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

André Joaquim
INESC-ID, Instituto Superior Técnico, Universidade de Lisboa
R. Alves Redol 9, 1000-029 Lisbon, Portugal

Miguel L. Pardal
INESC-ID, Instituto Superior Técnico, Universidade de Lisboa
R. Alves Redol 9, 1000-029 Lisbon, Portugal

Miguel Correia
INESC-ID, Instituto Superior Técnico, Universidade de Lisboa
R. Alves Redol 9, 1000-029 Lisbon, Portugal

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

ABSTRACT

We present superTLS, a diverse and redundant vulnerability-tolerant 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. superTLS' premise consists its mechanisms are 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 and TLS-over-TLS.

CCS Concepts

•**Computer systems organization** → **Embedded systems;** *Redundancy;* Robotics; •**Networks** → Network reliability;

Keywords

Diversity; Redundancy; Security; Secure channels

1. INTRODUCTION

- Description
- The contributions of this paper are: x,y,z
- The rest of the paper is organized as followed: z,y,x

WOODSTOCK '97 El Paso, Texas USA

DOI: 10.475/123_4

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. SUPERTLS/ARCHITECTURE

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. 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`.