1-6-2001

A security analysis for label switching routers

M. Al-Ibrahim
University of Wollongong, uow@al-ibrahim.edu.au

M. Savsar
Kuwait University

W. Adi
Technical University of Braunschweig, Germany

A security analysis for label switching routers

Abstract

Label Switching Routers (LSR), such as IP switching of Ipsilon, use separate Virtual Circuits (VC)from different sources even having the same destination. Merging switches, on the other hand, allow multiple VCs of upstream traffic to use a single output VC if having same destination criteria. In this paper, we study IP switching of Ipsilon and identify certain security threats. We found that oscillation between routing and switching as a result of a malicious frequent suspension and releasing of flows is a main security threat that decreases performance of such systems. To stabilize the performance in face of such an attack, we propose to utilize merging switches to mitigate the implications of oscillation in LSR. The simulation results enhances this claim.

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as: Al-Ibrahim, M, Savsar, M & Adi, W, A security analysis for label switching routers, ACS/IEEE International Conference on Computer Systems and Applications, 25-29 June 2001, 525-529.

A Security Analysis for Label Switching Routers

Mohamed Al-Ibrahim
School of IT and CS,
University of Wollongong
Wollongong NSW 2522
Australia
ibrahim@network.kuniv.edu.kw

Mehmet Savsar
Department of Systems Eng.
Kuwait University
P.O. Box 5969, Safat 13060
Kuwait
mehmet@kuc01.kuniv.edu.kw

Wael Adi
Institut for Computer Engineering,
Technical University of Braunschweig
D-38106 Braunschweig
Germany
w.adi@tu-bs.de

Abstract

Label Switching Routers (LSR), such as IP switching of Ipsilon, use separate Virtual Circuits (VC) from different sources even having the same destination. Merging switches, on the other hand, allow multiple VCs of upstream traffic to use a single output VC if having same destination criteria. In this paper, we study IP switching of Ipsilon and identify certain security threats. We found that oscillation between routing and switching as a result of a malicious frequent suspension and releasing of flows is a main security threat that decreases performance of such systems. To stabilize the performance in face of such an attack, we propose to utilize merging switches to mitigate the implications of oscillation in LSR. The simulation results enhances this claim.

1. Introduction

Increasingly, the Internet is growing in size and traffic, and is stimulating new designs of internetworking architecture. Some examples of switch routers that have recently appeared as a result of this trend are the IP switching by Ipsilon [3], the cell switching by Toshiba, the ARIS [5] by IBM, the SITA [2] by Finland Telecom, and the tag switching by Cisco. Sometimes this technology is referred to as Multi-protocol Label Switching. This technology is based on a number of criteria's that forms a special mechanism for establishing and terminating data transmissions. The first criteria is that, packets are switched in the hardware level after being routed for a time through software level. This establishes a Virtual Circuit through which the data is transmitted by the hardware speed. Second criteria is that, the connection is teared down when the switch does not notice data transmission for a specific period of time. Third criteria is that cells of a fragmented packet are accumulated in a buffer till a cell with an indication of end of packet arrives where the packet as a whole can be forwarded to the specific VC. The loss or the tamper of this cell has illusive indication for stream continuation. These unique proprietary mechanism of IP switch namely: cut through, tear down and End of Packet indication are a potential security flaws for such a system that could be a source for a number of scenarios for denial of service attack. The other objective of this paper that we try to address is, it is possible to solve certain security problems using different approaches other than the traditional ones. For example, we proposed to use a new sort of switches that have the capability of merging virtual connections to alleviate the impact of denial of service on the non-merge switches that are used in the label switch routers.

This paper is organized as follows. First, in section 2 we give general description and necessary background for label switching technology and proposed solution. Then we focus on the oscillation problem as a main security threat in IP switching, while in section 4 we propose a remedy for such a threat.

2. Label Switching Illustrated

Internet Protocol (IP) suite provides the foundation for the current data communication infrastructure. IP protocols have proven to be very flexible due to their connectionless nature and have been deployed widely over the past two decades. Additionally, they dominate current network technology. Asynchronous Transfer mode (ATM), on the other hand, can provide integrated services of media types and different bits rates. It offers unprecedented scalability and cost performance as well as the ability to reserve network resources for real-time oriented traffic and support for multi-point communication. Both network technologies, IP and ATM, have their strengths and weaknesses. For instance, one limitation of ATM networks has been the relatively large gap between the speed of the network data paths and that of control operations needed to configure those data paths to meet changing users'

0-7695-1165-1/01 $10.00 © 2001 IEEE

needs. IP's greatest strength, on the other hand, is its inherent flexibility and its capacity to adapt rapidly to changing conditions. These complementary strengths and limitations make it natural to combine IP with ATM to form a natural alliance that combines the best aspects of both technologies.

