superTLS: A Diverse and Redundant Secure Communication Channel for Privacy in Cloud

André Joaquim
INESC-ID, Instituto Superior Técnico, Universidade de Lisboa
Lisbon, Portugal

Miguel L. Pardal
INESC-ID, Instituto Superior Técnico, Universidade de Lisboa
Lisbon, Portugal

Miguel Correia
INESC-ID, Instituto Superior Técnico, Universidade de Lisboa
Lisbon, Portugal

{andre.joaquim, miguel.pardal, miguel.p.correia}@tecnico.ulisboa.pt

ABSTRACT

We present superTLS, a diverse and redundant vulnerability-tolerant secure communication channel for privacy in cloud. There have always been concerns about the strength of some of encryption mechanisms used in SSL/TLS channels and some of them were regarded as insecure at some point in time. superTLS is our solution to mitigate the problem of secure communication channels being vulnerable to attacks due to unexpected vulnerabilities in its encryption mechanisms. It is based on diversity and redundancy of cryptographic mechanisms and certificates to provide a secure communication channel even when one or more mechanisms are regarded vulnerable. superTLS relies on a combination of k mechanisms/cipher suites, with k being the diversity factor and $k > 1$. Even when $k - 1$ mechanisms are regarded as insecure or considered vulnerable, superTLS relies on the remaining secure, diverse and redundant mechanism to maintain the channel secure. We evaluated our channel by comparing it to a normal TLS channel.

CCS Concepts

•**Networks** → **Application layer protocols;** *Network security;* •**Computer systems organization** → **Redundancy;** •**Security and privacy** → *Security protocols;* Symmetric cryptography and hash functions;

Keywords

Secure communication channels; Diversity; Redundancy; TLS; Vulnerability-Tolerance

1. INTRODUCTION

Secure communication channels are mechanisms that allow two entities to exchange messages or information securely in the Internet. A secure communication channel has three properties: *authenticity*, *confidentiality*, and *integrity*. Regarding authenticity, in an authentic channel, the messages can not be tampered. Regarding confidentiality, in a confidential channel, only the original receiver of a message is able to read that message. Regarding integrity, no one can impersonate another. The information regarding the original sender of a message can not be changed. Several secure communication channels exist nowadays, such as TLS, IPsec or SSH. Each of these examples is used for a different purpose, but with the same finality of securing the communication.

Transport Layer Security (TLS) is a secure communication channel widely used. Originally called Secure Sockets Layer (SSL), its first released version was SSL 2.0, released in 1995. SSL 3.0 was released in 1996, bringing improvements to its predecessor such as allowing forward secrecy and supporting SHA-1. Defined in 1999, TLS did not introduce major changes. Although, the changes introduced were enough to make TLS 1.0 incompatible with SSL 3.0. In order to grant compatibility, a TLS 1.0 connection can be downgraded to SSL 3.0, which brought security issues. TLS 1.1 and TLS 1.2 are upgrades which brought some improvements such as mitigating CBC (cipher block chaining) attacks and supporting more block cipher modes of operation to use with AES. TLS is divided in two sub-protocols, Handshake and Record, constituted by several mechanisms each. The Handshake protocol is used to establish or re-establish a communication between a server and client. The Record protocol is used to process the sent and received messages.

Internet Protocol Security (IPsec) is an Internet layer protocol that protects the communication at a lower level than SSL/TLS, which operates at the Application layer [1].

Secure Shell (SSH) is an Application layer protocol, such as SSL/TLS. SSH is a protocol used for secure remote login and other secure network services over an insecure network [2].

A secure communication channel becomes insecure when a vulnerability is discovered. Vulnerabilities may concern the protocol's specification, cryptographic mechanisms used by the protocol or specific implementations of the protocol. Many vulnerabilities have been discovered in SSL/TLS originating new versions of the protocol with renewed security aspects such as deprecating cryptographic mechanisms or enforcing security measures. Concrete implementations of SSL/TLS have been also considered vulnerable by hav-

WOODSTOCK '97 El Paso, Texas USA

DOI: 10.475/123_4

ing implementation details causing a breach of security and affecting devices worldwide.

- Description

superTLS is a secure communication channel tolerant to vulnerabilities which does not rely on only one cryptographic mechanism. It is our belief that *diversity* and *redundancy* of cryptographic mechanisms and certificates can help mitigate existent vulnerabilities. In our project's context, diversity and redundancy consist in using two or more different mechanisms/cipher suites with the same objective. For example, MD5 and SHA-3 are both hash functions used to generate digests. In a real case, where MD5 has become insecure, our diverse and redundant secure communication channel relies upon SHA-3 to keep the communication secure. Using diversity and redundancy of cryptographic mechanisms, when a one of those mechanisms is successfully attacked, another mechanism is able to maintain the security and availability of the communication.

- The contributions of this paper are: x,y,z

Using diversity and redundancy, superTLS aims at increasing security over current secure communication channels. Guaranteeing a diversity factor $k > 1$, which implies having k different cipher suites with optimally k different mechanisms for each of the following:

- Key exchange;
- Authentication;
- Encryption;
- MAC: HMAC/AEAD (used for data integrity). **NOTE: In TLS, HMAC is used for CBC and stream cipher. AEAD is used for GCM and CCM (MtE)**

Although SSL/TLS supporting strong encryption mechanisms, such as AES and RSA, there are other factors than mathematical complexity that can contribute to vulnerabilities. Diversifying encryption mechanisms includes diversifying certificates and consequently keys (public, private, shared). Diversity of certificates is a direct consequence of diversifying encryption mechanisms due to the fact that each certificate is related to an authentication and key exchange mechanism.

One of the challenges of this project is to study if diversity and redundancy have a real impact on increasing security of a communication channel while having reasonable performance and time-related costs which required a precise measurement of our solution.

- The rest of the paper is organized as followed: z,y,x

The rest of the document is organized in the following way: Section 2 presents the related work. Section 3 presents the architecture of the proposed solution. Section 4 presents the evaluation. Section 5 presents some conclusions.

2. RELATED WORK

What are the current issues/vulnerabilities in the existing systems/mechanisms?

- Brief TLS
- Mechanisms vulnerabilities
- Brief combining mechanisms OR brief diversity

3. OVERVIEW

SuperTLS is a diverse and redundant secure communication channel. It aims at increasing security using diverse and redundant cryptographic mechanisms and certificates, and it is based on the TLS 1.2 protocol. Although being an independent secure communication channel, superTLS is compatible with TLS 1.2 but does not support all of TLS 1.2 cipher suites. (such as the ones containing PSK and SRP mechanisms)

This project aims to solve the main problem originated by having only one cipher suite negotiated between client and server. When one of the cipher suite's mechanisms becomes insecure, the secure communication channels using that cipher suite may become vulnerable. Unlike TLS communication channels, superTLS does not rely in only one cipher suite. Using superTLS, more than one cipher suite is negotiated between client and server and, consequently, more than one encryption mechanism will be used for each purpose – key exchange, authentication, encryption and MAC.

Although most cipher suites used by TLS 1.2 are regarded as secure, as stated in Section 2, there is not any assurance that a governmental agency or a company with high computational power and financial resources is not able to break one of the encryption mechanisms in the near future.

3.1 Protocol Specification

- Images updated from the thesis' project

3.2 Implementation

- Explain second cipher suite [X-Factor] audition and selection

4. EXPERIMENTAL EVALUATION

5. CONCLUSIONS

This paragraph will end the body of this sample document. Remember that you might still have Acknowledgments or Appendices; brief samples of these follow. There is still the Bibliography to deal with; and we will make a disclaimer about that here: with the exception of the reference to the LaTeX book, the citations in this paper are to articles which have nothing to do with the present subject and are used as examples only.

6. FUTURE WORK

- Usar duas libraries e usar funÃğÃţes duma e doutra

7. REFERENCES

[1] S. Kent and K. Seo. Security Architecture for the Internet Protocol (RFC 4301), 2005.
[2] T. Ylonen and C. Lonvick. The Secure Shell (SSH) Protocol Architecture (RFC 4251), 2006.

8. REFERENCES

Generated by bibtex from your .bib file. Run latex, then bibtex, then latex twice (to resolve references) to create the .bbl file. Insert that .bbl file into the .tex source file and comment out the command `\thebibliography`.