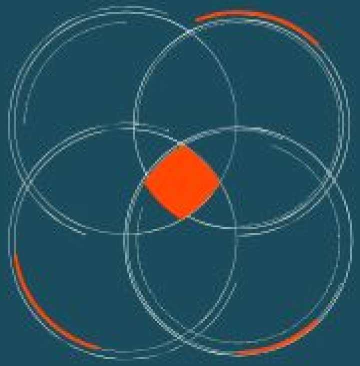
VMRacks
Managed Security Services

WHITE PAPER

THE IMPACT OF WEAK PROTOCOLS AND CIPHERS ON APACHE SERVERS FOR HEALTHCARE



Adam Bitting
Stephen Trout

Abstract

Secure internet communications in healthcare depend on effective end-to-end data protection technology, adapting to meet the challenges of ever-growing, sophisticated cyber attacks. The Transport Layer Security (TLS) protocol, along with it's now deprecated predecessor Secure Sockets Layer or SSL, has enabled these basic data protections for years, through complex, cryptographic protocols. These protocols serve to establish the secure channels most browsers utilize when visiting HTTPS sites.

Unfortunately, vulnerabilities in TLS protocols have led to major data breaches in recent years, potentially revealing the personal, protected healthcare information (PHI) of thousands of patients. To meet these mounting security challenges, TLS, like SSL before it, has needed to evolve, adapting to new protocol versions and technologies to secure privacy protections. These protections have since become standardized and required by such entities as the Department of Health and Human Services (HHS) in its HIPAA regulations, along with the National Institute of Standards and Technology (NIST).

Yet even as the algorithms or cipher suites used to perform encryption and decryption in TLS connections tend to become "weak" over time - due largely to the increasing sophistication of malicious attacks - it is incumbent for healthcare entities to keep pace with adopting the latest protocols. This White Paper examines current technology in cryptographic security for healthcare data, surveying hospital websites for their protocols at the present time, and urging the adoption of enhanced configuration methodologies for the widely relied upon Apache web server,

Table of Contents

01 Introduction

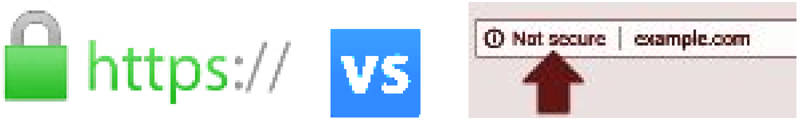
Like an older car with no seat belts installed, the internet was originally launched without the security protocols now required to protect personal data. Since the intent was to share only free, public information - both government-related and for academic pursuit - the fledgling internet protocols simply weren't designed to handle the flow of private, sensitive information.

Clearly, times have changed. Since the Hypertext Transfer Protocol, or HTTP (the set of rules used to communicate with web servers) was not designed to encrypt data, it became clear that both commercial business transactions and the transfer of personal data - such as protected health information (PHI) - could easily be intercepted. Like a passenger without a seatbelt, anyone handling sensitive data was at increasing risk for harm.

Enter the HTTPS protocol. With an encrypted layer wrapped around it (like a seatbelt), this protective barrier - commonly known as Transport Layer Security (TLS) - now provided a tunnel for authentication and data encryption between two different endpoints. Secure data transfer was enabled as the client's server request was confirmed by an SSL Certificate - an electronic document containing the server's public, cryptographic key - and the website traffic could then be authenticated as legitimate.

The Necessity of Encryption

Today, just as seat belts in cars are now the standard, current data protections for sensitive information rely on encryption as a baseline requirement. Fortunately, many websites today have adopted HTTPS (Hypertext Transfer Protocol Secure) for connections. This is now denoted by a green padlock in the Google Chrome browser address bar, with newer versions of the browser flagging HTTP sites as “Not Secure”. With HTTPS enabled, a web browser will check a website's security certificate and verify that it was issued by a legitimate certificate authority.



