radware

SSL Attacks on the Rise

Protective Technology Turned Attack Vector

Table of Contents

01 SSL as an Attack Vector

02 Different Types of SSL/ Encrypted Attacks

03 Different Than SSL Vulnerabilities

04 SSL Everywhere

05 Not Just for Commerce

06 Complicating Detection and Stressing Mitigation Performance

07 Asynchronous Traffic

08 Strategies for Protection from SSL Attacks

01

SSL as an Attack Vector

It's been over 20 years since the earliest versions of the Secure Socket Layer (SSL) protocol emerged from a team of engineers at Netscape Communications. As the Internet and more specifically the World Wide Web began its precipitous climb in the early 1990's these engineers recognized that to drive deeper interactions online, a standard for securing communications would need to be widely adopted.

As is always the trend, mass adoption of certain technologies is followed closely by efforts to exploit its wide use through a number of security threats. SSL is no exception to this rule, and has experienced a large number of highly publicized vulnerabilities that force users to move to new, more secure versions and ultimately a replacement protocol such as Transport Layer Security (TLS).

However, exploits of newly identified vulnerabilities are not the only way that SSL adoption is being used as a weapon in the hands of malicious attackers and adversaries behind cyber threats. SSL is increasingly being used to mask and further complicate attack traffic detection in both network and application level threats.

02

Different Types of SSL/ Encrypted Attacks

Cyber-attacks, including Distributed Denial of Service (DDoS) attacks and advanced web application attacks continue to plague businesses as they move to more online operations. For both types of attacks, those leveraging encrypted traffic as an attack vector are on the rise, further challenging many of the cyber threat solutions currently in place. Most cyber-attack mitigation technologies do not actually inspect SSL traffic, as it requires decrypting the encrypted traffic. According to Radware's 2014 Global Network and Application Security Report, as much as 25% of attack activity today is using SSL-based attack vectors.

SSL-based attacks take many forms, including:

ENCRYPTED SYN FLOODS

These attacks are similar in nature to standard, non-encrypted SYN flood attacks by exhausting resources in place to complete the SYN-ACK handshake. The difference is these attacks further complicate the challenge by encrypting traffic and forcing use of SSL handshake resources.

SSL RENEGOTIATION

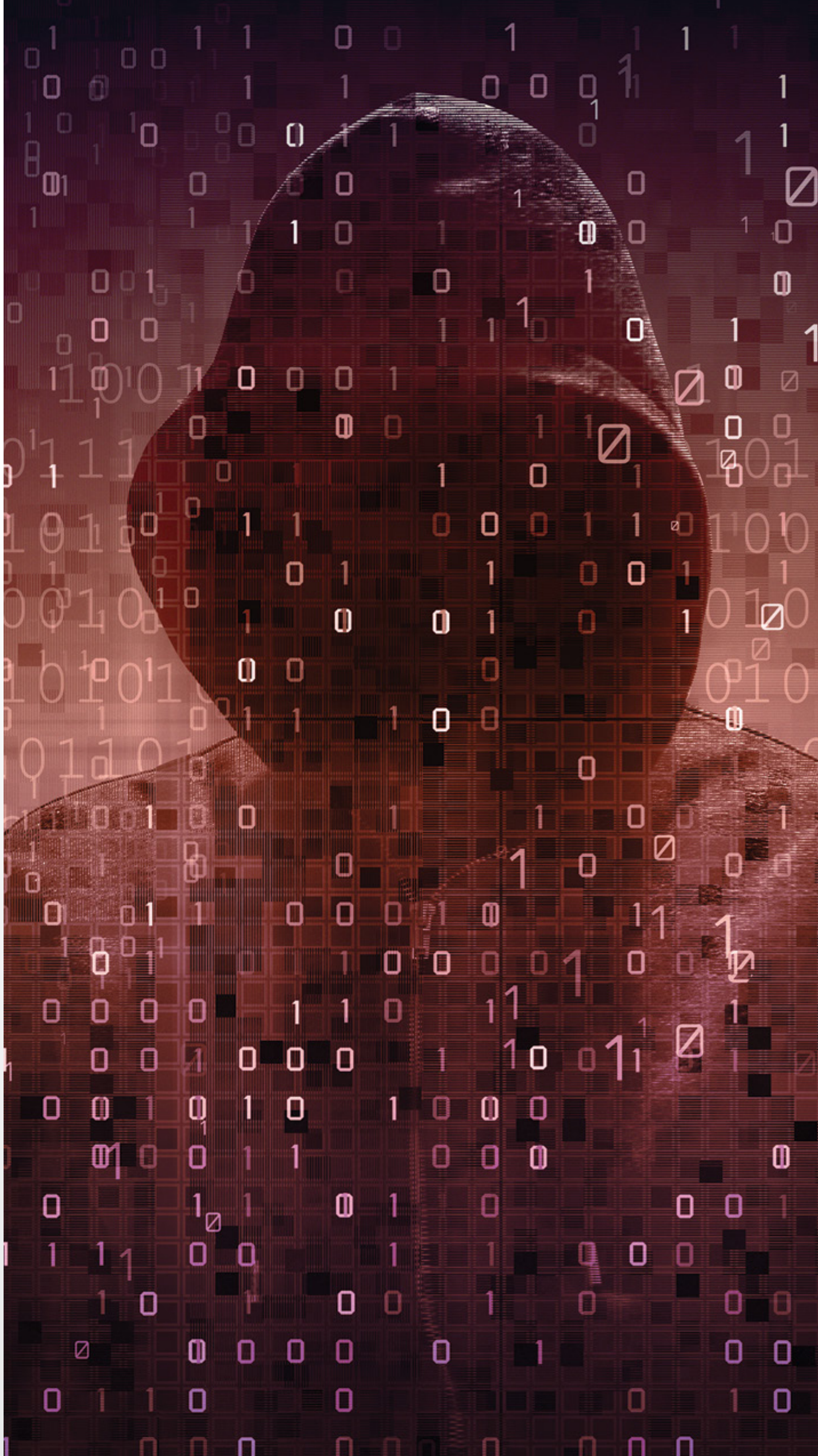
Work by initiating a regular SSL handshake, and immediately requesting for the renegotiation of the encryption key. The tool constantly repeats this renegotiation request until all server resources have been exhausted.

