Attacks on SSL/TLS

Team Members
Ernest Kushevski

Introduction and Motivation

In recent years there has been an uptick in attacks on Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. These protocols are an integral part of network security. However, there are vulnerabilities associated with these protocols which are being exploited more and more every day. Some of the more high profile attacks have been BEAST, CRIME, padding attacks and renegotiation.

Many of the preliminary studies and articles we have analyzed, such as "Backdoors in SSL/TLS" and “Hackers break SSL encryption used by millions of sites,” do a tremendous job of looking at how the attacks are successful, but fall short of forward-thinking problem solving. The availability of alternate solutions or the possibility of a stronger TLS was glaringly absent from the studies.

The focus of this project will be to analyze these major attacks and see how TLS implementations can be hardened in the future.

List of attacks we are planning to analyze

BEAST
CRIME/BREACH
Padding Attacks
Renegotiation

Problems/Hypotheses

Research the major attacks on SSL and TLS.
Hypothesis: A number of attacks against SSL/TLS exist but are generally difficult to implement.
Understand why older versions of SSL/TLS continue to be used
Hypothesis: Implementing new version of SSL/TLS is too costly due to old codebase and/or a “if it isn’t broken, why fix it” mentality
Identify hardening techniques for future implementations of TLS
Hypothesis: Hardening techniques and/or secure implementations exist for TLS
Alternatives to TLS/SSL
Hypothesis: SSL/TLS is the gold standard due to ease of use/implementation and recognition, however viable alternatives do exist

Evaluation Criteria

The delivery mechanism of the attack.
The relative ease of executing the attack.
Countermeasures currently available.
Costs of implementing the newest TLS algorithms
Cost and availability of hardening techniques
Evaluation of different implementations of TLS based on effectiveness and ease of use
Cost/benefit of using other cryptosystems

Mutual Dependencies

Delivery mechanism and ease of use are inversely related. The more complex the mechanism is the more difficult the attack is to accomplish. This further depends upon the countermeasures in place to prevent such attacks. Likewise, the costs and benefits of implementing a particular protocol are influenced the risk factor of a successful attack which is predicated on the aforementioned criteria.

Questions we will be seeking to answer

Why is SSL still prevalent?
Do the instances of SSL directly impact the amount of successful attacks?
What are the vulnerabilities of TLS?
How can the TLS vulnerabilities be mitigated?
Is TLS fundamentally flawed?
Are there alternatives to TLS?
How can TLS be hardened to prevent more attacks?

Experiments and Verification the investigation

We will perform experiments that follow an analytic framework by examining the various architectures of attacks, protocols, and implementations and try to discern strengths and weaknesses of each against the others. This will be from both a strictly technical standpoint as well as enterprise cost. For example, we will look at the mechanism of the renegotiation attack and attempt to examine whether it would be effective against all ranges of TLS protocols and implementations and real and hypothetical creative alternatives. We will then examine whether these alternatives are actually viable and cost effective.

Time Schedule

October 27 – Understand how the BEAST and CRIME/BREACH attacks were implemented and the effects of both.

November 10 – Understand how the renegotiation and paddings attacks are implemented and the effects as well as an understanding of the impact SSL has on future attacks.

November 24 – Document steps users/enterprises should take to harden their TLS implementations including which implementations are most secure. Identify any alternatives to TLS and their cost benefit.

December 8 – Have final project, including presentation ready for review and submission.

Why Might the Specification Change

The specification has changed once already, as an original member unexpectedly dropped from the group. Additionally, the specification may change if a new attack is either launched or discovered while our research is being conducted. Another reason to change the specification is if we are unable to identify either hardening techniques or alternative to TLS during the course of research.

Table of Contents

Team Task Distribution

Our plan of attack is to each read and analyze the same material and compare notes. From the comparisons we will formulate opinions and conclusions together. The drafting of the report, slides, and presentation will be completed by both us and will have an equal share of the work. We will review and edit each other's work and come to an agreement if any disputes occur.

References

[1] C. H. Wu and J. D. Irwin, *Introduction to Computer Networks and Cybersecurity*, 1st ed. Boca Raton, FL: CRC Press, 2013, pp. 1009-1049.

[2] L. L. Peterson and B. S. Davie, *Computer Networks: A systems Approach*, 5th ed. Burlingotn, MA: Morgan Kaufmann, 2012, pp. 670-675.

[3] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Upper Saddle River, NJ: Pearson Ed. Inc., 2014, pp. 525-538.

[4] Testing for weak SSL/TLS ciphers, insufficient transport layer protocol. (2015, Mar. 22). OWASP.org. [Online]. Available: https://www.owasp.org/index.php/Testing_for_Weak_SSL/TLS_Ciphers,_Insufficient_Transport_Layer_Protection_(OTG-CRYPST-001)

[5] T. Dierks and E. Rescorla, "The transport layer security protocol Version 1.2," RTFM, Inc., San Francisco, CA, RFC 5246, Aug. 2008.

[6] I. Ristic. (2013, Jun. 25). SSL Labs: deploying forward secrecy. [Online]. Available: https://community.qualys.com/blogs/securitylabs/2013/06/25/ssl-labs-deploying-forward-secrecy

[7] S. Bhople, "Server based DoS vulnerabilities in SSL/TLS protocols," M.S. thesis, Dept. of Math. And CS., Eindhoven Univ. of Tech., Eindhoven, Netherlands, 2012.

[8] O. Kelka, "Attack vectors in SSL/TLS secure communication," M.S. thesis, Dept. of CS and Eng., Czech Tech. Univ., Prague, Czech Republic, 2010.

[9] C. Meyer, "20 years of SSL/TLS research an analysis of the Internet's security foundation," Ph.D. thesis, Dept. of Elec. Eng. and IT, Ruhr-Univ., Bochum, Germany, 2014.

[10] *NIST Guidelines for the Selection, Configuration, and Use of Transport Layer Security Implementations*, Special Publication 800-52, 2014.

[11] A. Veerayyagari, J. S. Dondapati, A. Yeluri, "Back doors in SSL/TLS," unpublished.

[12] Goodin, D. (2011, Sep. 19). Hackers break SSL encryption used by millions of sites: Beware of BEAST decrypting secret PayPal cookies. The Register [Online]. Available: http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl