# Study of SSL/TLS Attacks

Tejas Sontakke, Anamika Kesharwani, Deepika Mallappa

**Title of the Project:** Study of SSL/TLS Attacks

**Introduction:** Web threats got bigger and much more aggressive in the year 2014 as various loopholes in commonly used tools and encryption protocols were exposed and criminals made it harder to escape their malicious clutches. Vulnerabilities and new variants of malware underlined that website security deserves full – time, business critical attention. SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook). In this Modern world, Security is one of the main criteria which anybody look after before communicating and SSL provides the same.

SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text. If an attacker is able to intercept all data being sent between a browser and a web server, he can intercept and exploit that information.

More specifically, SSL is a security protocol. Protocols describe how algorithms should be used. In this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted. Even after the deployment of these security measures, the attackers can detect loopholes and exploit it, thereby compromising the data integrity and web security.

Through this Project, we aim to analyze the SSL/TLS protocol Versions in detail and the attacks on SSL/TLS Versions. In addition, we aim to focus our analysis on the recent vulnerabilities, find the weaknesses which gave way for the breach in security and try and find any possible loopholes in the currently deployed systems.

## Motivation:

Since its introduction in 1994 the Secure Socket Layer (SSL) protocol (later renamed to Transport Layer Security (TLS)) evolved to the main standard for securing the transport layer

Internet users, including many security professionals, often blindly rely on SSL/TLS to provide the confidentiality and integrity of our personal data, at least when using our web browsers. We expect SSL/TLS to do so even in the face of attackers with the ability to hijack and redirect our network connections and DNS traffic (i.e., a man-in-the-middle attack).SSL/TLS can be used for ensuring data confidentiality, integrity and authenticity during transport. A main feature of the protocol is its flexibility. Modes of operation and security aims can easily be configured through different cipher suites. During its evolutionary development process several flaws were found and attacks launched.

To resist these attacks, our browsers rely on a list of trusted certificate authorities to authenticate server certificates. Browser vendors audit these certificate authorities, but must presume that neither the trusted root authorities nor any intermediate authorities chaining to a trusted root will sign a certificate for an entity without first verifying that the entity controls the domain name listed in the certificate.

Unfortunately, our faith in SSL/TLS is increasingly misplaced. Over the last few years, there have been several major attacks on SSL/TLS including attacks on its most commonly used ciphers and modes of operation.

Given our time constraints, if feasible , we would give a demonstration of how an active attack is performed.

## Tentative list of Evaluation Criteria:

1) Conducting a brief study of SSL /TLS Protocols.
2) Analysis of Attacks on SSL V2.0, V3.0: Methodologies used, vulnerabilities exposed.
   a) SSL/TLS versions used, loopholes exposed.
   b) How is the attack accomplished.
   c) Solution provided.
   d) Demo (if time permits)
   e) Lessons Learnt.
3) Study of various encryption and Compression techniques used.
4) Evaluating the server security as a whole: We inspect server security levels in three categories:
   a. Protocol support
   b. Key exchange support
   c. Cipher support

5)Protocols we are planning to explore:

- Freak attack: Attack on FREAK(Factoring RSA export keys) in SSL/TLS protocol
- Poodle attack: The man in the middle attack (Padding Oracle)
- Breach attack: Security attack against HTTPS when using HTTP compression (Browser Reconnaissance and Exfiltration via adaptive compression of hypertext)
- Heartbeat attack: Security bug in open SSL Cryptography.
- Beast attack: Browser Exploit against SSL/TLS.
- Bar Mitzvah attack.

6)Study of the Implemented solution for the attacks.

7)Finding unexplored tricks to defeat SSL/TLS from an attacker's POV.

**Mutual dependencies among various evaluation criteria**

Understanding basic concepts of SSL/TLS Protocol in detail will enable us to understand the implementation of the present encryption techniques in SSL/TLS latest version figuring some more exposed way which can cause breach in future.

Also, understanding the attacks will make us aware of how the hackers breach a network, how they exploit and gain advantage.

**Plan of Action**

1) Study the SSL/TLS protocol in detail.

2) Research about the recent attacks on the latest SSL/TLS Version.

3) The adopted approach to solve the Attack.

4) Try finding any broken links which might be exploited in the future.

**Time schedule:**

| *Week* | *Task* |
|---|---|
| 10/26/2015 – 11/08/2015 | Study of SSL /TLS protocol in detail. |
| 11/09/2015 – 11/15/2015 | Study of various attack tools like<br>• PacketCreator.<br>• Sslsniff<br>• Sslstrip<br>• Chapcrack.<br>• Ettercap<br>• Dsniff<br>• Cain N Abel |
| 11/16/2015 – 11/22/2015 | Tejas: Study of Attacks on the SSL/TLS Handshake Protocol<br><br>Anamika: Attacks on the Record and Application Data Protocols<br><br>Deepika: Attacks on the PKI |
| 11/23/2015 – 11/29/2015 | Tejas: Beast attack, Crime & Breach attack.<br>Anamika: Poodle & RC4 attacks.<br>Deepika: Freak & Heart bleed attacks. |
| 11/30/2015 – 12/05/2015 | Evaluating the server security levels and study of possible loopholes in the latest SSL/TLS version. |
| 12/06/2015 – 12/12/2015 | Documentation & Final Report |

**Tentative table of contents of the final report:**

a. Introduction and Motivation.

