ISSN:0975-9646
Ch.Pandu Ranga Rao et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1741-1742

Sensing Malicious Packet Losses

Ch.Pandu Ranga Rao,M.Vani Pujitha
Department of Computer Science and Engineering
V R Siddhartha Engineering College
Vijayawada—522007

Abstract: **In this paper, we consider the problem of detecting whether a compromised router is maliciously manipulating its stream of packets. In particular, we are concerned with a simple yet effective attack in which a router selectively drops packets destined for some victim. Unfortunately, it is quite challenging to attribute a missing packet to a malicious action because normal network congestion can produce the same effect. Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities. Previous detection protocols have tried to address this problem with a user-defined threshold: too many dropped packets imply malicious intent. However, this heuristic is fundamentally unsound; setting this threshold is, at best, an art and will certainly create unnecessary false positives or mask highly focused attacks.**

I proposed a compromised router detection protocol that dynamically infers the precise no of congestive packet losses that will occur. Once the congestion ambiguity is removed, subsequent packet losses can be safely attributed to malicious actions. This protocol is the first to automatically predict congestion in a systematic manner and that is necessary for making any such network fault detection practical. In the remainder of this paper, we briefly survey the related background material, evaluate options for inferring congestion, and then present the assumptions, specification and a formal description of a protocol that achieves these goals. This protocol can be evaluated in a small experimental network and demonstrate that it is capable of accurately resolving extremely small and fine-grained attacks.

Keywords: **Internet dependability, distributed systems, reliable networks, malicious routers.**

I. INTRODUCTION

The Internet is not a safe place. Unsecured hosts can be compromised within minutes of connecting to the Internet and even well-protected hosts face the problems with denial-of-service (DoS) attacks. Indeed, through the combinations of social engineering and weak passwords, attackers have seized control over thousands of Internet routers. Some controversial presentations demonstrate how Cisco routers can be compromised via simple software vulnerabilities. Once a router has been compromised in such a fashion, an attacker may interpose on the traffic stream and manipulate it maliciously to attack others—selectively dropping, modifying, or rerouting packets.

Several researchers have developed distributed protocols to detect such traffic manipulations, typically by validating that traffic transmitted by one router is received unmodified by another . However, all of these schemes—including our own—struggle in interpreting the absence of traffic. While a packet that has been modified in transit represents clear evidence of tampering, a missing packet is inherently ambiguous: it may have been explicitly blocked by a compromised router or it may have been dropped benignly due to network congestion. In fact, modern routers routinely drop packets due to bursts in traffic that exceed their buffering capacities, and the widely used Transmission Control Protocol (TCP) is designed to cause such losses as part of its normal congestion control behavior. Thus, existing traffic validation systems must inevitably produce false positives for benign events and/or produce false negatives by failing to report real malicious packet dropping.

II. NEED AND IMPORTANCE OF PROJECT PROBLEM

In the existing system, the sender sends the packets without the intermediate station. The data packets has been losses many and time is wasted. Retransmission of data packets is difficulty. In this project Network routers occupy a unique role in modern distributed systems. They are responsible for cooperatively shuttling packets amongst themselves in order to provide the illusion of a network with universal point-to-point connectivity.

However, this illusion is shattered - as are implicit assumptions of availability, confidentiality, or integrity - when network routers are subverted to act in a malicious fashion. By manipulating, diverting, or dropping packets arriving at a compromised router, an attacker can trivially mount denial-of-service, surveillance, or man-in-the-middle attacks on end host systems. Consequently, Internet routers have become a choice target for would-be attackers and thousands have been subverted to these ends. In this paper, we specify this problem of detecting routers with incorrect packet forwarding behavior and we explore the design space of protocols that implement such a detector.

We further present a concrete protocol that is likely inexpensive enough for practical implementation at scale. Finally, we present a prototype system, called Faith, that implements this approach on a PC router and describe our experiences with it. We show that Faith is able to detect and isolate a range of malicious router actions with acceptable overhead and complexity. We believe our work is an important step in being able to tolerate attacks on key network infrastructure components.

III. OBJECTIVE

This project aims at to design, develop, and implement a compromised router detection protocol that dynamically infers, based on measured traffic rates and buffer sizes, the number of congestive packet losses that will occur.

Once the ambiguity from congestion is removed, subsequent packet losses can be attributed to malicious actions.

IV. METHODOLOGY

DATA QUEUE:

A data queue is a buffer, maintained by a sender , for transmission and retransmission of the data packets provided by the sender application. New data packets are added to the data queue as they arrive from the sending application, up to a specified buffer limit. The admission rate of packets to the network is controlled by congestion control algorithms.

TRAFFIC VALIDATION:

The first problem we address is traffic validation: what information is collected about traffic and how it is used to determine that a router has been compromised.

Consider the queue Q in a router r associated with the output interface of link (r, rd) in the below figure. The neighbor routers rs1, rs2 , . . . , rsn feed data into Q.

We denote with Tinfo(r,Qdir,PI ,T) the traffic information collected by router r that traversed path segment PI over time interval T. Qdir is either Qin, meaning traffic into Q, or Qout, meaning traffic out of Q.

The following are the steps for controlling congestion.

1) The router discards the one or more packets before the buffer becomes full.
2) To determine when to start discarding, routers maintain running avg. of their queue lengths .
3) If the avg. is lower than the some lower threshold, congestion is min. and packet is queued.
4) If avg. is greater than the some upper threshold, congestion is very high and packet is discarded.
5) In this way, the buffer is prevented from getting full by discarding packets and congestion is prevented.

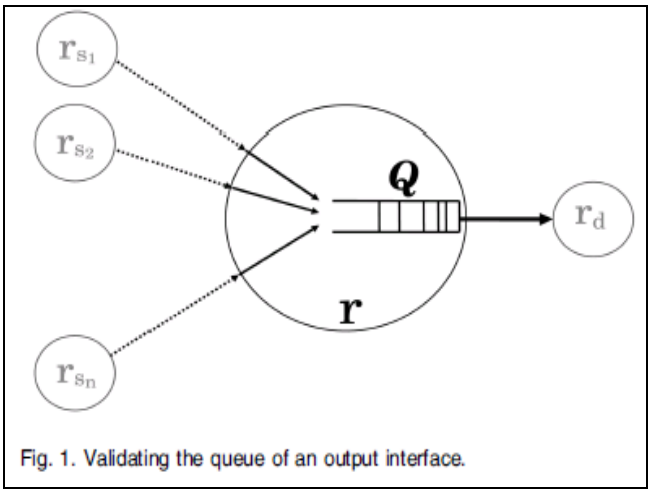

Fig. 1. Validating the queue of an output interface.

V. HYPOTHESIS

In the normal network criteria, even if there are no attacks from the intruders or attackers then there may be a chance of minimum no. of packet losses. Once the router has been compromised, attackers may interpose on the traffic stream and manipulate it maliciously to attack others- selectively dropping, modifying, or rerouting packets.

In normal case, when a text file can be send from source to the destination then there may be a chance of minimum of packet losses. If the attackers maliciously attacking the routers, then there may be a chance of max no. of packet losses. By using this project, we can identify and detect whether the packets have been loss or not while transmitting the data from sender to the receiver.

VI.CONCLUSION

To the best of our knowledge, this paper is the first serious attempt to distinguish between a router dropping packets maliciously and a router dropping packets due to congestion. Previous work has approached this issue using a static user-defined threshold, which is fundamentally limiting. Using the same framework as our earlier work (which is based on a static user-defined threshold) we developed a compromised router detection protocol that dynamically infers, based on measured traffic rates and buffer sizes, the number of congestive packet losses that will occur. Subsequent packet losses can be attributed to malicious actions. Because of non determinism introduced by imperfectly synchronized clocks and scheduling delays, protocol uses user-defined significance levels, but these levels are independent of the properties of the traffic. Hence, protocol does not suffer from the limitations of static thresholds. We evaluated the effectiveness of protocol through an implementation and deployment in a small network. We show that even fine-grained attacks, such as stopping a host from opening a connection by discarding the SYN packet, can be detected.

VII.REFERENCES

[1] A.T. Mizrak, Y.-C. Cheng, K. Marzullo, and S. Savage, “Detecting and Isolating Malicious Routers,” IEEE Trans. Dependable andSecure Computing, vol. 3, no. 3, pp. 230-244, July-Sept. 2006.

[2] R. Thomas, ISP Security BOF, NANOG 28, http://www.nanog.org/mtg0306/pdf/thomas.pdf, June 2003.

[3] K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, and R.A. Olsson, “Detecting Disruptive Routers: A Distributed Network Monitoring Approach,” Proc. IEEE Symp. Security and Privacy (S&P ’98), pp. 115-124, May 1998.

[4] B.R. Smith and J. Garcia-Luna-Aceves, “Securing the Border Gateway Routing Protocol,” Proc. IEEE Global Internet, Nov. 1996.

[5] B.R. Smith and J. Garcia-Luna-Aceves, “Securing the Border Gateway Routing Protocol,” Proc. IEEE Global Internet, Nov. 1996.

[6] J.R. Hughes, T. Aura, and M. Bishop, “Using Conservation of Flow as a Security Mechanism in Network Protocols,” Proc. IEEE Symp. Security and Privacy (S&P ’00), pp. 131-132, 2000.

[7] A. Mizrak, Y. Cheng, K. Marzullo, and S. Savage, “Fatih: Detecting and Isolating Malicious Routers,” Proc. Int’l Conf. Dependable Systems and Networks (DSN ’05), pp. 538-547, 2005.

[8] A. Kuzmanovic and E.W. Knightly, “Low-Rate TCP-Targeted Denial of Service Attacks: The Shrew versus the Mice and Elephants,” Proc. ACM SIGCOMM ’03, pp. 75-86, 2003.

[9] M. Mathis, J. Semke, and J. Mahdavi, “The Macroscopic Behavior of the TCP Congestion Avoidance Algorithm,” SIGCOMM Computer Comm. Rev., vol. 27, no. 3, pp. 67-82, 1997.

[10] N. Cardwell, S. Savage, and T.E. Anderson, “Modeling TCP Latency,” Proc. INFOCOM ’00, pp. 1742-1751, 2000.