*Attacking SSL/TLS Implementations*

Shawn Philip Babu  
Information Systems Security  
Concordia UniversityMontreal, Canada  
shawn0111babu@mail.com  
  
line 1: 2nd Given Name Surname  
line 2: *dept. name of organization (of Affiliation)*  
line 3: *name of organization (of Affiliation)*line 4: City, Country  
line 5: email address or ORCID  
  
line 1: 3rd Given Name Surname  
line 2: *dept. name of organization (of Affiliation)*  
line 3: *name of organization (of Affiliation)*line 4: City, Country  
line 5: email address or ORCID  
  
line 1: 4th Given Name Surname  
line 2: *dept. name of organization (of Affiliation)*  
line 3: *name of organization (of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

line 1: 5th Given Name Surname  
line 2: *dept. name of organization (of Affiliation)*  
line 3: *name of organization (of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

line 1: 6th Given Name Surname  
line 2: *dept. name of organization (of Affiliation)*  
line 3: *name of organization (of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

*Abstract*—SSL stands for Secure Sockets Layer and, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details. TLS (Transport Layer Security) is just an updated, more secure, version of SSL. We still refer to security certificates as SSL because it is a more commonly used term, but when you are [buying SSL](https://www.websecurity.digicert.com/ssl-certificate?inid=infoctr_buylink_sslhome) from DigiCert you are actually buying the most up to date TLS certificates with the option of [ECC, RSA or DSA encryption](https://www.websecurity.digicert.com/security-topics/how-ssl-works). However, there are undeniable differences between the libraries that implement SSL/TLS protocol and vulnerabilities in these libraries. Hence, the two main questions asked are: what’s the difference between TLS vs SSL? And is it something we need to worry about? In this report, we summarize some of the limitations by considering implementations of each along with review of past protocol-based and software-based vulnerabilities.

# Introduction

JEMY & EKASMEET

(Times new roman 10)

# Limitation of SSL/TLS Implementations

SHAWN & HARSHITHA

(Times new roman 10)

# How SSL/TLS secure data ?

VENKY & SANDEEP

(Times new roman 10)

# Comparisions of DIfferent versions of SSL/TLS

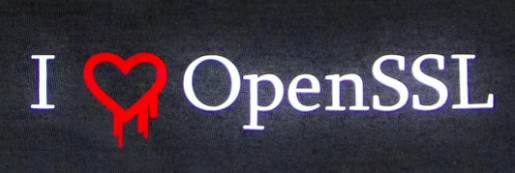
VENKY & SANDEEP

(Times new roman 10)

# Vulnerabilities in SSL/TLS-Protocol based

**Heartbleed attack:**

Heartbleed is a security vulnerability that was discovered in April 2014 and has been widely regarded as one of the most significant security breaches in recent years. It affected the popular OpenSSL cryptographic software library, which is used to secure communications over the Internet, including email, messaging, and online transactions.

