Chapter 8

A Security Analysis of MPLS Service Degradation Attacks Based on Restricted Adversary Models

Abdulrahman Al-Mutairi
University of London, UK

Stephen D. Wolthusen
University of London, UK & Gjøvik University College, Norway

ABSTRACT

Whilst the security and integrity of exterior gateway protocols such as the Border Gateway Protocol (BGP) and, to a lesser extent, interior gateway protocols, including the Multi-Protocol Label Switching (MPLS), have been investigated previously, more limited attention has been paid to the problem of availability and timeliness that is crucial for service levels needed in critical infrastructure areas such as financial services and electric power (smart grid) networks. The authors describe a method for modeling adversaries for the analysis of attacks on quality of service characteristics underpinning such real-time networks as well as a model of policies employed by MPLS routers based on simplified networks and give an analysis of attack vectors based on assumed adversaries derived from the introduced method.

INTRODUCTION

Multi-Protocol Label Switching (MPLS) protocol is widely deployed not only as an interior gateway protocol within single organization networks, but also in networks where well-defined Quality of Service (QoS) characteristics are critical including electric power, financial services, and other critical infrastructure networks where demanding hard real-time requirements are in place. Whilst such networks were historically isolated, the current, so-called Next Generation Network (NGN) infrastructure visualizes such networks on top of internet substrate protocol (Lee and Knight, 2005).

Unlike in the case of the Border Gateway Protocol (BGP) exterior gateway protocol, even the existence of flows may not be visible due to the implementation of different routing techniques.
such as labels aggregation that is used for efficiency purposes (Rosen, Viswanathan, & Callon, 2001) or due to the confidentiality of traffic flows, also some routing policies must be considered confidential (Subramanian et al., 2005). However, at the same time MPLS networks tend to be better managed and monitored, imposing limitations on what an adversary may be considered capable of. In this work we describe a simplified network model to capture selected timing characteristics and identify the relevant parameters which may be subjected to deliberate attacks that may affect QoS directly or indirectly. To this end we also provide a simplified model of MPLS routing policies that is then forming the base of an analysis of attack vectors that adversaries of different capabilities may deploy to violate the QoS characteristics of given network flows.

Based on the above, we model common adversaries with more limitations that could emerge in MPLS networks. Then, we give an analysis primarily for QoS-related attack classes that adversaries may be able to deploy depending on the level of adversary capabilities ascribed, which itself provides guidance for the security requirements levied on MPLS routers and links interconnecting these routers.

Adversaries may seek to affect QoS parameters of a particular traffic flow and the relevant service level agreements (SLA) rather than launching Denial of Service (DoS) attacks against the entire network. Also, adversaries may seek to exploit knowledge of the attacked network to inform their possible attack targets and strategies as this will give insights into response behavior to disturbances induced by the adversary directly, by non-malicious traffic and incidents on shared network resources, or combinations of these.

The main contributions of this work are therefore the adversary modeling method that could be used to extract more suitable adversary models for specific security analysis for MPLS networks, based on which we perform a threat analysis describing several classes of attacks which an adversary may launch against policy mechanisms by manipulating the policy engines directly through mis-using the used signaling protocols or by altering the decision elements that policy engines use for routing processes; mainly, label entries in label stack.

RELATED WORK

As our work is motivated by the notion of mapping the QoS requirements which is mainly defined by hard real-time characteristics into the underlying networks for a well defined security analysis, we find that works addressing the availability and functionality of real-time networks are closely related. Indeed, a well designed real-time network that is capable of processing real-time traffic efficiently requires well studied and analyzed techniques to make sure all of the components in such networks act consistently and accordingly.

Yerraballi (Yerraballi and Mukkamalla, 1996) presented a way to analyze real time systems ability to meet the deadlines of tasks; particularly, by addressing the problem of end-to-end schedulability in distributed real-time system. Some of the concerns were discussed in the case that execution time changes (e.g arrival changes) in fixed priority scheduling environment. Alternatively, Thiele (Thiele, Chakraborty, & Naedele, 2000) presented a performance analysis approach using real time calculus which extends the basic concepts of network calculus. Basically, the presented method is aimed to analyze the flow of event streams through a network of computation and communication resources in any event stream environment.

Stoimenov (Stoimenov, Chakraborty, & Thiele, 2010) proposed an interface algebra based on the real time interfaces for verifying buffer overflow/underflow constraints and the worst-case traversal time (WCTT). Indeed the main contribution was the confirmation of the composable of multiple components while satisfying the buffer and WCTT constraints. In addition, Stoimenov et al. presented