Security-enhanced Quality of Service (SQoS)[†] Design and Architecture

P. Sakarindr, N. Ansari, R. Rojas-Cessa, and S. Papavassiliou
Advanced Network Laboratory
Department of Electrical and Computer Engineering
New Jersey Institute of Technology, Newark, NJ 07102 USA
{ps6, nirwan.ansari, rrojas, symeon.papavassiliou}@njit.edu

Abstract

The security and QoS issues have traditionally been considered separately with different objectives and implementation architectures. No protocol has been designed and implemented so far to parameterize security as QoS parameters. However, it has been noted recently that security and QoS are highly intertwined; security mechanisms may severely affect QoS mechanisms in terms of network performance and data confidentiality, and vice versa. In addition, the users are not given the choices on which security services and mechanisms as well as which security level should be applied to the user traffics. In this paper, we propose a network security framework, referred to as Security-enhanced Quality of Service (SQoS) with two major objectives. One objective is to offer the users elastic choices on the treatment of messages with appropriate security mechanisms with respect to their own QoS and budget requirements. Another objective is to facilitate interaction between security and QoS mechanisms in the most efficient manner by providing information to each other and performing tasks requested by each other.

I. Introduction

Since security and QoS systems have traditionally been considered separately with different objectives and implementation architectures, we first present several reasons why security should be integrated as a dimension of QoS, as also suggested in [1].

First, the two systems have mutually dependent performances. Security mechanisms can actually be strengthened and enhanced with information obtained by the QoS system. On the other hand, malicious activities on the network such as DoS attacks, Denial-of-QoS attacks, and the bandwidth stealth diminish the QoS performance significantly, as in [2], [3]. With a secure system, network QoS may still be guaranteed even under the attack. Furthermore, the security system can be implemented to assure users that when an attack happens to any traffic flow, QoS of remaining flows may be preserved; that is, the QoS crosstalk problem is prevented.

Second, while QoS classes are currently available from ISPs, no flexible security services have been offered in such a way that the users have more options to configure the appropriate security levels for their traffic flows.

To encounter these problems, we propose in this paper an architecture attempting to achieve two major objectives: to allow information sharing and cooperation between the security system and the QoS system, and to offer users a broad variety of security mechanisms enabled on their traffic. The major functionalities performed by Security-enhanced Quality of Service (SQoS) include various aspects of network security: confidentiality; authentication; non-repudiation; authorization and access control; QoS-associated network attack detection and prevention; integrity; accounting; and suspicious traffic quarantine.

The paper is organized as follows: section II discusses related works, and details of SQoS are deliberated in session III; session IV presents preliminary analysis of the SQoS network, followed by the conclusion.

II. Related Works

There have been quite a few research works to define security as a dimension of QoS. Ref. [4] presented a taxonomy of security services, in which users are offered various security services. A security vector was proposed to represent the level of services within the range of security services and mechanisms. The attributes of their security vector include security components, security services, level of security, and service area. The cost function was also derived in their follow up work [5].

III. SQoS Network

Since the security mechanisms generally require tremendous resources to execute the tasks, we suggest that the SQoS-based router must be upgraded with additional resources, such as dedicated-processors (CPU cycles), memories, and control and signaling bandwidth. In our SQoS architecture, each edge router will be embedded with a new security system as shown in Fig. 1. No modification is required at the core routers.

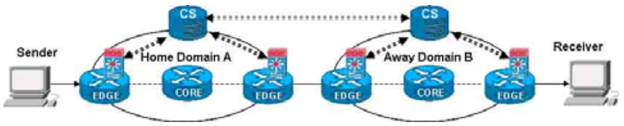


Fig. 1. The SQoS network.

The domain immediately connected to the sender is called the Home-domain and other domains along the path are referred to as the Away-domains. The home-domain provides

[†] This work has been supported in part by National Science Foundation under Grant 0435250 and the New Jersey Commission on Science and Technology via NJWINS.

the security information of the flow and negotiates with away-domains to assure that the security services chosen by the customer will be honored by all away-domains.

All security services are offered by the ISP at the edge routers; for example, six services in this paper including authentication, message integrity, authorization, message confidentiality, non-repudiation, and access control. There are many security mechanisms being loaded into the router to execute these services. For each service, all mechanisms are grouped into four service degrees (SD), represented by two bits according to the complexity of the mechanism, that is, there are four degrees for each security service as follows: default (SD=00), low (SD=01), medium (SD=10), and high (SD=11). Therefore, each service can be executed by different sets of security mechanisms, depending on how secure and how delay and cost the packet experiences at the router. The high service degree indicates that the most secure security mechanism available for that service will be executed and long delay will be expected. In addition, each router or domain has a default that may not necessarily be the same. The domain operator decides which service degree deploys which security mechanisms, according to the network policy. For instance, an edge router connected to a security-sensitive private company may be expected to configure with more secure security mechanisms as the default.