The marriage of both technologies promises to deliver a robust network technology. *Label Switching* is the general term for this technology. It is based on the integration of layer 2 (Data link layer) and layer 3 (Network layer) datagram labels to provide a high speed cut through mechanism for layer 3. (i.e. shift routing to layer 2 with higher speed) see Figure 1. In Label Switching , rather than examining and analyzing each header at each router, the router will examine the label assigned to the packet at hardware level, thereby accelerating the forwarding process.

Merging Flows in LSR

Consider a VC that has already been established to a certain destination with certain QoS parameters. Then if another flow with the same destination and specification raised from an ingress having the same destination label, even from a different source, then it is possible to merge the flows at the switch to form a joint egress stream. The idea is in caching the VC in switch memory so that the next cells appearance of the suspended flow, recognized by flow identifier, does not have to be routed (at layer 3). In Cached Switched Virtual Circuits, circuit time-out is 20 seconds. Virtual circuits that are idle for longer than this amount of time are cached for future re-use. After 300 seconds (5 minutes) for example, of idle time, they are torn down [9]. If a switch has already established a VC for a flow to the same destination then the merge switch may use this VC to direct the flow. Provided an optimal, fair and efficient scheduling algorithm is used in merging, VC switch merging in general reduces call setup time for establishing a VC in a switch and hence saves switch resources

This approach is useful because it (1) reduces the label space at each switch, (2) saves setup time to establish a VC (3) reduces the number of VC's and (4) reduces the pricing cost for call setup of a virtual circuit.

Widjaja et al. in [1] described the specification of implementing VC merging in switch from two directions: the hardware and the performance implication. They concluded that the overhead of VC merging in terms of the additional buffer requirement is minimal contrary to the widespread belief. The results claimed that the overhead decreases as utilization increases, or as the traffic becomes more burst. Based on simulation results, the study encourages deploying such switches, provided a fair, optimal and efficient scheduling algorithm is used.

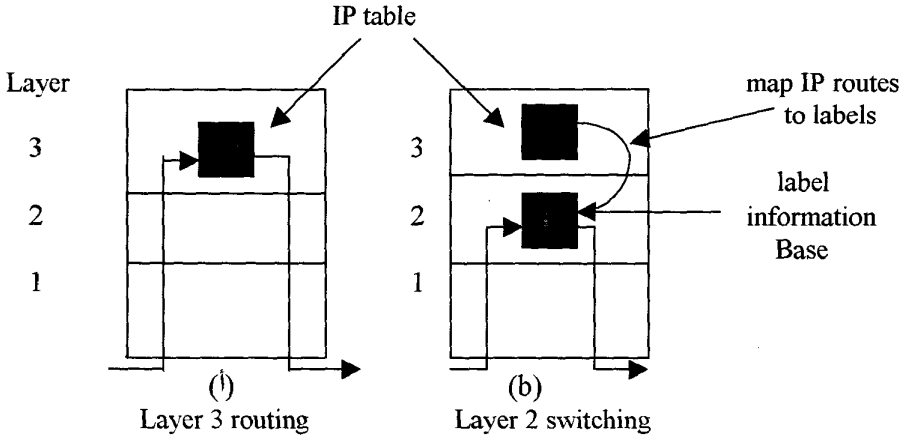

Figure 1. (depicted from [1])

3. Security Threats on label Switching Networks

We will consider IP Switching of Ipsilon as case study of a MPLS network, and as the best of our knowledge, there is no relative work similar to this case study. As mentioned before that IP switching employs a special mechanism for establishing a connection and forwarding IP packets as well as adopting a special mechanism for cutting through and tearing down a connection. Due to the space limitation we will focus in particular on the cut-through mechanism and study its security implications.

