Improving the SLA-based Management of QoS for Secure Multimedia Services

Sandrine Duflos[1], Valérie C. Gay[2], Brigitte Kervella[1] and Eric Horlait[1]

[1]Laboratoire d'Informatique de Paris VI
8, Rue du capitaine Scott, 75015 Paris, France
{sandrine.duflos, brigitte.kervella, eric.horlait}@lip6.fr
[2]UTS Faculty of IT
PO Box 123, Broadway NSW 2007, Sydney, Australia
Valerie.Gay@uts.edu.au

Abstract. This paper proposes to integrate security parameters into the Service Level Specification (SLS) template proposed in the Tequila project to improve SLA-based management of QoS [8], [21]. Integrating those parameters in the QoS part of the Service Level Agreement (SLA) specification is essential in particular for secure multimedia services since the QoS is negotiated when the multimedia service is deployed. Security mechanisms need to be negotiated at deployment time when sensible multimedia information is exchanged. In this paper we show that including security parameters in the SLA specification improves the SLA-based management of QoS and therefore the negotiation, deployment and use of the secure multimedia service. The parameters this paper proposes to integrate have the advantage to be understandable by both the end-users and service providers.

1 Introduction

Today, many multimedia services are available to end-users over the Internet. They allow the exchange of more or less sensitive information needing different levels of protection. These services have generally Quality of Service (QoS) requirements according to the medias used (audio, video, text, etc.) and also security requirements depending on the type of the service used and the sensibility of the data they exchanged. For example a personal electronic multimedia medical file exchange requires a high security protection whereas multimedia e-mail or videoconference services might not have the same security requirements.

The protection during the exchange is usually achieved using security mechanisms and protocols. However, adding security to a service increases the resource consumption and the delay of the exchange, and therefore decreases the quality of the service. The Centre for Information Systems Security Studies and Research (Monterey California) published studies on these issues [9], [24].

To provide the best possible QoS for secure services, we think that security needs to be negotiated and deployed at the same time than QoS since security processing

consumes resources from both the end-user (EU) and the provider (e.g.: CPU, throughput, delay) and has therefore an impact on the QoS.

A SLA is a specific contract between a service provider (SP) and its customers [26]. It contains, on one hand, general information to identify the customer and the service to provide. On the other hand, it contains technical information to identify the required quality for those services [26], [27]. This second (technical) part corresponds to the Service Level Specification (SLS). The integration of QoS in SLS is the subject of many projects and publications [5], [10], [2], [11], [12], [20], [13]. They are presented in sections 2.1 and 2.2. The SLA specifications used or defined in these projects are not explicitly considering security. We suggest to group QoS and security together for negotiation and deployment in the SLS.

Our proposal is to extend the SLS template defined by the members of the Tequila project using parameters to express security. The selection of these parameters is discussed in one of our previous publications [4]. The parameters have the advantage of being understandable by both EUs and SPs. Integration of such parameters would allow the improvement of SLA-based management of QoS with the generation of network policies that ensure the reservation of adequate amount of resources for both the security and QoS needs. In addition, integration of security parameters within the SLS would enable SPs to propose Security of Service (SoS) to their customers. This allows customers to get the level of security they require for their services, without needing to be experts in security and without necessary having the appropriated security mechanisms available on their host.

This paper gives in Section 2 a state of the art on SLS for QoS and SoS management. Section 3 describes how to insert selected SoS parameters in an existing SLS. Section 4 presents the mapping of SLS parameters onto network policies and Section 5 gives an example of mapping. Section 6 discusses issues on the influence of security mechanisms on network and service performance to improve SLA-based management of QoS and SoS. Section 7 concludes on open issues and perspectives of this work.

2 Service Level Specifications for QoS and security management

In this section we first describe existing work on SLS for QoS management. We then present existing work on security for SLS and finally we explain our choices to integrate security parameters in SLS.

2.1 Service Level Specifications for QoS management

A lot of work deals with SLS for QoS management. We can mention various projects such as Aquila (Adaptive Resource Control for QoS Using an IP-based Layered Architecture) [5], [10], Cadenus (Creation and Deployment of End-User Services in Premium IP Networks) [2], Mescal (Management of End-to-end Quality of Service across the Internet At Large) [11], Sequin (Service Quality across Independently Managed Networks) [12] and Tequila (Traffic Engineering for Quality of Service in the Internet, at Large Scale) [20], [13].

