

# Exploring Communications Security Using the Transport Layer Security Protocol

## An Independent Research Proposal

Submitted  
to: Monica Orlando  
by: Mike Xu  
on: November 22, 2013

### **Abstract**

The goal of this proposed research project is to conduct a thorough investigation of the Transport Layer Security (TLS) protocol in order to understand its role in protecting data being transferred over the internet. TLS is a standard set of methods and procedures for encrypting and decrypting information between two hosts across an untrusted network. The cryptography applied to the data ensures the authenticity of each hosts identity as well as making it mathematically impractical for any malicious agent between them to decipher the message.

Two hosts who wish to establish a secure TLS connection advertise their respective security capabilities to each other and decide upon a set of connection parameters in a process known as the TLS handshake. Once the connection has been described, asymmetric encryption keys are exchanged across a Public Key Infrastructure to secure a one-way channel of communication. A symmetric encryption key is then encrypted and sent from the server to the client where it is decrypted and used to establish a two-way secure channel.

Due to the complexity of this process and its reliance on the practical security of other systems such as the Public Key Infrastructure, TLS faces a number of points of vulnerability. Because it is so much easier to reap the economic and social benefits of communicating over the internet than it is to comprehend the intricacies of its operation, an overwhelming majority of existing applications are less than optimally secured. The research proposed in this document will attempt to identify the current known exploits against TLS, explore their practical implications towards internet security, and explore possible techniques to safeguard against them. This proposal includes relevant background information about computer security relating to TLS, a scheduled research plan, asserts the qualifications of the researcher, and provides an estimated budget for the project.

2397 Euclid Heights Blvd  
Cleveland OH, 44106

November 22, 2013

Ms. Monica Orlando  
Department of English, CWRU  
11112 Bellflower Road  
Cleveland, OH 44106

Dear Professor Orlando:

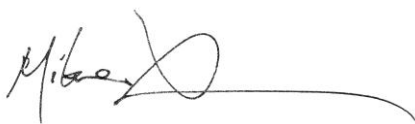
Attached is a proposal for an independent research project titled "Exploring Communications Security Using the Transport Layer Security Protocol." This document is being submitted in order to fulfill the final project requirement of Unit 2: Independent Research Proposal of ENGL 398: Professional Communication for Engineers. It describes an exploratory research project I would like to undertake in order to improve my expertise in computer security to strengthen my web development career path. Also included is a literature review of the topic, plan and schedule of work for my own research, description of my qualifications to conduct this research, and budget for the project.

TLS is the most prevalent cryptographic protocol currently used to secure internet communications. It does so by having one party encrypt data using a method that can only be decrypted by the intended recipient, thus ensuring its security regardless of the path taken. This endpoint security is necessary because data traveling across the internet is not passed in a predictable efficient path, but between many untrusted intermediary agents dictated by complex political and corporate policies. The increased utility and complexity of the internet is accompanied by vulnerabilities to increasing numbers of attack vectors. The presence of malicious parties attempting to exploit and undermine its efficient usage necessitates an ever deeper understanding of its operation in order to preserve its integrity.

As you are the intended audience of this proposal, I have attempted to describe all relevant technology by building up from basic non-technical principles. The included literature review contains as much information as I felt was necessary to communicate the significance of this research project while omitting as many technical details of implementation as possible. The actual research to be conducted would be done on a much deeper technical level.

I appreciate you taking the time to review the attached document. Please feel free to respond with any comments or questions you may have. Thank you for your consideration of my proposal.

Regards,

A handwritten signature in black ink, appearing to read 'Mike Xu', with a long horizontal flourish extending to the right.

Mike Xu

## Table of Contents

---

<b>1   Project Description.....</b>	<b>3</b>
<b>2   Literature Review.....</b>	<b>3</b>
<b>2.1   Overview.....</b>	<b>3</b>
<b>2.2   Cryptography.....</b>	<b>3</b>
<b>2.3   Security Protocols.....</b>	<b>4</b>
<b>2.4   Transport Layer Security.....</b>	<b>5</b>
<b>2.5   Vulnerabilities.....</b>	<b>6</b>
<b>2.6   Conclusion.....</b>	<b>6</b>
<b>3   Project Details.....</b>	<b>7</b>
<b>3.1   Schedule of Work.....</b>	<b>7</b>
<b>3.2   Plan of Work.....</b>	<b>8</b>
<b>4   Qualifications.....</b>	<b>8</b>
<b>5   Budget.....</b>	<b>9</b>
<b>6   Bibliography.....</b>	<b>9</b>

