BEAST Attack

Vivek.Yadav

26 October 2019

1 Introduction

BEAST is short for Browser Exploit Against SSL/TLS revealed in Sep 2011 therefore, early SSL/TLS is an unsafe method to protect sensitive data [1].

1.1 About

BEAST Attack is most commonly triggered if the HTTPS connections is configured with older versions of TLS/SSL (TLSv1.0, SSLv3.0 and lower). A practical way to exploit a vulnerability in older versions of TLS/SSL (TLSv1.0, SSLv3.0 and lower) has been discovered by Security researchers Thai Duong and Juliano Rizzo [2].

1.2 After Discovery and Effects

After discovery of the vulnerability by security researchers, there was research going on related to practical use of the vulnerability for exploitation in the past but lucky there was no such incident found.

The early SSL/TLS can be exploited by leveraging the weakness in cipher block chaining (CBC) through block-wise attack [2]. It makes easier for the attacker to perform Man in the Middle attack [3]. This could be very damaging for the victim because the sensitive data can be decrypted and used for malicious activity.

2 Cipher Block Chaining

In order to under the block-wise attack we have to first understand about the Block Cipher and Cipher Block Chaining (CBC).

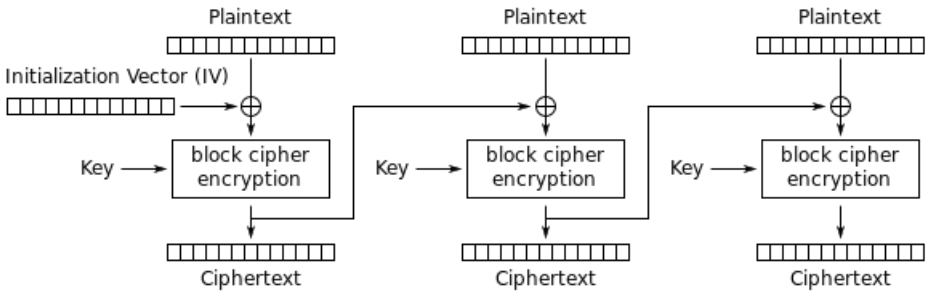
2.1 Block Cipher

Block Cipher is is a deterministic algorithm (always produces same output for a particular input) operating on fixed-length groups of bits, called blocks, with symmetric key specifying an unvarying transformation [4]. Block ciphers are

widely used in the many algorithms such as Blowfish, RC5, Rinjndael/AES, IDEA, Lucifer/DES.

2.2 Cipher Block Chaining (CBC)

It was invented by Ehrsam, Meyer, Smith and Tuchman and used for operating the block ciphers, intended to securely transmit multi-block data message between two stations [5]. An initialization vector is used for the encryption and uniqueness of the first block.

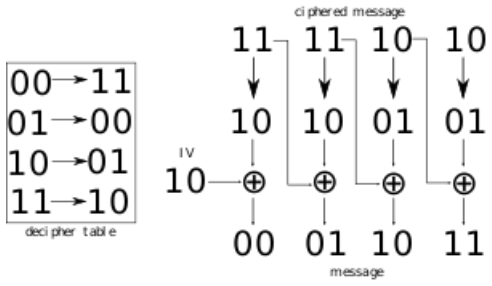


Cipher Block Chaining (CBC) mode encryption

...Image 1 [6]

If the first block has index 1, the mathematical formula for CBC encryption is:
$C_i = E_K(P_i \oplus C_{i-1})$,
$C_0 = IV$[6]

while the mathematical formula for CBC decryption is:
$P_i = D_K(C_i) \oplus C_{i-1}$,
$C_0 = IV$[6]



...Image 2 [6]

All the cipher-text blocks after the first cipher text blocks use previous cipher text blocks replacing the initialization vector. Therefore, each block of plaintext, before getting encrypted, is XOR(ed) with the previously encrypted ciphertext block [5].

2.3 Drawback

However, some experts warn against certain vulnerabilities of cipher block chaining, including the use of predictable initialization vectors. Research

..TODO.. (To much for now)

3 Blockwise Attack (BA) model

To understand this attack model we have to learn about the security notions and plaintext-recovery attack.