HTTPS FLOODS

Generate floods of encrypted HTTP traffic, often as part of multi-vector attack campaigns. Compounding the impact of “normal” HTTP Floods, encrypted HTTP attacks add several other challenges, such as the burden of encryption and decryption mechanisms.

ENCRYPTED WEB APPLICATION ATTACKS

Multi-vector attack campaigns also increasingly leverage non-DoS, web application logic attacks. By encrypting the traffic, these attacks often pass through both DDoS and web application protections undetected.



03

Different Than SSL Vulnerabilities

The Information Technology universe that leverages SSL got a major wake-up call in April 2014 with the disclosure of the Heartbleed vulnerability associated with OpenSSL implementations. While far from the first, Heartlbleed was arguably the SSL vulnerability with the widest potential reach and impact, as an estimated 17% of SSL implementations were using the vulnerable instance of OpenSSL software.

Some other major SSL vulnerabilities have emerged over the years, including the long standing (and still impactful) RC4 vulnerability originally discovered in 2002, and the more recent POODLE vulnerability that exploits some software logic to failback to SSL 3.0 (exposing other known vulnerabilities).

These SSL vulnerabilities are not directly related to the SSL DDoS and advanced web application attacks described earlier. However, these vulnerabilities can cause a distraction from addressing broader non-vulnerability based attack weaknesses, and highlight the tendency towards exploitation of broadly adopted technologies.

04

SSL Everywhere

Despite some high profile security issues, SSL (and TLS) remain the standards for ensuring secure communications and commerce on the web, and has seen dramatic growth in recent years. When SSL was conceived and introduced, a relatively small number of businesses had websites, and even fewer were managing commerce or critical aspects of business operations online. Today, most businesses of reasonable size have an active website to drive consumer engagement and at a minimum, properly secure communications (if not transactions) through its website.

According to Netcraft, the use of SSL by the top one million websites has increased by 48% over the past two years. As more and more sites add SSL or TLS capabilities, user adoption in turn also increases.

The technology industry has actively been pushing broader adoption of SSL/TLS through initiatives such as the “Let’s Encrypt” project that is launching a new, free certificate authority in an effort to move more users over to encrypted online communication and commerce.

05

Not Just for Commerce

For many years, it was recommended to implement SSL to support ecommerce sites or any credit card transactions. Those limitations have gone away with the growth of other purposes for secure communications. One area of dramatic growth is encrypted email services.

A recent series of attacks highlighted how providers of encrypted service can become targets for encrypted attacks. ProtonMail is a leading provider of encrypted email services, providing a secure means of communication to over 500,000 users. In November 2015, ProtonMail was targeted with a series of advanced DDoS attacks that included volumetric attacks over 100 Gbps as well as application layer attacks. The attacks also included multiple encrypted attack vectors including SSL SYN flood attacks that required advanced behavioral analysis to identify malicious traffic and maintain legitimate encrypted traffic flows.

06

Complicating Detection and Stressing Mitigation Performance

In the same way SSL and encryption protect the integrity of legitimate communications, it equally obfuscates many attributes of traffic used to determine if it malicious versus legitimate. Identifying attack traffic within encrypted traffic flows is akin to finding a needle in a haystack in the dark. Most cyber-attack solutions struggle to identify potentially malicious traffic from encrypted traffic sources and isolate it for further analysis (and potential mitigation).