While this is a positive sign, it is critical that TLS/SSL be enabled with the latest protocol versions and cipher suites to ensure the strongest security. It is equally important to disable the older versions, including SSL 2.0 and 3.0, as well as TLS 1.0 and TLS 1.1. Additionally, the pervasive "heartbleed" vulnerability - not a protocol flaw, but an implementation bug which exploits a flaw in OpenSSL encryption software (a widespread implementation of SSL/TLS) and tricks websites, servers, and even medical devices into releasing sensitive information - must also be addressed by updating to the latest OpenSSl version.

Which SSL/TLS Version is Best?

At present, due to their use of older cryptographic techniques, all versions of SSL and TLS 1.0 protocols are susceptible to attacks such as the POODLE, SLOTH, and DROWN vulnerabilities, and should be disabled. The most widely accepted TLS protocol at the time of this writing is TLS 1.2, and unlike previous versions, now offers modern authenticated encryption (also known as AEAD). In other words, if you're not supporting TLS v1.2 *at a minimum,* your security is lacking.

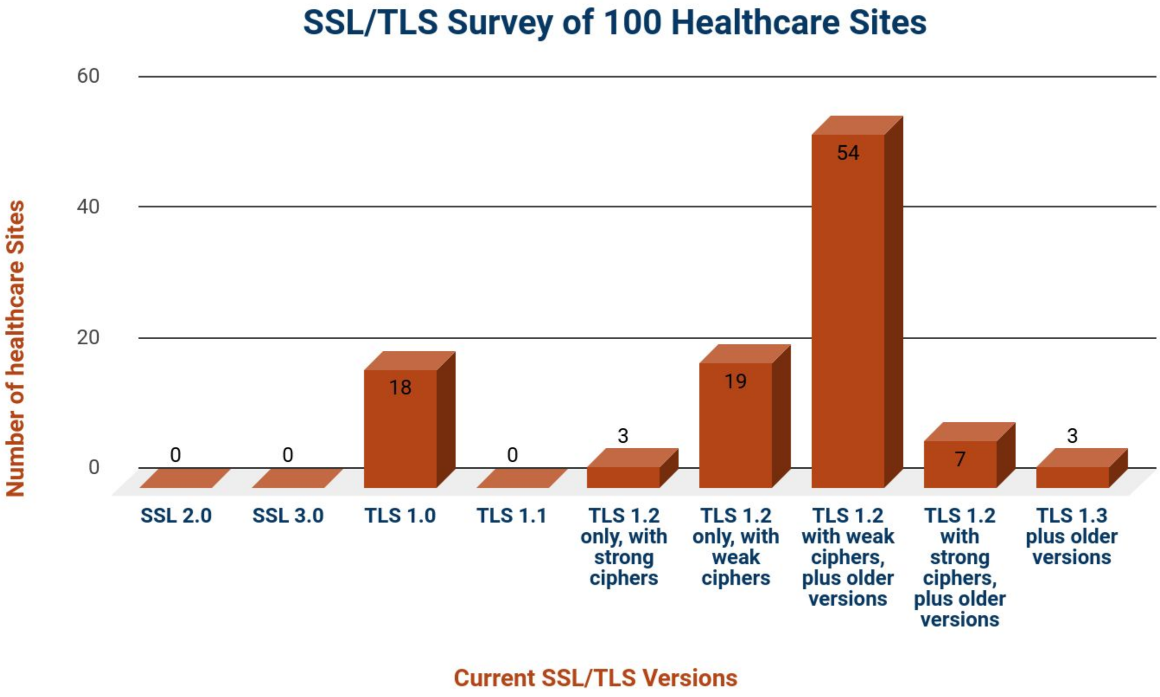
02 How Secure are Healthcare Sites?

Statistics reveal that hackers have found a veritable "gold mine" in holding health records for ransom - due in large part to SSL/TLS vulnerabilities. Primarily, it's the wealth of personal information these records contain - including social security numbers, financial information, and health insurance, combined with the relative ease of cracking into less than adequate health networks (substandard IT) - that literally make them a treasure trove for illicit profit.