- Background study about SSL/TLS.
- Characteristics of SSL/TLS.
- Importance and usage.
- Versions of SSL.
- SSL-TLS transformation.

b. Loopholes & Attacks.

- Vulnerabilities exploited.
- Techniques used in the attacks.
  - Diagrams.
  - Pseudo codes.
  - Graphical representation.
  - Development environment used.
  - Programming language used.
  - Experimental implementation.
  - Results.
  - Inference.

c. Countermeasures for recovery.

- Techniques used to mitigate the attacks.
- Updated version of SSL.
- Possible alternative solutions.

d. Possible weak links in the most recent version.

e. Conclusion.

f. References cited in IEEE format.

## References:

[1] A.Freier , P.Karlton, P.Kocher (2011 Aug) “SOCKETS LAYER (SSL) PROTOCOL VERSION 3.0”. [Online]. Available: https://tools.ietf.org/html/rfc6101

[2] Bodo Moller, Thai Duong, Krzysztof Kotowicz (2014, Sept) “THIS POODLE BITES: EXPLOITING THE SSL 3.0 FALLBACK”. [Online]. Available: https://www.openssl.org/~bodo/ssl-poodle.pdf

[3]T.Dierks, C.Allen (1999, Aug)“The TLS Protocol”, [Online]. Available: https://tools.ietf.org/html/rfc2246

[4] “Imperial Violet Poodle attacks on SSLv3“ (2014, Oct 14). [Online]. Available: https://www.imperialviolet.org/2014/10/14/poodle.html

[5] Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe (2014, May 21), “How to Recover Any Byte of Plaintext on RC4” , [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-662-43414-7_8#page-1

[6] Nadhem J. Alfardan “ On the security of RC4 in TLS”, [Online]. Available: http://dl.acm.org/citation.cfm?id=2534793

[7] Richard Barnes (2014, Oct 14), “Mozilla Security Blog”, [Online]. Available: https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/

[8]Information Security, “How exactly does the OpenSSL TLS heartbeat (Heartbleed) exploit work?”, [Online]. Available: http://security.stackexchange.com/QUESTIONS/55116/HOW-EXACTLY-DOES-THE-OPENSSL-TLS-HEARTBEAT-HEARTBLEED-EXPLOIT-WORK Accessed Apr. 10, 2014.

[9] A. Freier, P. Karlton, and P. Kocher (1996, Nov. 18), "The SSL 3.0 Protocol", Netscape Communications Corp.

[10] Hickman, Kipp (1995, Feb. 9) "The SSL Protocol", Netscape Communications Corp.

[11]Protocol Version 1.1", RFC 4346, April 2006.

[12] [TLS1.0] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999. [TLS1.1] Dierks, T. and E. Rescorla, "The Transport Layer Security

[13] OpenSSL Security Advisory (15 Oct 2014), “SRTP Memory Leak”, [Online]. Available: https://www.openssl.org/news/secadv/20141015.txt

[14] B. Moeller, A. Langley (2015, Feb 20)“TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks”, [Online]. Available: https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-05

[15] “This POODLE bites: exploiting the SSL 3.0 fallback” (2014, Oct. 14), [Online]. Available: https://googleonlinesecurity.blogspot.jp/2014/10/this-poodle-bites-exploiting-ssl-30.html

[16] “Lucky 13 – a new attack against SSL/TLS” (2014, Sept. 28). [Online]. Available: http://www.infosecurity-magazine.com/news/lucky- 13-a-new-attack-againstssltls/

[17] Gregory V. Bard (2014, Sept. 28), “A Challenging But Feasible Block wise-Adaptive Chosen-Plaintext Attack On Ssl”, [Online]. Available: https://eprint.iacr.org/2006/136.pdf

[18] Abdel Nasir Alshamsi, Takamichi Saito. (2014, Sept. 6). “A Technical Comparison Of IPSec and SSL” (Doctoral dissertation, Tokyo University of Technology). [Online]. Available: http://eprint.iacr.org/2004/314.pdf

[19] “BlackHat2014USA_Prompt_20140808 - Cryptographic protocol Evaluation toward Long-Lived Outstanding Security Consortium (CELLOS)”. (n.d.). [Online]. Available: https://www.cellos-consortium.org/index.php?BlackHat2014USA_Prompt_20140808 [09 SEPT 13 Dr. Kris Gaj ECE646 cryptography GMU 2014 2014]

[20] Antoine Delignat-Lavaud., & Karthikeyan Bhargavan (2014, Sept. 28). “Virtual Host Confusion: Weaknesses and Exploits”(2014), [Online]. Available: https://bh.ht.vc/vhost_confusion.pdf

[21] Dan Goodin (2011, Sept. 19) “Hackers break SSL encryption used by millions of sites”. [Online]. Available:

http://www.theregister.co.uk/2011/09/19/beast_expl oits_paypal_ssl/ [28 SEPT 2014]

[22] IBM. (2014, Sept. 12). “IBM WebSphere Developer Technical Journal: Using the Java Secure Socket Extension in WebSphere Application Server.” [Online]. Available: http://www.ibm.com/developerworks/websphere/tec hjournal/0502_benantar/ 0502_benantar.html

[23] Cisco (2014, Sept. 28)."Introduction to Secure Sockets Layer Internet" [Online]. Available: http://euro.ecom.cmu.edu/resources/elibrary/epay/S SL.pdf