A. IP modification and SQoS Header

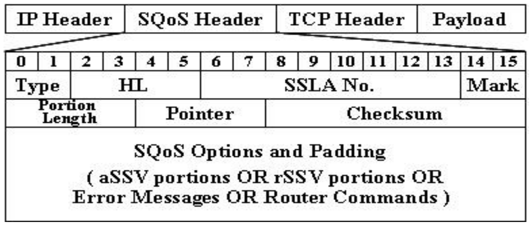
To realize the SQoS network, a modification to the TOS field of the IP header and an addition of the SQoS header are needed as shown in Fig. 2.

The reserved seventh bit in the TOS field is used as a “security bit” to indicate whether a traversing flow is SQoS-compliant. In addition, information used to classify packets is determined in the SQoS header inserted between the IP header and the TCP header. The SQoS network allows two kinds of transmissions: data transmission and router configuration process. The TYPE field specifies whether the packet is either a probing packet (00), a data packet (01), an error packet (10), or a router command (11). The first three types are packets used in the data transmission process, while the last type is the packet used for the router configuration process. The HL (Header Length) field determines the total length of the SQoS header. The SSLA No. field defines the number of Security Service Level Agreement (SSLA), which is a mutual contract between the domain ISP and the user, and will be discussed shortly in section C. The MARK field indicates the color marking and the scheduling of the packet waiting for the security service operation. The three-color marking scheme is suggested, and will be further discussed in section D. The PORTION LENGTH and POINTER fields are used to point to the position of the next SSV portions or error messages or commands.

The SQoS Option includes the requested Security Service Vector (rSSV) portion, available SSV (aSSV) portion, error message, and router command. The rSSV indicates the security service and service degree requested by the user for each domain (it is the same throughput the path for the probing packet, but may vary from domain to domain along the path for the data packet). An error message reports to the sender and the domain on any error occurred during transmission. The router command is used to modify the router configuration files.

B. Modified Explicit Endpoint Admission Control

We adopted from [6] the concepts of service vector and endpoint admission control in order to provide a domain-granular security service selection while still having the scalability advantage.


IP Header | SQoS Header | TCP Header | Payload

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Type | HL | SSLA No. | Mark

Portion Length | Pointer | Checksum

SQoS Options and Padding
(aSSV portions OR rSSV portions OR
Error Messages OR Router Commands)

Fig. 2. The modifications in IP header.

There are two communication phases taken place for data transmission: probing phase and data phase. The probing phase happens during a connection establishment and the data phase starts after the connection has been set up. During the probing phase, the sender who wants to exercise security service options sends the probing packet through all domains along the path. The probing packet verifies whether satisfied security services can be offered along with sufficient resources for the following data packets. This probing packet contains the same rSSV for every domain, which will be discussed shortly in section C. Any edge router performs the following basic tasks: verifying the sender's identity; examining the rSSV; verifying whether the sender has a privilege to request the services; checking available resources; writing down its aSSV portion; and forwarding the probing packet to the next hop. The receiver replies with an ACK packet containing all aSSV portions to the sender. The sender then evaluates all services offered and concludes whether to proceed to the data phase or to drop this connection and try again later.

During the rSSV examination, if the sender does not have the privilege to request or if any requested security service is not stored in a security service and policy (SSP) database, an error message is sent to notify the sender that the requested service is unknown or not accessible, and the probing packet is discarded. The number of error messages is counted to see if the user tends to maliciously corrupt the network. If the security service is unknown, the query is sent to the central server (CS) for downloading the missing service. The SQoS network requires the SSP database in the central server for maintaining information of both security services/mechanisms and SQoS policies. More details of the central server will be discussed in section D. The router also estimates the total processing time (T_S), in which the data packet experiences.

During evaluating information from the ACK packet, two possible conditions are examined: whether the security services are satisfied and whether the estimated T_S exceeds the delay threshold. The sender also calculates the cost for each connection. However, the cost function is beyond the scope of this paper; thus, it is not presented here. The sender may reduce the requested security services so that the requested services are satisfied with acceptable delay and cost.

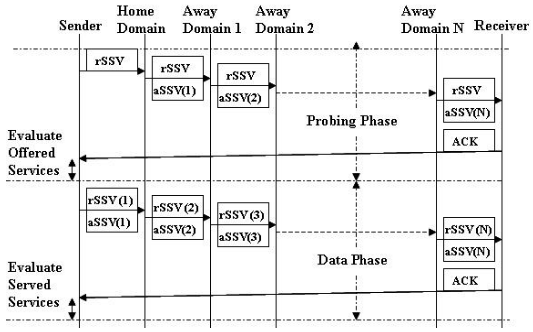


Fig. 3. The transmission diagram.

