Proof Of Concept for Opportunistic Security in MPLS Networks

Salil Ajgaonkar B.E

A Dissertation

Presented to the University of Dublin, Trinity College

in partial fulfilment of the requirements for the degree of

Master of Science in Computer Science (Future Network Systems)

Supervisor: Stephen Farrell

August 2018

Declaration

I, the undersigned, declare that this work has not previously been submitted as an exercise for a degree at this, or any other University, and that unless otherwise stated, is my own work.

Salil Ajgaonkar

August 7, 2018

Permission to Lend and/or Copy

I, the undersigned, agree that Trinity College Library may lend or copy this thesis upon request.

Salil Ajgaonkar

August 7, 2018

Acknowledgments

...ACKNOWLEDGMENTS...

Salil Ajgaonkar

University of Dublin, Trinity College
August 2018

Proof Of Concept for Opportunistic Security in MPLS Networks

Salil Ajgaonkar, Master of Science in Computer Science

University of Dublin, Trinity College, 2018

Supervisor: Stephen Farrell

Multiprotocol Label Switching (MPLS) is a high performance packet switching technology which supports packet switching for multiple protocols and access technologies. It provides networking corporations and government high speed, reliable data transfer over geographically dispersed sites as well as maintaining flexibility and high bandwidth data exchange.

Such heavy reliance on MPLS by big companies and the general public to manage their data means that any forms of successful attacks often have the potential to disrupt vital everyday operations. Attacks ranging from data theft to denial of service if successful may lead to severe damages to the corporation as well as the owner of the data.

Earlier work conducted by the Internet Engineering Task Force(IETF) have analyzed the various vulnerabilities and security threats that plague the MPLS technology and have drafted a potential resolution to some of the security issues. The work proposed the implementation of Opportunistic Security in the MPLS network using payload encryption to encrypt the underlying application data and protocols using secure key exchange between end to end or hop by hop Label Switching Routers (LSR's) on an MPLS Label Switched Path (LSP).

This paper aims to provide a proof of the concept to this proposed solution by implementing it on a practical controlled environment and measuring its effects on the overall functionality and feature of the presently running MPLS technology. The aim of this paper is to provide an idea regarding the feasibility of this solution in practical commercial application in the world.

Summary

MPLS is a network routing technology which uses circuit switching and packet switched network technologies to support data routing for multiple internal protocols. It is a protocol independent and highly scalable technology whose flexibility enables efficient utilization of network resources resulting in high quality of service at low cost. MPLS relies on the use of fixed bytes of data that represent as labels for routing decisions. These labels are pushed on top of a data packet at the ingress switch of an MPLS cloud. All the succeeding Label Switching Routers (LSR's) in the MPLS cloud refer these labels to appropriately route the data to the correct destination. The path to the destination is pre-configured in the LSR's Label lookup table rather than an IP routing table. This avoids any complex lookups or reading long network addresses and implementation of longest match algorithms. Once the MPLS packet reaches the egress switch of the MPLS cloud, the MPLS label is popped off and the data packet is then transmitted as a regular IP packet along the succeeding switches. The LSRs between the ingress and the egress switch of the MPLS cloud also have the capability of pushing and popping off the MPLS labels on the data packet to efficiently engineer the network traffic.

Networking corporations and service providers can leverage this flexibility to scale their network services. Using the advantages of MPLS they are able to run high bandwidth applications over seamless IP based networks that connect multiple, remote site [2].The reliance on MPLS VPNs by corporations and government agencies means

that attacks ranging from intercepting sensitive data to disrupting data, voice and multimedia services can significantly impact vital operations [2].

Data Security in MPLS previously mainly relied on Data security (e.g., confidentiality) in MPLS has previously relied on just two features: 1) Physical isolation of MPLS networks has been used to ensure that interception of MPLS traffic was not possible. 2) Higher-layer protocol security such as IPsec has been used whenever a particular flow has determined that security was desirable [1]. However these features have a number of vulnerabilities. The network is still vulnerable to network taps between links, misconfiguration of routers, data replication, as well as users might not enable end to end security of their applications [1].

To mitigate these vulnerabilites to some extent, the IETF drafted an internet-draft titled "Opportunistic Security in MPLS Networks draft-ietf-mpls-opportunistic-encrypt-03" which proposed a novel idea of implementing Opportunistic Security (OS) in the currently existing MPLS implementation. The internet draft suggested the implementation of opportunistic encryption of data packet payload which is held by the MPLS packet. As the LSR's only rely on the information contained in the MPLS labels for routing information the contents of the MPLS packet are of no significance for the flow of traffic. Thus end-to-end or hop-by-hop encryption of the data payload of the MPLS packet by the LSRs can contribute greatly to maintain the confidentiality, integrity and authenticity of the data that flows through the MPLS network.

This paper aims to implement this proposed experimental idea in a controlled environment by simulating the flow of traffic in an MPLS network in a virtual network and comparing the difference in performance between MPLS with the OS and MPLS without the OS. This will help validate or invalidate the proposed solution experimentally and further spread more light on its impact and feasibility on real world implementation.

Contents

List of Tables

List of Figures

Chapter 1

A first chapter

...

1.1 Section 1.1

...

Chapter 2

Another chapter

...

Bibliography

Appendix

...