## **1 | Project Description**

The purpose of this research project is to investigate the current state of communication security protocols involving data in transit by exploring the capabilities and vulnerabilities of the Transport Layer Security (TLS) protocol. Over the past several decades, the internet has become the backbone on which nearly all businesses and organizations are built. As the volume of information traveling through it increases exponentially over time, so too does the importance of protecting that data against theft and corruption. The research to be conducted in this project aims to establish the current practical uses and limitations of TLS in order to better understand best practices of internet security.

Most of the effort for this project will be spent doing literature research regarding TLS and understanding its constituent components. Once baseline knowledge about the protocol has been established, I will conduct more specific research from the point of view of its vulnerabilities. For each one, I will research subsystems of TLS affected by the exploit and attempt to safely reproduce software attacks when possible. As this project is exploratory in nature, the expected outcome is merely an increased understanding of the TLS protocol. However, by thoroughly comprehending the inner workings of TLS from the perspective of its weaknesses, I may hopefully be able to propose a more substantial research project to engineer an improvement of the protocol itself. At the very least, I will be able to confidently establish a set of best practices when utilizing TLS by appropriately compensating for any deficiencies in its reliability. This would allow me to develop software that is dependably secure even if TLS is not.

## **2 | Literature Review**

### **2.1 | Overview**

The general approach to securing internet communications involves transforming the data into a ciphertext using an encryption key and algorithm that can only be decoded by the intended recipient using a matching decryption key. Various protocols specify the methods by which keys can be exchanged, algorithms to be used for encryption, and the metadata needed to facilitate their transactions. The following literature review will overview the principles and technology behind the origin of TLS, describe the details of its implementation, and outline known potential vulnerabilities.

### **2.2 | Cryptography**

The general principle behind cryptography as a method of securing data is the notion that a message can be transformed to and from a comprehensible form using specific key and algorithm. A key is a string of characters which the algorithm uses to generate a unique set of

mathematical transformations to apply to a given set of data. Without the appropriate decryption key, there is no feasible way to accurately produce the transformations necessary to revert an encrypted message back into plaintext. Although it is possible to break practically every cipher by exhaustively testing every possible key (brute force attack), modern cryptographic systems are designed so that the computational costs of doing so become astronomical with increasing key lengths [1]. Thus, the protective capabilities of a sound cryptographic system is contingent upon the secure distribution of decryption keys.

Because a key is required to both encrypt and decrypt data, cryptographic methods can be classified as either symmetric or asymmetric. This designation indicates whether the same or different keys are used for each operation. In a symmetric key system, the sender and receiver must know the shared key used for both encryption and decryption [1]. A key that becomes compromised by an attacker will undermine the security of the entire system [2]. A naïve implementation of such a system would not be practical for securing information across the internet due to the need for a secure channel to communicate the key in the first place. Conversely, an asymmetric key cryptosystem utilizes two distinct, but mathematically related, keys to perform each operation. The keys are generated in such a way that calculating one of the pair using the other is computationally infeasible [3]. This way, one of the keys can be made publicly available for distribution, while the other remains private. Depending on the specific implementation of the public-key algorithm, asymmetric key cryptography can provide various advantages. The identity of the sender can be verified by the encrypting the data using the private key because users who decrypt it using the public key will be able to recreate the original message. Additionally, a public key can be used for encryption of a message so that no one but the intended recipient possessing the private key can decrypt it.

## **2.3 | Security Protocols**

Data security protocols are collections of rules and procedures used to protect information traveling through a computer network. They specify the steps that must be taken throughout the lifespan of a connection in order to do so. Initially, an entity authentication mechanism must be used to verify the relative identities of the parties involved in communication. Next, a key setup phase must be executed in order to establish cryptographic keys for encoding and decoding data. Finally, the protocol must define some functionality for securing the application-level data to be passed between the two parties.

