Information Assurance in the SQoS Network

Pitipatana Sakarindr, Nirwarn Ansari, and Roberto Cessa-Rojas
Advanced Networking Laboratory, ECE Department, NJIT
Uiversity Heights, Newark, NJ 07102 US
{ps6, nirwan.ansari, roberto.rojas-cessa }@njit.edu

Abstract **In the SQoS network as introduced in [1] and [2], the border router in every autonomous system (AS) provides customized security mechanisms to the incoming packets. Some serious problems have been recently raised particularly when there are one or more compromised routers that attempt to modify, delete, or fabricate any part or the whole packet into the SQoS network. The compromised router can either passively or actively perform the malicious activities against the forwarding packets. The SQoS network does not explicitly specify the method to detect whether the data contained in the packets have been abused by the compromised routers or by the end host itself. We deliberate the threats and later propose several methods to detect both the malicious routers and end hosts such that SQoS information and payload is authentic and integrity-protected.**

Index Terms— Information assurance, SQoS network.

I. Introduction

The compromised router can maliciously conduct the following attacks against the packets: firstly, the passive attacks in which the compromised router can inspect, delay, or relay the packets to the third party; secondly, the active attack in which information can be modified or the packets can be injected into or deleted from the networks by the compromised routers as well as the compromised routers attempt to impersonate the other nodes in order to mislead or conceal their malicious behaviors.

The routers in the SQoS network provide several customized security mechanisms to the packets in an AS-to-AS manner, implying that only the edge routers execute the requested services. Apparently, the routers must be examined whether they follow appropriate procedures correctly.

In this paper, we present the problem statements in Section II, followed by the proposed solutions to the problems in Section III. We present the conclusions and discuss future works in Section IV.

II. Problem Statements

In this paper, we focus on detecting malicious routers and assuring the end hosts that data payload is safeguarded and the requested security services will be properly executed in the SQoS network. We separate the SQoS network into two environments: inter-autonomous system environment and intra-autonomous system environment. The intra-autonomous system environment creates a virtual tunnel between two edge routers, and it is considered as the outer part of the SQoS network. The two edge routers encrypt and decrypt the packets with its pair-wise symmetric key. The inter-autonomous system environment has a virtual end-to-end path from the sending end host to the receiving end host, and this path consists of passways. A passway is defined as the link between the two border routers of two adjacent autonomous systems. These environments can be illustrated in Fig. 1.

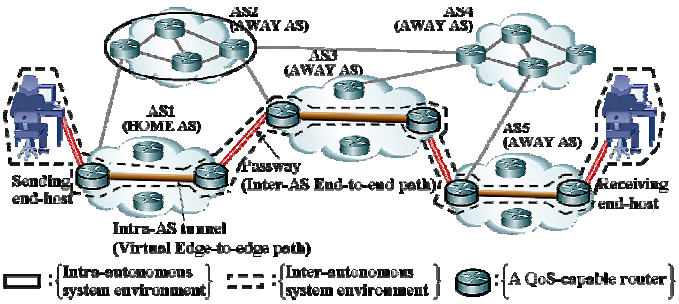

Figure 1. The environments of autonomous systems in the SQoS network.

The virtual edge-to-edge path means that the forwarding of the packet inside the AS on the edge-to-edge path is transparent to the forwarding on the end-to-end path. The implementation is to copy the IP header, encrypt the packet with a pair-wise symmetric key of the two edge routers, and concatenate the copied IP header at the front of the encrypted packet. When the packet reaches the other edge router, the copied IP header is stripped off and the encrypted packet is decrypted with the key. We use the concept of virtual edge-to-edge path to solve the threats, and it will be further discussed in Section III.

In this section we list the processes in SQoS that may be the target of the attacks, and cast the threats resulted from both the misbehaved routers and malicious end hosts. The threats basically threaten the following major characteristics of traffic: a validity of SQoS information, integrity of the data payload, and a fulfillment of the SSLA agreement.

A. Processes in the SQoS network that may be the Target of the Attacks

1. When the router receives the probing packet during the probing phase or the data packet during the data transmission phase with the requested services in the requested-security service vector (rSSV), it examines its resources before accepting or denying such a request. The result is recorded as either the offered services (during the probing phase) or the executed services (during the data transmission phase). In the SQoS network, the data packets can traverse the AWAY autonomous systems (ASes) with different security services and at different service levels. Every end host is ensured that the packet will be appropriately treated by the AWAY AS's routers in accordance with its SSLA, which the end host and its HOME AS are committed.
2. The routers in the HOME AS and AWAY ASes must regularly keep on updating the services and policies in the

SSP database. In addition, the routers in the HOME AS routinely update the customer profile in the SSLA database. Note that only the routers in the HOME AS maintains the customer profile in the SSLA database.