Security Notions: The security goal and an attack model together in combination define the secuity notions [7]. The better security notions are displayed by the attack model that can accurately capture the attackers in the real world, therefore, it was explained that the BA model has a better security notions since it captures real world attackers very well [2].

Plaintext-Recovery Attack: In [8] Joux, Martinet and Valette, used the Dai's attack to highlight the fact that after only two encrypted blocks, the BA model with the CBC encryption scheme is not secure; there is a process mentioned in [2] exposing this vulnerability by conducting the plaintext-recovery attack against CBC in the Blockwise Chosen-Boundary Attack (BCBA).

3.1 Proof of Concept

The SSL is compromised by hackers which allows them to decrypt the encrypted data communication between the webserver and the end-user in significantly less amount of time, without having the knowledge of the security breach by any party [9]. The process to extract the unencrypted plaintext from an encrypted session have been fairly demonstrated by Thai Duong and Juliano Rizzo [10].

4 Security Against BEAST Attack

A famous quote from Bruce Schneier's book 'Beyond Fear', "We don't need to learn something completely new; we need to learn to be smarter, more skeptical, and more skilled about what we already know" [11], explicitly means that being alert and upto date can guarantee most of the safety.

(Directly cited from [12]) BEAST has three conditions that must be met for this attack to take place:

- JavaScript or applet injection into the same origin of the web site

- An attacker could inject a java applet into the page with either XSS or intercepting a request for a valid applet
- Network sniffing of the connection must be possible
- A vulnerable version of SSL must be used which is using a block cipher

4.1 Protection

Use Latest TLS: Disable TLS 1.0 and below on Apache, NGINX and IIS and use the latest one.

..TODO.. (To much for now).. Gather Content from the web site Gather

Be Alert: Adhering to the basic checks mentioned below can avoid from becoming the victim:

- Web Server Environments still using early SSL/TLS must upgrade to the latest SSL/TLS
- Update the browser to the latest stable version
- Check the TLS version in the browser, being used for communication
- Plugin that are not updated are prone to security breach even if the latest version of SSL/TLS is being for the purpose of communication.

References

[1] "P.c.i security standards council: Migrating from ssl and early tls."

[2] T. Duong and J. Rizzo, "Here come the ninjas," *Unpublished manuscript*, vol. 320, 2011.

[3] "Ssl/tls information disclosure (beast) vulnerability." [Online]. Available: https://docs.secureauth.com/pages/viewpage.action?pageId=14778519

[4] N. Ferguson, B. Schneier, and T. Kohno, "Cryptography engineering," *Design Princi*, 2010.

[5] W. F. Ehrsam, C. H. Meyer, J. L. Smith, and W. L. Tuchman, "Message verification and transmission error detection by block chaining," Feb. 14 1978, uS Patent 4,074,066.

[6] "Cbc encryption." [Online]. Available: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#CBC

[7] P.-A. Fouque, A. Joux, and G. Poupard, "Blockwise adversarial model for on-line ciphers and symmetric encryption schemes," in *International Workshop on Selected Areas in Cryptography*. Springer, 2004, pp. 212–226.

[8] A. Joux, G. Martinet, and F. Valette, "Blockwise-adaptive attackers revisiting the (in) security of some provably secure encryption modes: Cbc, gem, iacbc," in *Annual International Cryptology Conference*. Springer, 2002, pp. 17–30.

[9] D. Goodin, "Hackers break ssl encryption used by millions of sites," Sep 2011. [Online]. Available: https://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/

[10] Duong, "Beast," Sep 2011. [Online]. Available: https://vnhacker.blogspot.com/2011/09/beast.html

[11] B. Schneier, *Beyond fear: Thinking sensibly about security in an uncertain world*. Springer Science & Business Media, 2006.

[12] Ctxis, "Server technologies - https beast attack." [Online]. Available: https://www.contextis.com/en/blog/server-technologies-https-beast-attack