Due to the complex nature of asymmetric key cryptography, systems must be put in place to standardize the management of keys called Public Key Infrastructures (PKI) [2], [4]. These infrastructures are comprised of all the human, digital, and hardware assets used to create, manage, and distribute keys. Entities known as Certificate Authorities (CA) establish connections between sets of public keys and individual user identities. The digital certificates

issued by the CA are verified by a Registration Authority (RA) during use [5]. Various technology frameworks underpin the system used to store and manage the certificates.

## **2.4 | Transport Layer Security Protocol**

The TLS protocol is designed to allow a client and server to exchange messages across a potentially unsafe network path without risk of being read or modified. In order to establish a secure connection, a client must notify the server that it wishes to enable TLS for the session. Once both parties have agreed upon this, the connection is initialized by the client and server exchanging metadata detailing the security capabilities specific to each application's implementation of the protocol. Included among these are the TLS version number, session ID, compression methods, and cipher suite [6].

The cipher suite is a list of encryption algorithms available to each host for each phase of the connection. A key exchange algorithm is used initially to mutually assure the identities of the client and server, creating an asymmetric key connection [7]. This connection is used to encrypt and exchange a key (hence its name) used in a bulk encryption algorithm. Bulk encryption uses a symmetric key in order to allow two way encryption / decryption of the message stream between client and server. A message authentication algorithm is also used to generate a cryptographic hash of each block in the stream. These hashes are used to evaluate the integrity of the data that they digest. Finally, a pseudorandom function is included to generate a master secret that is seeded to produce ephemeral session keys [8].

Once the client and server have exchanged lists of compatible and preferred algorithms, they select a mutual cipher suite to use and proceed with the handshaking process. They execute the key exchange algorithm based on a signed certificate provided by the server. TLS employs the X.509 protocol [9] to assure the authenticity of identities described by these certificates. Because the certificate is signed with a private key, and the client is provided with a matching public key, it can be decrypted to verify the identity of the server.

Upon validation of this information, the client generates a temporary pre-master secret used to identify the current session, encrypts it using the server's public key, and send it to the server. After authenticating the client, the server uses its private key to decrypt the pre-master secret, and generates a master secret from it. This master secret is used to generate symmetric cryptography keys which are shared between the client and server. The handshake is terminated by the client and server each sending each other messages stating that future messages will be encrypted using the symmetric session key [8].

TLS is the most common method for encrypting web traffic, and is fully implemented in versions of all modern browsers. In addition to securing HTTP traffic, it can also be used to augment the Simple Mail Transfer Protocol (SMTP) and establish Virtual Private Networks (VPN). Its current version, 1.2, improves upon 1.1 and 1.0 with heightened protection against certain vectors of

attack such as cipher block chaining and a much stronger cipher suite. It was preceded by the Secure Socket Layer (SSL) protocol [8].