If the sender decides to proceed to the data phase, individual rSSV portions of corresponding domains are filled in the SQoS payload. The routers along the path provide the security services to the data packets, according to the associated rSSV portion, as shown in Fig. 3.

Furthermore, the security service performance is recorded by the router by replacing its rSSV portion with aSSV portion. The receiver replies the recorded aSSVs in the ACK packet so that the end-to-end security-enhanced QoS, end-to-end delay, and a total cost can be later evaluated by the sender.

C. Security Service Vector (SSV) and Security Service Level Agreement (SSLA)

The rSSV format of the probing packet is $rSSV = \{SS_x, SD_y\}$. On the other hand, the format of the aSSV portion, similar to that of the rSSV portion and the aSSV portion of the data packet, has the same format of $SSV = \{SS_x, SD_y\}_1, \ldots, \{SS_x, SD_y\}_j, \ldots, \{SS_x, SD_y\}_N$, where x is the x^{th} service, y is the y^{th} service degree, j is the j^{th} domain, and N is the number of domains along the path. All edge routers in any domain should be loaded with the same initial sets of services and mechanisms, which are not necessarily the same with other domains. The details of which security mechanisms grouped in each set may be provided in a SSLA manual. The diverse services and mechanisms yield higher flexibility to various security requirements at different domains.

The router verifies the user privilege based on SSLA. Some SSLA examples may be illustrated as follows:

Condition 1: Provide a customer host "High Authentication, Access Control, Confidentiality" services for Video Conference channels.

Condition 2: Provide a customer host "Acceptable Message Integrity and Message Confidentiality" services for HTTP traffic.

The first condition exemplifies the case that before the host holds a video conference among the executives, an executive must pass an authentication process and his identity must be in the dynamic access control list. It is ensured that an unauthorized staff cannot access to the communicating files, and even if he can somehow sneak to get them, the files are encrypted via all edge routers throughout the whole path. Furthermore, the flow authentication can be done between two domains, rather than between the original sender and the forwarding domain. The second condition shows the case that all HTTP traffics generated from the customer host will have message integrity and confidentiality services operated by a default set of mechanisms along the path.

D. Security System Architecture

Fig. 4 illustrates the architecture of the security system added into the edge routers that consists of many modules including detect/alert (D/A), pricing, policy, scheduling/marking, service engines, and loading.

During the probing phase, the scheduling/marking (S/M) module performs the following tasks: checks with the SSLA database whether the sender is legitimate to request the services; consults with the SSP database whether all requested security mechanisms have already been loaded; verifies whether they are being utilized or requested by other users; schedules all incoming traffics to wait for service operations by service engines. When the packet comes in, it is marked with either one of three resource utilization priorities (RUP), as shown in Fig. 5. There are three priority queues; high, medium, and low priority queues. The S/M module places the marked packet in the appropriate queue waiting to be served. The RUP color depends on the sender membership and an agreement between two adjacent domains.

The policy module enables the routers to check and update the SQoS policies from the domain's central server. The central server also distributes the notification to all routers if a newer policy is enforced. The cost module calculates the total cost of occupied resources and communication overhead by using either per connection-based or per packet-based cost function and records into the sender profile. During the probing phase, the pricing module estimates the total cost of data transmission such that the sender can decide if the cost is affordable. However, the cost function (C) will be reported in our future work.

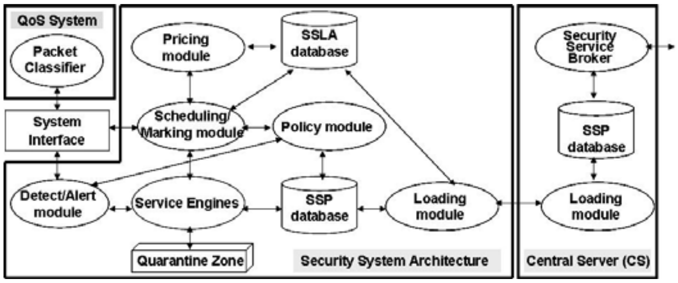


Fig. 4. The architecture of the security system.

Since the SQoS network aims to enable the security system to cooperate with the QoS system, a system interface is used to convert information between the two different systems. The D/A module is located between an interface and the service engines. If the QoS system receives suspicious activities, such as a large amount of out-of-profile traffics from one host or a very large amount of traffic destined at the same host, it issues an alert message to the D/A module. The D/A module then triggers the security service engine to execute policy-based security mechanisms, which are designed to tackle such suspicious acts. The suspicious packets can be quarantined or dropped depending on the network policy. When packets generated by the port scan protocol from one host and sent to a security-sensitive (private) server, the D/A module can request the QoS system to report the current activities of that host even it is not a SQoS-compliant flow.