Currently, a major cybersecurity study indicates that healthcare ranks 15th out of 18 major U.S. industries in terms of overall cyber health. In addition, a recent healthcare data breach report revealed that during the past seven years, a total of 2,149 breaches have occurred, amounting to 176.4 million patient records disclosed.

In an industry where protecting sensitive, personal and medical data is key, having the latest protocols and cipher suites is now a baseline necessity. Due to the quickly evolving, targeted nature of malicious attacks - such as the Heartbleed vulnerability (noted above) - the healthcare industry has been challenged to face emerging cybersecurity threats head-on. According to a recent Trustwave report, a healthcare record may now go for up to $250 on the black market, compared to $5.40 for a payment card.

So how are healthcare websites faring when it comes to replacing the weaker protocols and cipher suites? As VM Racks is actively working to increase data security in the field of healthcare, we decided to survey 100 large U.S. city hospitals to see what SSL/TLS versions and cipher suites their web server was supporting - whether SSL 2.0, 3.0, TLS 1.0, 1.1, or 1.2 versions (or a combination of these), and if they had a corresponding strong or weak cipher:



Here are the biggest takeaways from the survey:

- Only **3 out of 100** (3%) had enabled TLS 1.2 version *only*, with corresponding strong cipher suites
- 19% had enabled TLS 1.2 version *only*, but had not enabled strong ciphers
- More than half, **or 54%**, were using TLS 1,2 version with weak ciphers, *as well as supporting older SSL/TLS versions*
- 7% had enabled TLS 1.2 version with strong ciphers, *but were also supporting older TLS versions*

An encouraging sign is that 83% of the healthcare sites surveyed have at least adopted TLS 1.2 version or better. This is progress, and may in part be due to the PCI DSS standard which required that all sites accepting credit card payments remove support for TLS v1.0 by June 2018. The bad news - and this is significant - is that ***almost all sites surveyed*** **have a weakness in their security.**

The majority of healthcare sites surveyed (97%) have a weakness which leaves them vulnerable to attack - either because they continue to support older, weaker TLS versions at various locations in their system, and/or they have not enabled the strongest ciphers.

In order to support older clients ("backwards compatibility"), some healthcare companies continue to support TLS v1.0 and TLS v1.1 - for now. However, they must understand that they do so at great risk. Even TLS version 1.2 has become increasingly vulnerable to the new, so-called "man-in-the-middle" or eavesdropping attacks, initiated through phishing emails or by connecting to unsecured servers where traffic may be monitored by an attacker.

We should note that at the time of this writing, the TLS v1.3 protocol - touting more robust security and improved speed - is currently being unveiled. TLS 1.3 will remove all obsolete or insecure features and support for legacy encryption algorithms; however, it has yet to obtain widespread adoption.

03 TLS and the Apache Server

In 2014, the Heartbleed vulnerability, capitalizing on a flaw in the OpenSSL implementation of the TLS/DTLS "heartbeat functionality," was utilized by hackers to steal security keys from Community Health Systems - a major U.S. hospital chain - and effectively compromise the confidentiality of approximately *4.5 million patient records.*

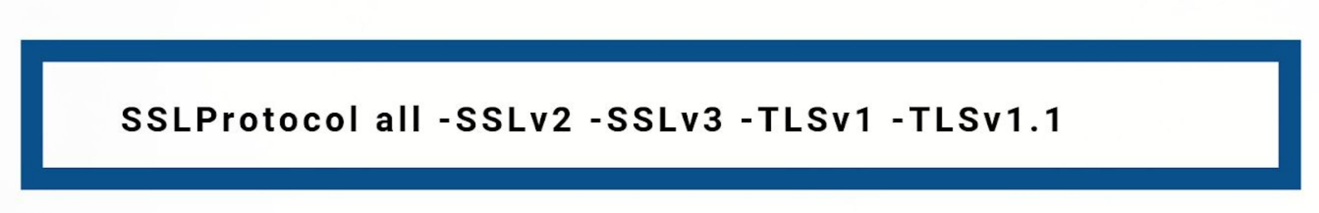
Since the POODLE vulnerability (2014) had significantly weakened SSL version 3.0 and allowed attackers to exploit its design and decrypt data, SSL 3.0 was deemed an unsafe protocol. Additionally, BEAST (first demonstrated in 2011), and CRIME (2012), have also impacted the later TLS 1.0 and TLS 1.1 versions. While the latter two versions are due to be officially deprecated by Google, Microsoft, Mozilla, and Apple in 2020 - with TLS 1.2 becoming the default version - it should be noted that continuing to run anything *less than* TLS 1.2 *right now* means that these networks remain a target.