3. In the SQoS network, the SSLA indicates which customer is authorized to request which services. Thus, the router at the HOME AS must verify that the customer has an authorization to request the security services, based on its profile. The router is supposed to update frequently its SSLA database for any new or modified customer profile.

The control communications among components in the SQoS network is illustrated in Fig. 2.

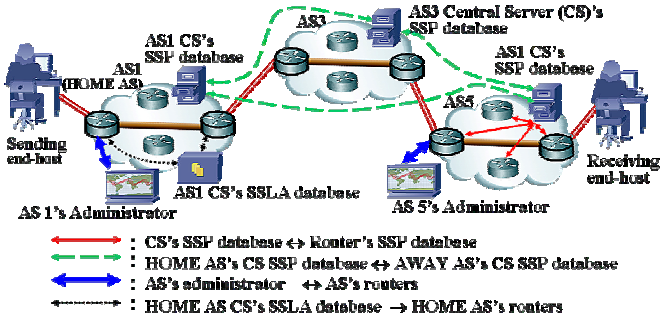

Figure 2. The communications among compenents in SQoS.

4. In the SQoS network, the routers are not necessarily required to keep SQoS information of all SQoS-aware traffics due to a limited storage. Instead, the router tags the preference into the probing packet so that the following data packets can be appropriately forwarded based on this preference. The preference is given, depending on the customer profile marked by the SSLA number in the SQoS header [1] (for different class traffics) and arrival time in a first-come-first-serve manner (for the same class traffics). Upon the receipt of the probing packet, the SQoS-capable router compares its SSLA number with the customer profile from the SSLA database for the customer's authorization. The preference is assigned based on a "preference timeout", and other SQoS information, which includes the customer profile and requested services. The router signs it with its private key. This signature is concatenated following the aSSV in the probing packet. When the associated data packet arrives with the corresponding requested-SSV and preference information, the services are then scheduled to be served accordingly. If the associated data packets arrives after the preference timeout expired, the router can reassign the lower preference, but within the same class. Because the routers at the AWAY ASes do not maintain the SSLA database and the SSLA number in the SQoS header can be spoofed, preference information from the HOME AS's router is used by those routers at the AWAY ASes to verify the class of traffic without knowledge of the actual customer profile.
5. Since the end-to-end path might be routed through many ASes that are operated with different network management policies and are using different network protocols, an accurate transition of the requested services between adjacent systems should be carefully designed. In the existing QoS-enabled networks, the autonomous systems can communicate and exchange policies and QoS information between their central server's SSP databases via several existing inter-AS routing and signaling protocols, such as RSVP security properties [3] and IP/MPLS inter-autonomous system traffic engineering protocol [4]. Thus, the AWAY AS's routers can execute the requested services with the same procedures as the HOME AS's router does.

B. *Threats from Malicious Routers and End-Hosts*

The threats can be categorized into two groups, and the threats in each group correspond to the processes mentioned earlier.

a) Malicious Router Threats

1. The malicious router can deny the requested services due to a lack of resources or unrecognized services, or offer the degraded services due to insufficient resources.
2. The malicious router may not regularly update the SSLA database (as well as the SSP database if it is also the HOME AS's router). In addition, it may change the customer profile or simply ignore it.
3. The router may not properly verify the customer profile or preference information, even if it has up-to-date information in the SSLA database. In addition, it may offer the services that the customer does not pay for.
4. The malicious or malfunctioned router can give wrong or erroneous preference to the probing packet.
5. The malicious router can modify, fabricate, drop, and delay the targeted packet.

b) Malicious End-Host Threats

1. The malicious end host may disrupt the processing router by requesting invalid (unrecognized) services.
3. The end host may request the requested services on which it has no privilege.
4. The malicious end host may alter the preference information to get its packets to be served first.

Additionally, the malicious end host and router can launch the replay attack against other routers by resending the copied packet in which its original has previously been executed. The replay attack aims to impersonate the legitimate sender, to cause congestion in the router's processing, etc.

Note that there are other possible attacks that can be launched against the SQoS network, but due to the limited space, they will be addressed in our future works.

III. Proposed Solutions

Before we deliver the proposed solutions to those problems, we first address the existing tools that can be used to implement the proposed solutions.

- The utilization of X.509 V.3 certificates [5] can be a fundamental key in processing authentication and signing the digital signature. X.509 can be used in the SQoS network because the certificate authority (CA), i.e., AS's administrator, issues a digital certificate that binds the public key to the customer's identification entities such as IP address while keeping the private key secret. The

customer then signs the packet or any information with the issued certificate. In case of dispute, the CA can verify whether such information is indeed generated by the disputed customer.

- Communications among network entities in different domains. The BGP is an inter-AS routing protocol that distributes routing information between routers in different ASes (in peer-to-peer fashion), as well as other information between service providers. The S-BGP in [6] is a security-enhanced version of the BGP and enables the following major features: authentication and authorization of the routing information originator and peering BGP router, as well as the integrity of routing information. The original BGP and S-BGP versions can be deployed in the SQoS network such that SSP information (via SBGP message) is protected, depicted as the shattered line in Fig. 2 where the central servers from AS1, AS3, and AS5 exchange information, particularly updating their SSP databases.
- Communications between network administrator and network entities. The administrator can manage the routers and check the router status to find any network problems. The simple network management protocol (SNMP) can be used to provide an essential management tool in the SQoS network. More gratefully, the SNMP version 3 has added the remote configuration and basic security capabilities in the network management, such as authentication and authorization [7]. SNMP can be used when the AS's administrator communicates with the routers to request and retrieve the router status and other parameters, depicted as the bold line in Fig. 2 where the AS's administrator requests and receives the router status and a snapshot of packet portions from the router. The method to taking a snapshot will be described shortly.
- Communications between network entities can be also implemented with the SNMP request and response messages, depicted as the dotted line in Fig. 2 where the AS's administrator requests or receives from the router the router status, including its queuing status, the number of packets waiting in queue for each preference, and a snapshot of portions of the denied packet.

The modification of the BGP and SNMP to incorporate into the SQoS network is not shown in this paper due to a limited space.

The first solution to the threats is to investigate the router status with helps from the end hosts and the AS's administrator. There are four cases that trigger the communications between the router and administrator.

1) For the case that the router denies or degrades the requested services, the router must immediately report the router status along with the snapshot of the portions of the packet.
   - If the router does not report immediately to the administrator, it will be immediately marked as a *bad* router. Such information in the report is primarily used to calculate the charge for each customer using the services. In the disputed case, it can then be used as an evidence to compare information reported by the end hosts and the router.
   - Information from the router will be matched with that from the end hosts. The end host, whose requested services are denied or degraded, launches the complaint to the administrator. Although the packets of some end-hosts have not been compromised by that malicious router, they should keep temporarily information about their served services for later possible disputes. Thus, the administrator can ask for such information from these end hosts. Depending on the AS's policy, the router may be marked as a *bad* router if information from the end hosts and itself are not matched, or the administrator may probate the router for a period of time before marking it if this incident is persist.
2) The case that the AS administrator checks specifically the router behavior by requesting a particular router its router status.
   - The administrator may routinely check on the specific routers on probation.
3) The case that one of the requested security service is indeed a request to have a check on its packet at all times.
   - The end host may contract the SSLA for the strict checking on its packets at every router.
4) The case that it is a routine for the router to report the router status to the administrator.
   - The router reports to the administrator about its status periodically. However, this may not be necessarily due to a huge overhead and can be skipped.

There are two scenarios that the requested services are denied: one with the HOME AS's router and the other with other AWAY AS's router. The end host complains to its HOME AS's administrator who will investigate and conclude (in the first scenario), or it relays the complaint to the target AWAY AS's administrator (in the second scenario). The AWAY AS's administrator requests a report from the router, verifies if the target router is acting maliciously, and returns the result to the HOME AS's administrator to conclude.

One way to detect the malicious routers and to protect the packet from any packet attacks (such as packet dropped, fabricated, deleted, modified, and impersonated) is to check a fingerprint (snapshot) of the packet. However, this will incur huge communications overhead. An alternative way is to take the snapshot of several small portions from the packet.

Let L be the packet length (in byes). It is divided into N portions, each L/N bytes. The size of each portion corresponds to the size of a block in the hash function used in X.509 public key infrastructure (PKI). Padding may be added to fill up the last portion. The router takes a snapshot of the portions at random, each tagged with the portion number. Since the whole packet is not recorded, there is a probability that the modified portion has not been captured. To fix this problem, the router must capture the portions such that they are at least "k-portions distant" away from each other. If X portions are to be captured, the communications overhead is XL/N bytes per AS, and if there are Y autonomous systems on the end-to-end path, the communications overhead is as small as XYL/N bytes.

When the router takes the snapshot of the portions of the packet, it hashes these portions along with the SQoS information and signs with its private key. In addition, the following parameters should also be recorded: time when the packet arrived at an incoming link, time when the packet is delivered onto an outgoing link. This signature is put together with the aSSV portion, and the end host stores this signature but cannot decrypt it because of the unknown public key. Depicted in Fig. 2, in the dispute case, the end host in AS1 reports this signature to the administrator. If the target router is within the same AS1, the administrator can reveal information with the router's public key because the key is known. If the target router is outside AS1, says in AS5, the AS1's administrator can retrieve that router's public key from the AS5's administrator. Although the malicious end host may also retrieve the public key from the compromised router but it cannot modify and escape the detection because it does not have the private key. Similarly, if the end host alters preference information (in the probing packet), it will be detected since preference information is encrypted with the router's private key and the malicious end host knows only the public key.