The Aquila, Cadenus and Tequila consortia provide IP Premium services over the Internet [18]. These three projects have worked together to define an SLS template tailored to IP networks. The resulting SLS, the Tequila SLS consists of the four following units:

- The common unit, which contains general information identifying the context of the SLA (information about the provider, the customer, the service type, the time and the period of SLA applicability).
- The topology unit, which gives information on the points used by the service to access the provider domain, and the relationship of traffic generation and consumption amongst them.
- The QoS unit, which describes the traffic streams that are subject to the SLA and the nature and extent of service differentiation provided to them.
- The monitoring unit, which defines a set of parameters that need to be collected and reported to the customer in order to be compared with the SLA ones.

Each unit is also divided in sub-units that are not detailed here.

This SLS template is in the process of being standardised through the IETF. The documents containing the drafts are [25], [21], [22], [8]. Furthermore, it is used in other projects such as Sequin or Mescal. The Sequin project handles the Tequila work to provide an SLS template for the IP Premium service between National Research and Education Networks and the trans-European research backbone GEANT [23]. The Mescal project, which builds on Tequila results, uses the Tequila SLS for inter-domain interactions. It aims at negotiating the QoS between Customer and SP and between two SPs, while the Tequila project focused mainly on Customer-SP interactions [19].

2.2 Service Level Specification for SoS management

Little work has been conducted on security integration in SLS. The Arcade Project is one of the exceptions. It defines an SLS for IPsec [1], [28]. It proposes security parameters to integrate into SLS by succinctly defining a network level security SLS specific to a Linux implementation of the IPsec protocol [17]. Two categories of parameters are distinguished in this SLS: the *SLA-dependent* and the *SLA-independent* parameters. The *SLA-dependent parameters* are inherent to the SLA. The *SLA-independent* gather the parameters that can be reused in others SLAs, where a similar service is required. They consist of parameters that are used in the IPsec security association. Their objective is to map the SLS onto the IETF/DMTF IPsec Configuration Policy Information Model [14]. This SLS does not consider QoS.

2.3 Our choices to integrate security in SLS

Of the studied projects none is considering both quality and security of service. The SLS defined in the Tequila project represents a complete specification for the IP service and is becoming a standard. However it is specific to QoS management and does not include security parameters despite the impact of security processing on the quality of the service. This SLS is a good base to add security parameters.

3 Extension of the Tequila SLS template with security parameters

This section describes how we integrate the SoS parameters identified in [4] in the Tequila SLS template to improve the QoS management of secure services.

These parameters have the advantage of being interpretable by both EU and SPs. Two abstraction levels are therefore available: one abstract level that can be qualified, understandable by non expert EU and a precise level that can be quantified, interpretable by the expert EU and its SP to negotiate the service configuration and deployment. The identified qualitative parameters correspond to the common security services (confidentiality, authentication, integrity and non-repudiation) plus optional parameters derived from security protocols (security protocol, tunnelling and no-replay). To each qualitative parameter corresponds a set of quantitative values.

Supplying SoS is a quality guarantee for secure multimedia services. It is essential to consider security as a parameter to provide a good quality to the service. Also, security processing acts on the quality of the service. It increases resource consumption, induced delay and traffic load. Considering security as a QoS functionality makes it easier to take into account the impact of security on the QoS. It is also a logical placeholder since security and QoS are applied to the same traffic. Also, as the traffic is already described in the traffic descriptor sub-unit of QoS unit it avoids the useless repetition of the traffic description. This sub-unit contains combination of DiffServ Information, Source information, Destination Information and Application Information [8]. The Source, Destination and Application Information is necessary for security protocol configuration [17],[3].

To introduce SoS parameters in the SLS, we choose to add a new sub-unit to the QoS unit of the Tequila SLS template, the SoS parameters sub-unit, rather than adding a specific security unit. This sub-unit contains the common parameters plus the selected security protocol and the protocol options described in [4].

Fig. 1 presents the extension of the Tequila SLS QoS unit for security with quantitative guarantees. Only the two sub-units useful for SoS management are shown. The other QoS sub-units are outside the scope of this paper. The additional parameters are in bold. The first column presents the sub-unit. The second and third columns correspond respectively to the qualitative and associated quantitative parameters, and the fourth contains examples of associated selected values.

The negotiated values associated to the SoS parameters can be either qualitative or quantitative depending on the EU expertise. In the first case, a level, an on/off choice or a default value can be attributed to the parameters. In the second case, a subset of specific parameters is associated to the common ones except for the non-repudiation parameter which is ‘on or off’ depending on the type of authentication algorithm. Therefore, if non-repudiation is selected, the authentication algorithm must be a digital signature.