In light of these vulnerabilities, the System Administrators at VM Racks routinely disable weak ciphers and allow only the latest, strong ciphers in HTTPS connections. As noted, currently the TLS 1.2 protocol is the accepted standard necessary to effectively enhance server security.

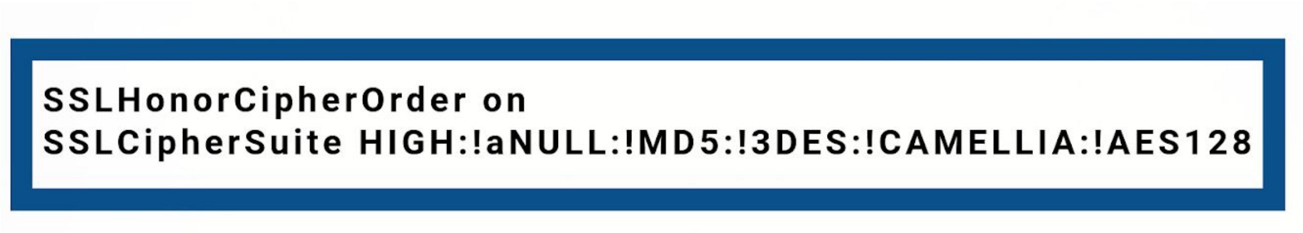
Configuring the Apache Server

The Apache Server powers more than half of all websites globally, making it by far the most popular open-source web server going. Unfortunately, it has also been the victim of numerous Heartbleed-like vulnerabilities. Apache most often runs on Linux, using cipher suites to encrypt and protect personal data. As noted, some of those ciphers may be weak, and some are strong.

The following will update SSL protocols and ciphers in Apache Server, by removing support for TLS versions 1 and 1.1, and disabling SSLv2 and SSLv3:



```
SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
```



```
SSLHonorCipherOrder on
SSLCipherSuite HIGH:!aNULL:!MD5:!3DES:!CAMELLIA:!AES128
```

Unfortunately, new variants of SSL/TLS attacks continue to be released regularly, so vigilance is required. Practically, this means that cybersecurity - especially for those who handle protected health information (PHI) - must be viewed as an ongoing and evolving process, not a one-time event (eg, purchasing a new firewall or anti-virus subscription).

04 Summary

With the prevalence of healthcare data breaches in recent years, it behooves healthcare organizations to become increasingly proactive in their data security. Cybersecurity, with all the implications inherent in that goal, must now be seen as an investment that healthcare companies commit to *for the long-term* - not merely because HIPAA requires it, but because the lives and welfare of real people are at stake. In essence, cybersecurity is now becoming a *vital part of patient care,* properly understood as *a change in culture and evolving process* - not a one-time event. As part of this new culture, an annual security risk assessment is crucial.

Healthcare servers must be configured for the latest security protocols - TLS 1.2 at minimum - with corresponding strong algorithms and cipher suites to withstand malicious attacks on sensitive data. At the same time, organizations must identify older, legacy protocols as part of their regular risk assessments, jettisoning them as quickly as possible in order to fix the holes through which vulnerabilities may enter.

Malicious attacks will continue to evolve, like mutating viruses that adapt to survive. Hackers and social engineers do much the same. Because this is so, risk must be reevaluated regularly. Adopting the latest security protocols as a strategic part of a company-wide cybersecurity plan will help to minimize risk, while positively impacting patient care.