To mitigate the threats when the router fails to recognize the requested service, there is a need to investigate whether the requested service is invalid; whether it is not available at the HOME AS; or whether the requested service is available at the HOME AS's central SSP database, but the router fails to keep update its SSP database. The AWAY AS's administrator signs the request with its private key and sends via BGP message to the HOME AS's administrator. The request is decrypted with the AWAY AS's public key that can be obtained from the CA to which both HOME AS and AWAY AS are registered (based on S-BGP's PKI [6]). The HOME AS's administrator examines its central server's SSP database, signs the result with its private key, and replies to the AWAY AS's administrator. Similarly, the AWAY AS's administrator decrypts it with the HOME AS's public key obtained from the CA.

The third solution is to have the AS's administrator randomly checks its routers if they regularly update the SSP database (for all ASes) and the SSLA database (for the HOME AS). When the router sends an update request via an SNMP message to the central server, it signs the request with its private key. The request is decrypted with the router's public key by the central server. This public key can be obtained from the CA (in this case, the administrator) to which both the router and central server are registered. After checking the authentication and authorization of the router and message, the server returns only the changed, signs the result with its private key, and replies to the router. Similarly, the router decrypts it with the server's public key obtained from the CA. The router replies with a response message acknowledging the update.

The simple solution to the threat due to the replay attack is for the router to encrypt timings when the router receives the packet and when the router forwards the packet. Fortunately, the preference timeout (in the probing packet) is already required to be put into the router's signature, so the replay attack is easily mitigated. The signature is encrypted with the router's private key such that no one can modify this timeout and escape the detection from the router. If the attacker attacks with the replay of data packets, the router can compare with timings recorded and drop the replayed packet. However, the router may be vulnerable when the information recorded is overwritten. Further investigation in this possible threat might be needed.

IV. Conclusions and Future Works

We have deliberated the threats that have been recently raised for the SQoS network. Several solutions have been proposed to countermeasure these threats. Our solutions provide information assurance in various aspects: authentication, authorization, access control, integrity, and confidentiality.

However, our solutions are based upon the fact that only certificate authorities are trustworthy. Thus, a problem can be raised if there is an untrustworthy administrator because the administrator is the CA in some cases. We believe that some solutions can be introduced to mitigate the effect, but might not absolutely eliminate this threat. This paper focuses on the threats that occur in the inter-autonomous system environment. The work to detect the malicious routers in the intra-autonomous system is in progress and will be reported in the future.

References

[1] P. Sakarindr, N. Ansari, R. Rojas-Cessa, S. Papavassiliou "Security-enhanced quality of service (SQoS) networks," *IEEE Sarnoff Symposium on Advanced in Wired and Wireless Communications*, pp. 129-132, April 2005.

[2] P. Sakarindr, N. Ansari, R. Rojas-Cessa, S. Papavassiliou, "Security-enhanced quality of service (SQoS) networks: a network analysis," *IEEE Military Communications Conferenc*e, October 2005.

[3] H. Tschofenig, R. Graveman, "RFC 4230: RSVP Security Properties," retrieved from ftp://ftp.rfc-editor.org/in-notes/rfc4230.txt, December 2005.

[4] R. Zhang, J.-P. Vasseur, "RFC 4216: MPLS Inter-Autonomous System (AS) Traffic Engineering (TE) Requirements," retrieved from ftp://ftp.rfc-editor.org/in-notes/rfc4216.txt, December 2005.

[5] R. Housley, W. Polk, W. Ford, D. Solo, "RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," retrieved from ftp://ftp.rfc-editor.org/in-notes/rfc3280.txt, January 2006.

[6] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (S-BGP)," in *IEEE J. on Selected Areas in Communications,* vol. 18, no. 4, pp. 582-592, April 2000.

[7] J. Case, R. Mundy, D. Partain, B. Stewart, "RFC 3410: Introduction and Applicability Statements for Internet-Standard Management Framework," retrieved from ftp://ftp.rfc-editor.org/in-notes/rfc3410.txt, December 2005.

[8] A. T. Mizrak, Y. C. Cheng, K. Marzullo, and S. Savage, "Fatih: detecting and isolating malicious routers," *Proc. Int'l Conf. on Dependable Systems and Networks (DSN'2005),* pp. 538 – 547, July 2005.