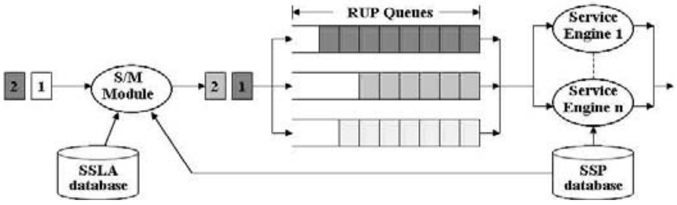


Fig. 5. An illustration of marking and queuing.

In addition to the loading module and SSP database, the central server is equipped with the security service broker, which is similar to a bandwidth broker in DiffServ networks. This broker negotiates with other domains' central servers so that the policies toward the sender's SSLA are honored by all domains along the path.

The SQoS network can include the existing QoS system with traffic conditioning components. However, this paper shows only the security point of view. Therefore, the QoS system shown in Fig. 4 has only the packet classifier component to connect with the security system.

IV. Preliminary SQoS Network Analysis

During the probing phase, the probing packet specifies the average (*M*) and longest (*L*) packet sizes of the data packets in the data payload. The router then estimates the processing time for packets of *M* and *L* bytes within T_S seconds. The processing time includes queuing time (T_Q), info-retrieving time (T_R), and operating times for *M*- and *L*-bytes packet ($T_{O|M}, T_{O|L}$) as $T_S = T_Q + T_R + T_{O|M,L}$. The queuing time is the time that the data packet waits in the queue. The priority-based weighted fair queuing in [7] and [8] is suggested to be implemented to provide fair queuing to traffics with respect to the membership class of the senders. The info-retrieving time is the average time refined for each module to retrieve information from the other modules. The average operating time is the mean time that the service engine uses to execute a specified service for a packet of M bytes. Basically, the operating time of each security mechanism for different packet sizes are measured in advance by the ISP operator.

To evaluate the services offered before proceeding to the data phase, the utility function $U\left(SSV_i\right)$, where *i* is the i^{th} router, can be used to gauge how much the requested services are available with respect to the estimated time T_S and cost C. The network security services is thus optimized with $max\left(U\left(SSV_i\right) - C\right)$, satisfying $min\, T_S$.

V. Summary

Since users have different aspects of security concerns, they should be given the choices of security services. Consequently, the ISPs can assign more accurate resources and improve the resource utilization. The SQoS network aims for two major advantages: first, a cooperation between security and QoS mechanisms to boost the network performance; second, the SQoS network aims to allow users to configure the preferred security services and service degrees for their traffics.

The SQoS network can be adopted to the service provider's networks by slightly modifying the existing QoS system and equipping the security system into all edge routers. Despite that the security system requires the resources and computational capabilities in order to execute the security mechanisms, user satisfaction on the enhanced and customized security will eventually convince the ISPs for widespread deployment.

We will analyze the expected impacts on QoS and security, explore all components of security system as well as the cost function in the future work.

References

[1] P. Bhattacharya, S. Hinrichs, K. Nahrstedt, and J. McHugh, "Security and quality of service interactions", National Information Systems Security Conference program (NISSC), Program RD2, 2000, retrieved on October 10, 2004 from http://csrc.nist.gov/nissc/program/ rd2.htm.

[2] E. Fulp, Z. Fu, D. Reeves, S. Wu, and X. Zhang, "Preventing denial of service attacks on quality of service", *Proc. of DARPA Information Survivability Conference and Exposition (DISCEXII'01),* Vol. 2, June 2001, pp:159-172

[3] A. Habib, M. Hefeeda, and B. Bhargava, "Detecting service violations and DoS attacks", *Proc. Network and Distributed System Security Symposium (NDSS '03),* pp: 177-189.

[4] C. Irvine and T. Levin, "Toward quality of security service", *Proc. of the* 2000 *New Security Paradigms Workshop*, September 2000, pp: 91-99.

[5] E. Spyropoulou, T. Levin, and C. Irvine, "Calculating costs for quality of security service", *Proc. of Annual Computer Security Applications Conference (ACSAC'00),* December 2000, pp: 334-343.

[6] J. Yang, J. Ye, S. Papavassiliou, and N. Ansari, "A flexible and distributed architecture for adaptive end-to-end QoS provisioning in next-generation networks", *IEEE Journal on Selected Areas on Communications*, Vol. 23, Issue 2, February 2005, pp: 321-333.

[7] S. Wan; Y.-C. Wang, and K.-J. Li, "A priority-based weighted fair queueing scheduler for real-time network", *IEEE Conference on Real Time Computing Systems and Applications*, RTCSA'99, December 1999, pp: 312-319.

[8] A. Kuzmanovic and E. W. Knightly, "Measurement-based characterization and classification of QoS-enhanced systems"*, IEEE Transactions on Parallel and Distributed Systems*, Vol. 14, Issue. 7, July 2003, pp: 671 – 685.