Oscillation

The decision to flip from routing to switching, i.e."*cut-through*" , so the data will no longer be routed, is a crucial one and depends on the classifier mechanism adopted in the switch, see Figure 1 (b). The cut-through occurs when the LSR encounters a long flow and decides after N number of packets to switch the traffic at layer 2 after being routed at layer 3. On the other hand, the flow "*tears-down*" if it encounters a gap or delay of packet arrival after a T amount of time. We define the phenomena of frequent flipping from routing to switching and from switching to routing as *Oscillation*. Oscillation may be caused by malicious suspending (blocking) of datagrams flowing. For example, consider a long lasting application such as http file that is forwarded through an IP switch of X/Y classifier. The switch may decide after forwarding N packets to cut-through. Suppose an attacker, is siting between an IP host and a switch , acting as a gate, and deliberately blocking the flow through the switch for a time T equals to time set in the switch that is required to tear down a VC connection. This action causes the VC to tear down while the actual application flow has not yet been terminated. The suspended flow will be released later and the LSR will start routing it again for a given number of packets N, and decides to cut-through, the flow will then be suspended for a T time, the VC will tear-down and so forth. This phenomena has severe implications on the performance of the IP switch, especially on those switches with a short timeout tear-down period and small number of packets to cut through. It causes "*Oscillation*" between routing and switching.

The other source of oscillation is IP Header Tampering. Port classifiers and protocol classifiers depend on the port number and UDP or TCP information in deciding whether to establish a VC. Tampering port numbers, from example, from 80 to 25, results changing flow nature from a long lasting flow (http) to a short lasting flow (smtp). This results routing a long lasting flow (layer 3) rather than switching it(layer 2). The switches that have a direct link to an IP sources (host or router) are most likely to face this attack, because these switches are the ones that take the decision to switch cells and to send IFMP cut-through messages to the next switch.

4. Proposed Security Scheme

To handle oscillation caused by blocking or suspending flows, we exploit the merging criteria of the merge switch and enhance security by reducing the implication of such an attack. The reader may noticed that we have used the word 'reduce' rather than 'eliminate', because the proposed scheme does not address to solve the problem. Rather, we attempt to 'alleviate' the implications of such an attack by using merge switches in the LSR. The basic idea is that when a new flow enters a switch and it happen that a previous flow had already established a VC with the same flow specification and destination, then the IP switch does not have to route the packet, but rather switch them directly to the same VC at layer 2. By this way, the oscillation attack is better handled in contrast to non-merge switches.

To study the implication of oscillation problem on the performance of both merge switch and non-merge switches, we ran a simulation program and set a comparison. We fixed the forwarding processing time for both type of switches based on assumption that both have relatively similar processing time [1]. We created different stream flows (data, audio and video) on both switches and mimicked the scenario in the previous section. Both flows of the different sources are destined to the same destination. We assume that one of the flows is subject to denial of service by an attacker who blocks the flow on frequent basis equals the time needed to tear down an established VC and release the flow after the connection is teared down. The goal is to study the performance of the switches in such sort of attacks as described in section 3.

Simulation Study

Simulation results are summarized in two graphs given in Figure 2 and Figure 3. Each point in the graphs is the average of 10 simulation runs at

different data releasing times introduced by the attacker. The data releasing time was changed from 1 to 10 seconds and the utilization's of layer 2 and layer 3 were determined by simulating the system for the non-merge and merge switches. The time between the arrivals of data packets was assumed to exponential with mean 0.08 milliseconds. The processing times were fixed at 0.01 and 0.04 milliseconds for layer 2 and layer 3 respectively. It was assumed that the data flow was cut through at 5 seconds. Figure 2 shows that as the attacker releasing time increases from 1 second to 10 seconds, the utilization of layer 2 also increases steadily for both types of switching, namely non-merge and merge cases. This implies that as the attacker increases the releasing time, he will be able to make layer 2 more and more busy. On the other hand, Figure 3 shows how layer 3 in the non-merge case reacts to the release time of the attacker. It is interesting that in the merge switch case; layer 3 has no effect at all with respect to the release time of the attacker. There will not be any oscillation for the same flow duration. In non-merging case however, layer 3 is affected until the release time is equal to the cut through time. We can conclude that if the cut through time is decreased, the utilization of layer 2 is increased and thus more and more data is processed.

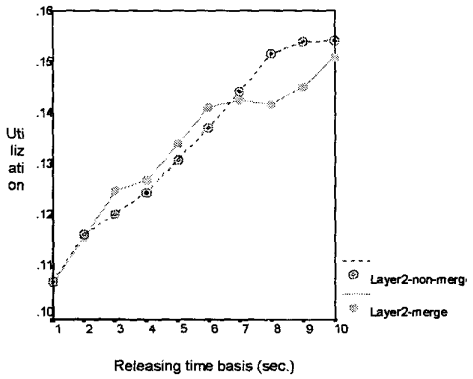

Figure 2.

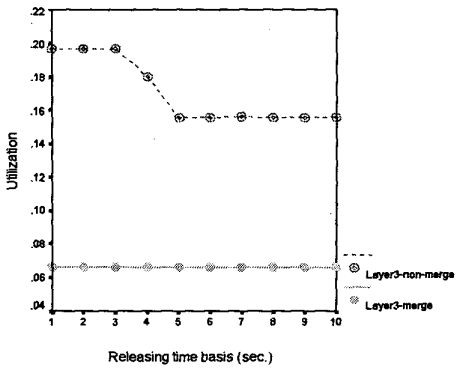

Figure 3.

Another obvious advantage of this scheme is apparent in reducing the number of labels and keys. In order for a merge switch to be used with cryptographic unit, their must exist a mechanism between the Crypt Unit and the Merging Unit to enable the Crypt Unit to assign different keys to the traffic when the output buffer is assigned with traffic of different destinations. In the case of merge switch, the cryptographic unit will use the same key for a new flow as the key that was used for the earlier established connection, thus reducing key pool size. This contrasts with the non-merge switch, where each VC has a different key even with VC's that have the same destinations. Besides, the key-agile unit has to work fast enough to change keys to keep synchronized with cell transmission.

5. Conclusion

New technology brings with it unprecedented security threats, and IP switching is relatively new technology that its security was investigated in this paper. We have described and simulated the " oscillation" attack and suggested to enhance the security in IP switching of Ipsilon against such a threat using merging switches. Simulation results on merge switches shows how it alleviates the implication of such an attack.

References

[1] I. Widjaja and A. El-Walid, "Performance Issues in VC-Merge Capable MPLS Switches", *IEEE journal on Selected Areas in Communications*, p: 1178 – 1189 , Vol : 176, June 1999.

[2] J. Heinanen, " SITA: Switching IP through ATM", *Telecom Finland*, Internet Draft, 1996.

[3] P. Newman, T. Lyon, and G. Minshall, " Flow Labeled IP: a connectionless Approach to ATM", Proc. *IEEE INFOCOM*, San Fransisco, vol. 3, pp.1251-1260, Mar. 1996.

[4] P. Newman, T. Lyon, G.Minshall, "Flow Labeled IP: Connectionless ATM Under IP" *Proceedings of IEEE INFOCOM'96, 1996.*

[5] A. Viswanathan, Y. N. Feldman, R. Boivie and R. Woundy, " ARIS: Aggregate Route-Based IP Switching" *IETF Internet Draft*, Mar 1997.

[6]. G. Parulkar, D. Schmidt and J. Turner, "IP over ATM: A strategy for integrating IP with ATM", *Proc. ACM SIGCOMM*, Cambridge, MA. Sept. 1995.

[7] B. Khasnabish and M. Ahmadi, *"In Search of a Fair Scheduling Policy for Serving Multi-Queue Systems"* , Proc. Of the Canadian Conference on Electrical and Computer Engineering, IEEE, N.Y., pp. 1239- 1242, vol. 2, 1993.

[8] S. Lin and N. Mckeown,"A simulation study of IP Switching", *Proc. of ACM SIGCOMM*, 1997.

[9] B. Mah, "Quality of Service and Asynchronous ATM in IP Internet work", *Ph.D. dissertation. Uni. Of California* , Berkely, Dec. 1996.

[10] D. Stevenson, N. Hillery and G. Byred, "Secure Communication in ATM Networks", *Communication of the ACM,* vol. 28, no. 2, Feb. 1995.

[11] S. C. Chaung, "Securing ATM Networks", *Journal of Computer Security*, vol. 4, no. 4, pp. 289-329, 1996.

[12] M. Luarent, "*Security Flow Analysis of the ATM Emulated LAN Architecture*", Proc. IFIP, 1996.

[13] M. Baladi, D. Bergamasco, and D. Malagrino, "VC Merging on ATM", Internet draft: http://www.polito.it/~dmalagri/research.

[14] Z. Liu and P. Nain, "Optimal Scheduling in Some Multi-Queue Single Server System", *Proc. of INFOCOM'90, IEEE*, vol. 3, pp.1213- 1219, June1990.

[15] C. Lund, S. Phillips and N. Reingold, " Adaptive holding policies for IP over ATM Networks", *Proc. of INFOCOM'95 , IEEE*, Boston, vol. 1, pp. 80-87, 1995.