Top 5 SSL/TLS Attack Vectors

How they have impacted IT and how you can avoid them
Hackers are getting increasingly sophisticated with their threats, and smaller businesses are now being targeted more than ever. In fact, the last five years have shown a steady increase in attacks targeting businesses with less than 250 employees.¹ When well-administered, SSL/TLS is an extremely effective data safety measure; however, it does require organizations pay attention to certain details and critical factors—or the hackers will find a way in.

SSL/TLS vulnerabilities exist in a lot of places, but there are five in particular that have recently plagued IT operations staff like none other:

- Heartbleed
- POODLE
- FREAK

Let’s talk about how these vulnerabilities impacted IT and the lessons we can learn from these potential attack vectors.

**SSL/TLS Attack Vector #1: Heartbleed**

One of the most impactful SSL/TLS bugs discovered to date, Heartbleed is a critical vulnerability in OpenSSL, a widely used cryptographic software library. This bug makes it possible for attackers to see the contents of the server memory, including data that may hold certificate private keys and authentication information such as cookies and passwords, allowing the attacker to masquerade as the rightful user.

**Heartbleed Fallout**

When it was first discovered, Heartbleed affected 17 percent of SSL/TLS secured websites, impacting more than 600,000 web servers.² Most notably, the Heartbleed vulnerability caused the exposure of 4.5 million patient records at Ohio-based Community Health Systems.³

**SSL/TLS Attack Vector #2: POODLE**

What people refer to as SSL/TLS today is actually TLS, with the most recent version of TLS being TLS 1.2. The attack vector POODLE (Padding Oracle On Downgraded Legacy Encryption) made it possible for attackers to take advantage of people supporting old versions of SSL 3.0 in tandem with TLS 1.2 to downgrade all connections to the less secure version and decrypt secure cookies sent over an SSL/TLS connection.

**POODLE Fallout**

Even five months after POODLE was first made public, 50% of the internet had not disabled SSL 3.0 on its sites, leaving 10 million sites vulnerable.⁴
SSL/TLS Attack Vector #3: FREAK
A classic man-in-the-middle attack, FREAK allows attackers to get between a client and server to snoop on private communications. It came as the result of a flaw in OpenSSL client software and was easily exploitable on poorly configured web servers.

FREAK Fallout
FREAK impacted hundreds of millions of iPhone, iPad and Android users. FREAK also affected all versions of Microsoft Windows.

SSL/TLS Attack Vector #4: Shellshock Bash Bug
Shellshock was the catchy name researchers made for a bug in Bash, a shell used in Unix operating systems, including the Linux OS versions popular on most web servers today. The vulnerability gave attackers an opening to potentially plant malware on web servers that could be served up to unsuspecting site visitors.

Shellshock Fallout
70% of web servers run on Linux and were potentially at risk. Though it wasn't directly related to SSL/TLS per se, Shellshock highlights how sites protected by SSL/TLS can still put visitors at risk without effective security hygiene on the server environment.

SSL/TLS Attack Vector #5: Bar Mitzvah Attack
Security researchers have now shown that a 13-year-old weakness in the RC4 encryption algorithm supported by many browsers and servers makes it possible for attackers to sniff credentials and other information during an SSL/TLS session.

Bar Mitzvah Fallout
Although AES encryption is currently in favour, 30% of TLS sessions still use RC4, which has been obsolete for more than a decade.

SSL/TLS Best Practices
In all of these cases, a joint effort between the organization and its CA can ensure minimal risk to the organization. To ensure that the encryption process can't be infiltrated, the website and CA must work together to ensure they are adhering to the following best practices:

Key length: Encryption algorithms must continually be updated to account for new capabilities in cracking old cryptography. Key length is a crucial variable in this upgrade process. As things stand, SSL/TLS certificate keys need to be at least 2048-bit RSA or 256-bit ECC to avoid being easily attacked and unencrypted by unauthorized parties.

Strong hash algorithm: As with key length, hash algorithms can also become obsolete. Today the only secure standard used for SSL/TLS certificates is SHA-2.

Root certificate security: CAs base all of the certificate key pairs they issue to customers off of a root certificate held internally at that CA. The value of that certificate must be heavily guarded by the CA, as the trustworthiness of all derivative certificates depends on the integrity of that root certificate.

Security of systems storing and using private SSL/TLS keys: The businesses to which CAs issue certificates must guard their private SSL/TLS keys religiously. These keys are the basis of trust for an organization's entire web infrastructure, and if they are compromised, attackers can easily spoof websites and act as impostors to unsuspecting web users.
Choosing the right CA and certificate product will help with the first three items, but the last one can create potential vulnerabilities, depending on the SSL/TLS the business is using and how they are managing it.

Organizations should seek out CAs that will respond quickly to re-key affected certificates when new attack vectors and vulnerabilities present themselves.

Similarly, an effective CA should also offer free vulnerability assessments and malware scans to help organizations to whom they issue certificates to understand where SSL/TLS risks lie. On the other side of the fence, the certificate-using organization itself needs to be prepared to patch systems in a timely fashion and rely on the most up-to-date TLS versions in order to ensure their SSL/TLS ecosystem depends on the most secure components.

The Importance of Your Certificate Authority

Work with a trusted CA that can handle any storm. While there are many new CAs on the market now that have sold their certificates based solely on price point, cost should only be one component in the evaluation process. An established CA with a solid reputation is more likely to address emergencies like Heartbleed, POODLE, FREAK, and Bash bug in a timely fashion. Low-cost CAs may not be nearly as responsive.

As the first CA in existence, Symantec has the legacy and the resources to support its certificate customers in good times and bad. As a company, Symantec’s internal security over root certificates and certificate infrastructure is impeccable. Since 2004, our trust services division has ensured a remarkable 100% uptime.9

Symantec also supports clients with up-to-date vulnerability and malware scanning and offers a free SSL/TLS tool to check the security configuration and vulnerability status of individual certificates.

To check your security status, go to https://cryptoreport.websecurity.symantec.com/checker.

Since 2004, our trust services division has ensured 100% uptime.9

---

2. “More Than a Half-Million Servers Exposed to Heartbleed Flaw,” InformationWeek, April 9, 2014
8. “SSL/TLS Suffers 'Bar Mitzvah Attack,'” InformationWeek, March 26, 2015
For global offices and contact numbers, please visit our website.

For product information in the U.S., call:
1-866-893-6565 or 1-520-477-3111

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/ssl

For product information in Asia Pacific, call:
Australia: +61 3 9674 5500
New Zealand: +64 9 9127 201
Singapore: +65 6622 1638
Hong Kong: +852 30 114 683

Symantec Website Security Solutions Pty Ltd
3/437 St Kilda Road, Melbourne, 3004
ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates

For product information in the Americas (Non-U.S.), call:
Mexico: 554 738 0448
Brazil: 800 038 0598

For product information in the U.K., call:
0800 032 2101 or +44 (0) 208 6000 740

Symantec (UK) Limited
350 Brook Drive
Green Park, Reading
Berkshire, RG2 6UH UK
www.symantec.co.uk/ssl

For product information in Europe, call:
+353 1 793 9053 or +41 (0) 26 429 7929
Germany: 0800 128 1000
France: 0800 90 43 51
Spain: 900 93 1298

Follow Us: