Recognition of mischievous data packets In the networking

G.Bala Venkata Kishore, B.Purnaiah, B.kishore Babu, A.Siddharatha Reddy

Abstract: The TCP has provided the primary means to transfer data reliably across the Internet however TCP has imposed limitations on several applications. Measurement Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities. Early detection protocols have tried to address this problem with a user-defined threshold the finding of detecting and removing compromised routers can be thought of as an instance of anomalous behavior-based intrusion detection. That can be the compromised router can that identified by correct routers when it deviates from exhibiting expected behavior. This protocol can be evaluated in a small experimental network and demonstrate that it is capable of accurately resolving extremely.

Index Terms: Mobile ad hoc network, Security Goals**,** efficient scheme, security, public-key, cryptography, Traffic validation, responses

—————————— ◆ ——————————

1 INTRODUCTION

TCP has provided the primary means to transfer data reliably across the Internet; however TCP has imposed limitations on several applications. Measurement and estimation of packet loss characteristics are challenging due to the relatively rare occurrence and typically short duration of packet loss episodes. While active probe tools are commonly used to measure packet loss on end-to end paths, there has been little analysis of the accuracy of these tools or their impact on the network. The main objective is to understand the problem of detecting whether a compromised router is maliciously manipulating its stream of packets. In particular to this concern 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 .Such attacks are not mere theoretical curiosities, but they are actively employed in practice. Attackers have repeatedly demonstrated their ability to compromise routers, through combinations of social engineering and exploitation of weak passwords and latent software vulnerabilities. One network operator recently documented Over 5,000 compromised routers as well as an underground market for trading Access to them several researchers has developed Distributed protocols. Detect such traffic manipula Tions 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. 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 Internet routing is based on a distributed system composed of many routers, grouped into management domains called Autonomous Systems (ASes). Routing information is exchanged between ASes in Border Gateway Protocol (BGP) [1] UPDATE messages. BGP has proven to be highly vulnerable to a variety of attacks [2], due to the lack of a scalable means of verifying the authenticity and legitimacy of BGP control traffic. In April 1997, we began work on the security architecture described in this paper. In this section we describe the problem–how the protocol works, the nature of observed BGP traffic in the Internet, the correct operation of BGP, the threat model and BGP vulnerabilities, and the goals, constraints and assumptions that apply to the proposed countermeasures.

2 Back Ground

In the background we have there are two threats posed by a compromised router. The attacker may subvert the network control plane (e.g., by manipulating the routing protocol into false route updates) or may subvert the network data plane and forward individual packets incorrectly. The first sets of attacks have seen the widest interest and the most activity largely due to their catastrophic potential. By violating the routing protocol itself, an attacker may cause large portions of the network to become inoperable At the time that we began this work, previously published work on improving the security of BGP, and more generally distance-vector protocols, included proposals for adding sequence numbers to BGP messages authentication of BGP messages [1,5,6], neighbor-to-neighbor encryption of BGP messages [4], and adding information to UPDATE messages to protect against tampering as the UPDATE propagates around the Internet [4,5,7].None of this work proposed a comprehensive solution to the BGP security problems described above; each focused on one or more aspects of the problem without considering the full range of issues that are critical to a viable solution. For example, none addressed issues associated with the generation and distribution of public key certificates and certificate revocation lists (CRLs) needed to support validation of signed UPDATEs. Some proposals made changes to BGP that are inconsistent with the protocol standards, a reasonable approach only if one were presented with a "clean slate." None of the prior work examined the statistics of BGP operating in the Internet; this sometimes led authors to focus on performance concerns that are not the major impediment to deploying viable solutions. Some of the work developed solutions for distance vector protocols, but erroneously claimed applicability to BGP, which is described as a path vector protocol. In contrast, the BGP security architecture reported in this paper is comprehensive, including a design for the infrastructure needed to establish and maintain the system. The optional transitive path attribute it employs is consistent with BGP standards and can be safely carried through routers not implementing S-BGP. This architecture incorporates the notion of an address attestation, which establishes that a "first hop" BGP speaker is authorized to advertise a route to a destination. No prior work includes an equivalent notion. Finally, the performance of the design presented here has been modeled based on actual BGP statistics. No other work has been so rigorously analyzed from a performance perspective.

3. THE CONGESTIVE LOSS

In building a traffic validation protocol, it is necessary to explicitly resolve the ambiguity around packet losses. Should the absence of a given packet be seen as malicious or In practice there are three approaches for addressing this issue:

.

Static Threshold. In the Threshhold Low rates of packet loss are assumed to be congestive, while rates above some predefined threshold are deemed malicious.

Traffic Modeling. In the Traffic Modeling Packet loss rates are predicted as a function of traffic parameters and losses beyond the prediction are deemed malicious.

Traffic Measurement. In the Traffic Measurement Individual packet losses are predicted as a function of measured traffic load and router buffer capacity. Deviations from these predictions are deemed malicious. Most traffic validation protocols, including WATCHERS Secure Trace route [12], and our own work described in [4], analyzes aggregate traffic over some period of time in order to amortize monitoring overhead over many packets. For example, one validation protocol described in [4] maintains packet counters in each router to detect if traffic flow is not conserved from source to destination. When a packet arrives at router r and is forwarded to a destination that will traverse a path segment ending at router x, r increments an outbound counter associated with router x. Conversely, when a packet arrives at router r, via a path segment beginning with router x, it increments its inbound counter associated with router x. periodically, router x sends a copy of its outbound counters to the associated routers for validation. Then, a given router r can compare the number of packets that x claims to have sent to r with the number of Packets it counts as being received from x, and it can detect the number of packet losses. Thus, over some time window, a router simply knows that out of m packets sent, n were successfully received. To address congestion ambiguity, all of these systems employ a predefined threshold: if more than this number is dropped in a time interval, then one assumes that some router is compromised. However, this heuristic is fundamentally flawed: how does one choose the threshold? In order to avoid false positives, the threshold must be large enough to include the maximum number of possible congestive legitimate packet losses over a measurement interval. Thus, any compromised router can drop that many packets without being detected. Unfortunately, given the nature of the dominant TCP, even small numbers of losses can have significant impacts. Subtle attackers can selectively target the traffic flows of a single victim and within these flows only drop those packets that cause the most harm. For example, losing a TCP SYN packet used in connection establishment has a disproportionate impact on a host because the retransmission time-out must necessarily be very long (typically 3 seconds or more). Other seemingly minor attacks that cause TCP time-outs can have similar effects a class of attacks All things considered, it is clear that the static threshold mechanism is inadequate since it allows an attacker to mount vigorous attacks without being detected. Instead of using a static threshold,then one could resolve ambiguities by comparing measured loss rates to the rates predicted by the model. One approach for doing this is to predict congestion analytically as a function of individual traffic flow parameters, since TCP explicitly responds to congestion. Indeed, the behavior of TCP has been excessively studied A simplified1 stochastic model of TCP congestion control.

$$B = \frac{1}{RTT}\sqrt{\frac{3}{2bp}}$$

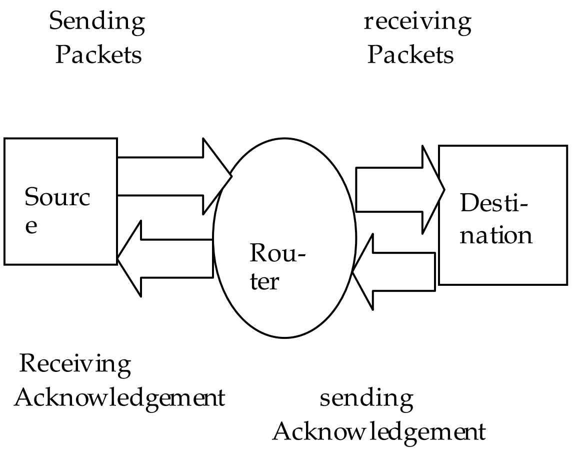

Fig 1: flow of data from source to destination

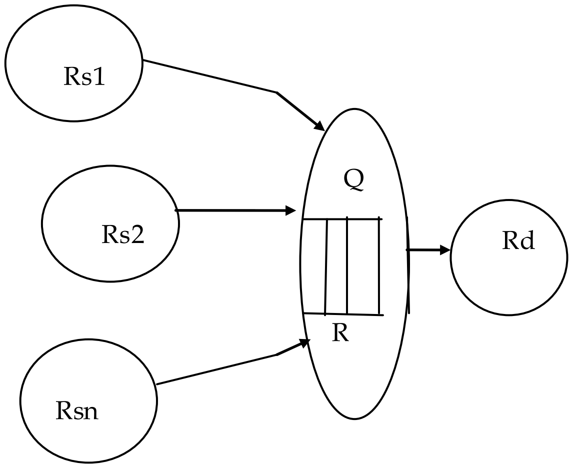

Fig 2: validating of queue of the output interface

4 Network Model

We have to consider a network to consist of individual homogeneous routers interconnected via directional point-topoint links. This model is an intentional simplification of real networks (e.g., it does not include broadcast channels or independently failing network interfaces) but is sufficiently general to encompass such details if necessary. Unlike our earlier work, we assume that the bandwidth, the delay of each link, and the queue limit for each interface are all known publicly. Within a network, we presume that packets are forwarded in a hop-by-hop fashion, based on a local forwarding table. These forwarding tables are updated via a distributed link-state routing protocol such as OSPF or IS-IS. This is critical, as we depend on the routing protocol to provide each node with a global view of the current network topology. Finally, we assume the administrative ability to assign and distribute cryptographic keys to sets of nearby routers. This overall model is consistent with the typical construction of large enterprise IP networks or the internal structure of single ISP backbone networks but is not well suited for networks that are composed of multiple administrative domains using BGP. At this level of abstraction, we can assume a synchronous network model.We defin of adjacent routers. Operationally, a path defines a sequence of routers a packet can follow. We call the first router of the path the source and the last router its sink; together, these are called terminal routers. A path might consist of only one router, in which case the source and sink are the same. Terminal routers are leaf routers: they are never in the middle of any path.

5 THE PROTOCOL X

The Protocol x detects traffic faulty routers by validating the queue of each output interface for each router. Given the buffer size and the rate at which traffic enters and exits a queue, the behavior of the queue is deterministic. If the actual behavior deviates from the predicted behavior, then a failure has occurred. We present the failure detection protocol in terms of the solutions of the distinct subproblems: traffic validation, distributed detection, and response.and the correctness of the protocol

6 The Single Packet Loss

The packet with fingerprint fp and size ps is dropped at time ts when the predicted queue length is q then we raise an alarm with a confidence value csingle, which is the probability of the packet being dropped maliciously. Csingle is the mean and standard deviation of X can be determined by monitoring during a learning period. We do not expect and to change much over time, because they are in turn determined by values that those selves do not change much over time. Hence, the learning period need not be done very often. A malicious router is detected if the confidence value csingle is at least as large as a target significance level slevel single.

7 Traffic Validation Correctness

The Traffic validation of the failure of detecting malicious attack by TV results in a false negative, and any misdetection of legitimate behavior by TV results in a false positive.Within the given system model of Section the example TV predicate is correct. However, the system model is still simplistic. In a real router, packets may be legitimately dropped due to reasons other than congestion errors in hardware, software or memory, and transient link errors. Classifying these as arising from a router being compromised might be a problem, especially if they are infrequent enough that they would be best ignored rather than warranting repairs the router or link. A larger concern is the simple way that a router isModeled in how it internally multiplexes packets. This model is used to compute time stamps. If the time stamps are incorrect, then TV could decide incorrectly. We hypothesize that a sufficiently accurate timing model of a router is attainable but have yet to show this to be the case. A third concern is with clock synchronization. This version of TV requires that all the routers feeding a queuehave synchronized clocks. This requirement is needed in order to ensure that the packets are interleaved correctly by the model of the router.The synchronization requirement is not necessarily Daunting; the tight synchronization is only required by routers adjacent to the same router. With low-level time stamping of packets and repeated exchanges of time it should be straightforward to synchronize the clocks sufficiently tightly. Other representations of collected traffic information and TV that we have considered has their own problems with false positives and false negatives. It is an open question as to the best way to represent TV. We suspect any representation will admit some false positives or false negatives.

8 CONCLUSIONS

This paper present to difference between a router dropping packets maliciously and a router dropping packets due to congestion this issue using a static user-defined threshold, which is fundamentally limiting. The same framework as our earlier work which is based on a static user-defined threshold 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.

REFERENCES

[1] R. Thomas, ISP Security BOF, NANOG 28, http://www.nanog org/mtg-0306/pdf/thomas.pdf, June 2003.

[2] 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.

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

[4] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. Katz, “Listen and Whisper: Security Mechanisms for BGP,” Proc. First Symp.Networked Systems Design and Implementation (NSDI ’04), Mar. 2004.

[5] S. Kent, C. Lynn, J. Mikkelson, and K. Seo, “Secure Border Gateway Protocol (Secure-BGP),” IEEE J. Selected Areas in Comm.,vol. 18, no. 4, pp. 582-592, Apr. 2000.

[6] Y.-C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Proc. ACM MobiCom ’02, Sept. 2002.

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

[8] S. Cheung, “An Efficient Message Authentication Scheme for LinkState Routing,” Proc. 13th Ann. Computer Security Applications Conf.(ACSAC ’97), pp. 90-98, 1997.

[9] M.T. Goodrich, Efficient and Secure Network Routing Algorithms, provisional patent filing, Jan. 2001.

[10] R. Perlman, “Network Layer Protocols with Byzantine Robustness,”PhD dissertation, MIT LCS TR-429, Oct. 1988.

[11] V.N. Padmanabhan and D. Simon, “Secure Traceroute to Detect Faulty or Malicious outing,” SIGCOMM Computer Comm. Rev.,vol. 33, no. 1, pp. 77-82, 2003.

[12] I. Avramopoulos and J. Rexford, “Stealth Probing: Efficient DataPlane Security for IP Routing,” Proc. USENIX Ann. Tecnical Conf.(USENIX ’06), June 2006.