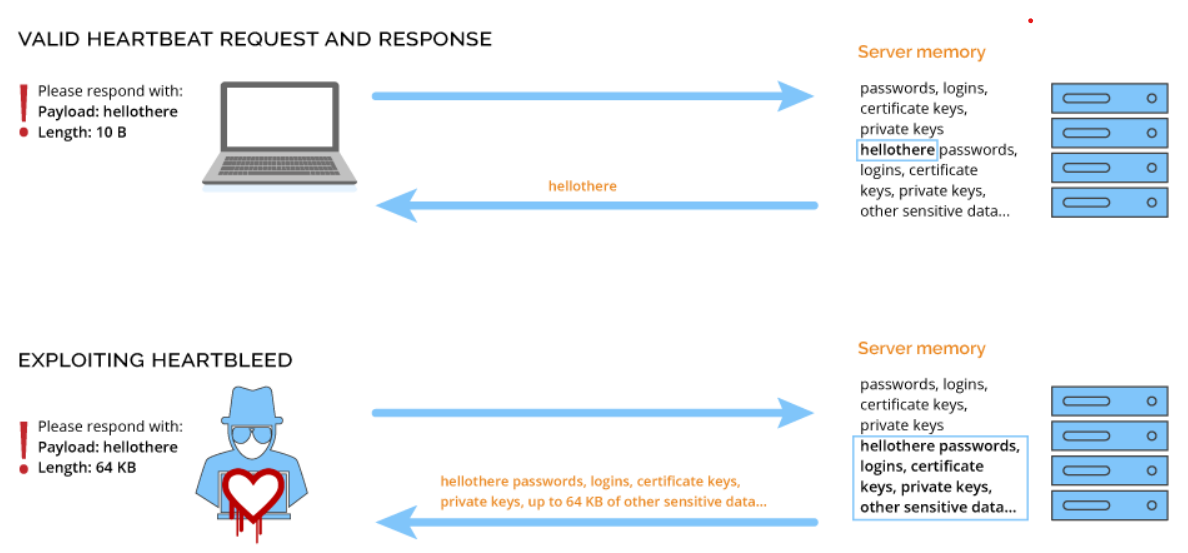


**Working:**

The Heartbleed attack exploits a flaw in the OpenSSL implementation of the Transport Layer Security (TLS) heartbeat extension. This extension is used to check if a connection between a client and a server is still active. The server sends a small message, known as a heartbeat message, to the client, which responds with the same message to indicate that the connection is still active.

The vulnerability in the OpenSSL implementation allowed an attacker to send a malformed heartbeat message to a server running a vulnerable version of OpenSSL. This malformed message could trick the server into sending back a larger response than intended, which could include sensitive information from the server's memory.

The attacker could then retrieve this sensitive information, such as passwords, credit card numbers, and other data, from the server's memory. This attack could be repeated multiple times, allowing the attacker to gather large amounts of sensitive information.



**Mitigation:**

1. Applying security patches
2. Changing passwords

**POODLE attack:**

POODLE, which stands for **Padding Oracle On Downgraded Legacy Encryption**, is a security vulnerability that was discovered in October 2014. It is a flaw in the design of SSL 3.0, an older version of the SSL/TLS encryption protocol that is used to secure Internet communications.

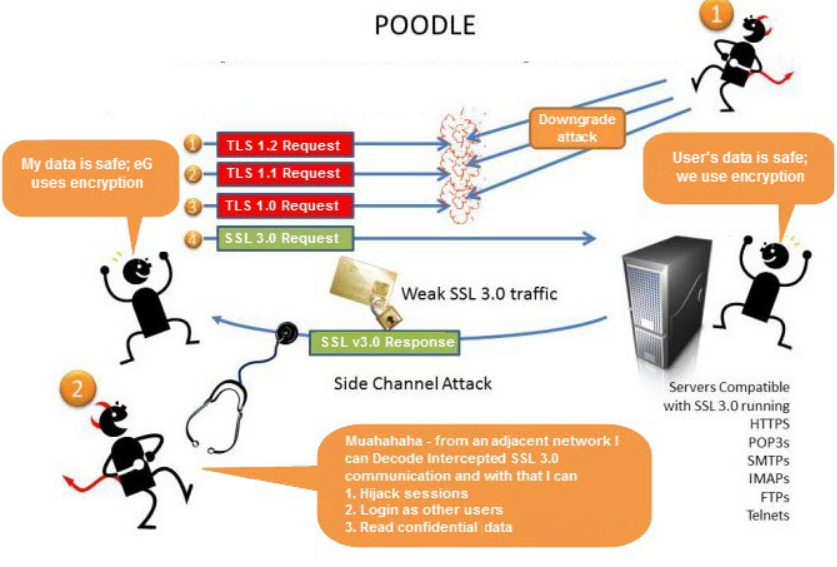
**Working:**

The POODLE attack exploits a flaw in the design of SSL 3.0, an older version of the SSL/TLS encryption protocol. In SSL 3.0, a block cipher mode known as CBC (cipher block chaining) is used to encrypt data. CBC encryption requires padding the plain-text to a multiple of the block size before encryption. The padding is then removed after decryption.

The POODLE attack works by exploiting a vulnerability in the way that SSL 3.0 handles padding. An attacker intercepts an encrypted message that is being transmitted between a client and a server using SSL 3.0. The attacker then modifies the padding bytes in the message to try to decrypt the encrypted data one byte at a time.

The attacker sends the modified message to the server, which attempts to decrypt it. If the padding is invalid, the server will send an error message back to the attacker. However, the error message contains information that the attacker can use to determine the decrypted value of one byte of the encrypted data.

By repeating this process multiple times, the attacker can gradually decrypt the entire message. This can allow the attacker to gain access to sensitive information, such as login credentials and personal data.



**Mitigation:**

1. Disable SSL 3.0
2. Use TLS\_FALLBACK\_SCSV
3. Implement Perfect Forward Secrecy (PFS)
4. Keep systems and software up-to-date

# Vulnerabilities in SSL/TLS-Software based

PRANATHI & SARAT

(Times new roman 10)

# Concluding Thoughts

##### References

1. G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*
2. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
3. I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
4. K. Elissa, “Title of paper if known,” unpublished.
5. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
6. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
7. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 198