## **2.5 | Vulnerabilities**

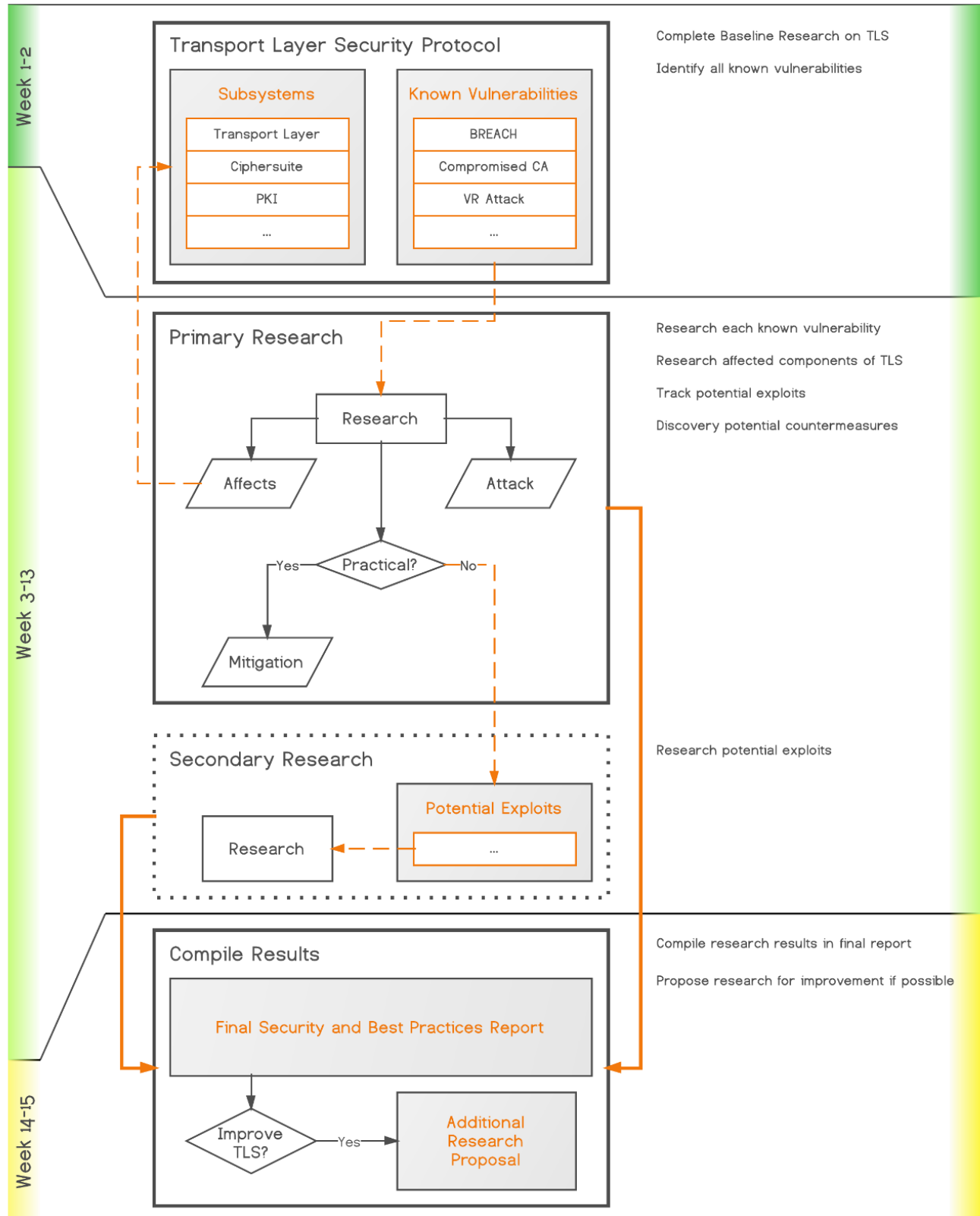
TLS currently faces a number of known vulnerabilities that can weaken its security in a variety of ways. Version rollback attacks can occur when a client's cipher suite is manipulated to select weaker algorithms [10]. A hacking technique known as Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext (BREACH) was developed by researchers and exploits a weakness in HTTP compression techniques that are used to optimize the transmission rate of nearly all internet traffic [11]. Additionally, in light of recent government mass surveillance disclosures, certificate authorities used to manage the authenticity of public key id's in asymmetric cryptosystems can no longer be fully trusted, and may provide a vector for man-in-the-middle attacks [12].

## **2.6 | Conclusion**

As I intend to pursue a career involving software and web development, the production of secure applications will be of utmost importance. By gaining a deep understanding of one of the most prevalent web security technologies in use today, I hope to be able to properly implement security in my applications and possibly propose an improvement to the protocol.

### 3 | Project Details

#### 3.1 | Schedule of Work





### **3.2 | Plan of Work**

The project will occur over the span of 15 weeks beginning on Monday, January 6<sup>th</sup>, 2014. The first two weeks will be spent completing a fairly deep baseline understanding of the technical operation of TLS and compiling a list of publically known exploits against it. Because TLS is a complex system with components spanning multiple fields of computing, attempting an exhaustive bottom-up study of them over the proposed timespan would be impractical and not necessarily productive. By studying each of the technologies that facilitate its vulnerabilities, I can gain much more practically useful information about TLS from a security standpoint.

For each exploit, I would conduct library research to determine how it is executed, the practical probability of its occurrence, and the specific principles of each layer of the TLS protocol that make it susceptible. Although some theoretical weaknesses in the protocol may be identified by researchers, they may be benign in real world implementations. For flaws that may be of practical significance, I would determine the proper direction of research for further investigation, and make note of it for future reference. The only practical experimentation that would be conducted is attempting to recreate software attacks on individual connections. This process would be done in a computer lab using multiple machines or a single box hosting multiple virtual machines and simulating the appropriate network conditions. This process would repeat until week 13 or until the list of known vulnerabilities has been exhausted.