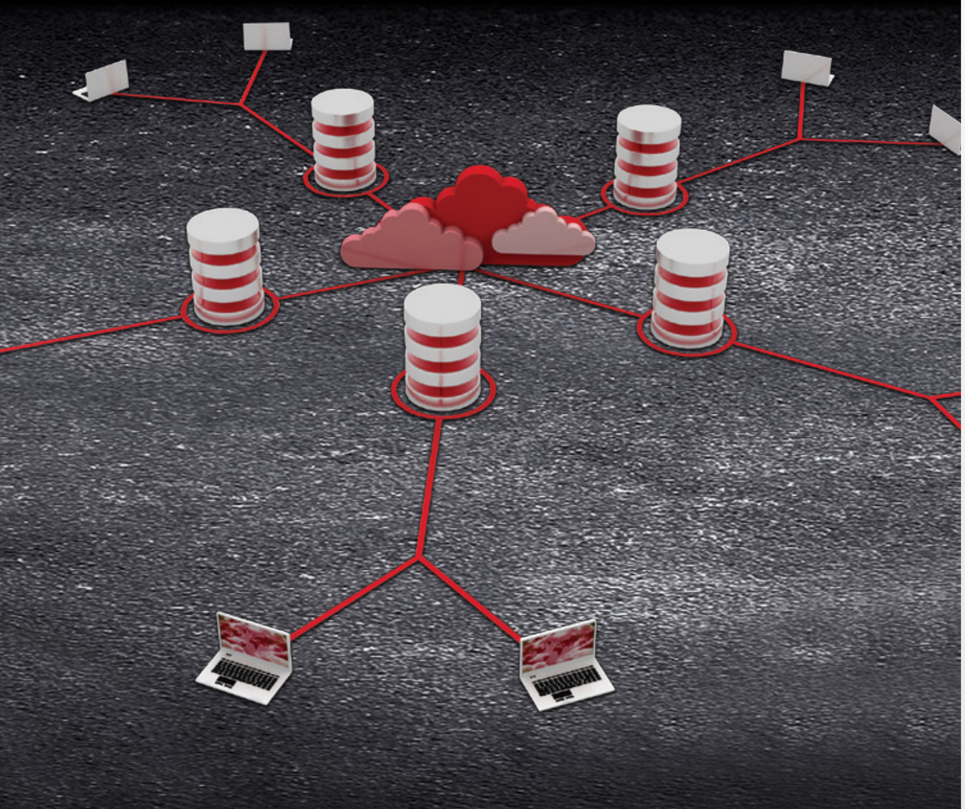
The other major advantage that SSL attacks offer to attackers is the ability to put significant computing stress on network and application infrastructures targeted. The process of decrypting and re-encrypting SSL traffic increases the requirements of processing the traffic, in many cases beyond the functional performance of devices used for attack mitigation.

Most are inline and stateful and cannot handle SSL encrypted attacks, making it vulnerable to SSL flood attacks. Fewer of these solutions can be deployed out-of-path, which is a necessity for providing protection while limiting impact on legitimate users.

Many solutions that can do some level of decryption tend to rely on rate limiting the rate of request, which results in dropped legitimate traffic and effectively completes the attack. Finally, many solutions require the customer to share actual server certificates, which complicates implementation, certificate management and forces customers to share private keys for protection in the cloud.

07

Asynchronous Traffic



SSL attacks are becoming more popular among attackers as it only requires a small number of packets to cause denial of service for a fairly large service. Attackers launch attacks that use SSL because each SSL session handshake consumes 15 times more resources from the server side than from the client side, meaning the attack has exponentially increased in size without requiring additional bots or bandwidth. As a result of these amplification effects, a single standard home PC can take down an entire SSL-based web server, while several computers can take down a complete farm of large, secured online services.

08

Strategies for Protection from SSL Attacks

For more information about
Radware SSL cyber attack protection, visit:
http://radware.com/solutions/ssl-attack-protection/

The unfortunate reality is that the majority of DDoS attack protection solutions only provide protection for certain types of attacks, and in many cases struggle with SSL attacks. The bottom line is that to provide effective protection, solutions need to delivery full attack vector coverage (including SSL), high scalability to meet the growing demands of the consumer, and innovative ways to minimize if not eliminate these threats.

Radware offers the industry's most complete SSL attack mitigation solution. The solution meets the needs of high capacity mitigation solutions, supports all common versions of SSL and TLS, and isolates suspicious encrypted traffic using behavioral analysis to limit legitimate user impact. It provides advanced challenges/response mechanisms to validate encrypted traffic flagged as suspicious but only impacts the initial user session. Authenticated user sessions pass through unimpacted, providing zero latency in peacetime and minimal latency when under attack.

Radware offers its solution in asymmetric deployment where only ingress encrypted traffic passes through the mitigation engine. The solution can integrate defense messaging between DDoS and WAF components to do analysis and mitigation of advanced encrypted attacks over HTTPS with signaling to perimeter defense. This allows for WAF level protection at line speed with no additional latency for legitimate users.