During my study of the known vulnerabilities, I will take note of any topics in my research that may indicate some additional vulnerability. If time permits before the 13<sup>th</sup> week of the project, I would spend the remainder of the extra time doing exploratory research and whatever testing possible on those topics.

The final two weeks of the project will be spent compiling all of the previous research to produce a single comprehensive report assessing the practical strength of TLS. It would include the risks and implications of each known weakness within TLS, describe any ways they can be mitigated by other aspects of software, and detail a list of suggested best practices concerning the use of TLS. If sufficient information can be generated to form some hypothesis to improve the security of TLS, I would additionally propose another research project to test its validity.

### **4 | Research Qualifications**

I believe that my past education and work experience qualify me to perform this research project. I have completed 3 years of computer science course work at Case Western Reserve University. Additionally, I have over 3 years of professional web development experience having worked for a large multibillion dollar corporation, freelanced for a small ecommerce business, and currently working on software development for a startup. These jobs have provided me with practical experience in internet security, and my future work will directly benefit from the knowledge gained from the proposed study.

## 5 | Budget

All of the work involved in this project can be done on one or more computers with internet connections. I already own sufficient hardware to do all the research necessary. The only costs associated with the project would be electricity to power the computers and payment for internet service. The numbers projected are based on my current location of residence. Internet over the course of 15 weeks (4 months) at \$30 per month would total \$120. Electricity consumption for two desktop and one laptop computer is estimated at \$20 per month, or \$80 for the duration of the project. The total budget for the project would not exceed \$200

Item	Cost (\$)
Internet Connection	120
Electricity	80
Total	200

## 6 | Bibliography

- [1] W. Diffie *et al.*, "Authentication and authenticated key exchanges," in *Designs, Codes and Cryptography*, Mountain View: Kluwer Academic Publishers, 1992, pp. 107 – 125.
- [2] R. P. Cowburn and J. D. R. Buchanan, "Cryptographic Key Distribution," International Patent Application PCT/GB2006//002685, Feb. 1, 2007.
- [3] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, pp. 198-208, Mar. 1983.
- [4] E. Bresson *et al.*, "Provably Authenticated Group Diffie-Hellman Key Exchange," in *Proceedings of the 8<sup>th</sup> ACM conference on Computer and Communications Security*. ACM, 2001, pp. 255-264.
- [5] D. R. Stinson, *Cryptography Theory and Practice*, 3<sup>rd</sup> ed. Boca Raton: Chapman & Hall/CRC, 2006.
- [6] *Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)*. Internet Engineering Task Force RFC 6353, 2011.
- [7] *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)*. Internet Engineering Task Force RFC 5764, 2010.
- [8] *The Transport Layer Security (TLS) Protocol Version 1.2*. Internet Engineering Task Force RFC 5246, 2008.
- [9] *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. Internet Engineering Task Force RFC 2459, 1999.

- [10] B. Smith. (Aug. 19, 2010). *[TLS] Limited rollback attacks in False Start and Snap Start* [Online]. Available email: [brian@briansmith.org](mailto:brian@briansmith.org)
- [11] Y. Gluck *et al.*, "Breach: Reviving the Crime Attack," Computer Systems Security Group, MIT, Cambridge, 2013.
- [12] C. Soghoian and S. Stamm, "Certified lies: Detecting and defeating government interception attacks against ssl," in *Financial Cryptography and Data Security*, Germany: Springer Berlin Heidelberg, 2012, pp. 250-259.
- [13] P. Zimmermann, "Pretty good privacy: public key encryption for the masses," in *Building in Big Brother: The Cryptographic Policy Debate*, L. J. Hoffman, Ed. New York: Springer-Verlag New York, 1995, pp. 93-107.
- [14] *Using OpenPGP Keys for Transport Layer Security (TLS) Authentication*. Internet Engineering Task Force RFC 6091, 2011.
- [15] D. Grigoriev and V. Shpilrain, "Secure Information Transmission Based on Physical Principles," in *Unconventional Computation and Natural Computation*, Germany: Springer Berlin Heidelberg, 2013, pp. 113-124.