Sub-Unit	Qualitative Parameters	Quantitative Parameters		Value
Traffic descriptor	Diffserv Information	DSCP		11101
	Source Information	Address	Type	IPV4 Address
			Value	190.20.1.1
	Destination Information	Address	Type	IPV4 Address
			Value	200.20.1.1
	Application Information	Protocol number		6
		Source port		1566
		Destination port		1566
SoS parameters	**Security protocol**	**Value**		ESP (or 50)
	Confidentiality	**Alg Name**		DES
		Alg Category		Block
		Alg Mode		CBC
		Alg Block size		64 bits
		Alg Key length		56 bits
		Alg round number		16
	Authentication	**Alg Type**		MAC
		Alg Name		HMAC
		Alg Key length		128 bits
	Integrity	**Hash function**		MD5
	Non-repudiation	**Value**		Off
	Tunnelling	**Source address**	**Type**	IPV4 Address
			Value	190.20.1.0
		Destination address	**Type**	IPV4 Address
			Value	200.20.1.1
	No-replay	**Sequence Number length**		32 bits

Fig. 1. In **bold:** proposed SoS parameters structure and example of quantitative SoS parameters

During the negotiation, it is possible not to select any of the security parameters or to use only part of it. For example, the required SoS can be confidentiality only. In this case, the common and optional parameters that are not selected can be qualitatively specified with the 'no', 'on' or 'off' value, or not specified at all. In the case where optional parameters are not specified, the options default values are attributed according to the security protocol selected.

In case quantitative values are attributed, as presented in Fig. 1, the SP can directly consider the SLS to configure security. However, in case of qualitative agreements, the SP must interpret the values. This interpretation is done through mapping tables such as Table 1, where a level corresponds to a set of algorithms to choose from. This choice is also possible with quantitative guarantees. Several alternatives can be associated to a particular SoS parameter.

Table 1. Example of a mapping table for confidentiality

Level	Name	Category	Mode	Block size	Key length	Round number	Security Protocol
High	AES	Block	CBC	128	128	9	ESP, TLS
	3DES	Block	CBC	64	192	48	ESP, TLS
	IDEA	Block	CBC	64	128	8	ESP, TLS
Medium	RC5	Block	CBC	64	128	16	ESP
	Blowfish	Block	CBC	64	128	16	ESP
Default	DES	Block	CBC	64	56	16	ESP, TLS
	RC2	Block	EBC	64	64	18	TLS
	DES	Block	EBC	64	56	16	TLS
No	NULL						

The SLS we propose is negotiated between a EU and its SP. The negotiated values are either qualitative or quantitative depending on the EU expertise. The quantitative parameters are derived from the SLS or obtained from the mapping tables that represent the SoS that can be provided by the SP. These parameters are used by the SP to configure its network. To do this, the SP must be able to translate the SLS into policies. These policies are then used to configure the SP network to provide the required security.

4 From SLS to Policies

The policies on which we map the SLS are described in a previous paper [7]. These policies are organised in a three levels hierarchy (service level, network level and element level policies). A service level policy is translated into a network level policy, which is also translated into several element level policies that are sent to the network elements where they are enforced.

Only SLS quantitative parameters are considered and mapped onto policies. The qualitative parameters must be previously translated in quantitative parameters through the mapping tables.

Therefore, the quantitative SLS is translated into the network level and then element level policies, as described in Table 2 and Table 3, where:

- **<*Sec-Prot*>** corresponds to the security protocol used (AH, ESP, TLS)
- **<*C-Algo parameters*>** represents the different confidentiality quantitative parameters. Several algorithms can be specified. In this case, the algorithm list is specified in braces. E.g.: {(AES, block, CBC, 128, 128, 9), (IDEA, block, CBC, 64, 128, 8), (3DES, block, 64, 192, 48)}. The NULL algorithm can be directly specified if confidentiality is not required.
- **<*A-I-Algo parameters*>** represents the different authentication and integrity quantitative parameters. The SLS non-repudiation parameter is not specified in the policy. It depends on the digital signature use as authentication algorithm and it is not necessary in the policy to configure network. As for confidentiality, several algorithms can be specified. Each list of parameters is described in brackets and the list of algorithms in braces. The NULL algorithm can also be directly specified if authentication and integrity not required.
- **<*Tunnelling parameters*>** corresponds to the type of the addresses and the IP source and destination addresses of the tunnel.
- **<*Seq-Number Length*>** refers to the sequence number length specified in the SLS.

Table 2. Network level policy

IF SourceIPaddress|UserIPaddresses = <SourceIPaddress|UserIPaddresses1..*> and SourcePortNo|UserportNo = <SourcePortNo|UserportNo> and DestinationIPAddress = DestinationIPAddress..(optional)> and DestinationPortNo = <DestinationPortNo (optional)> THEN CONNECT with <QoSDirection> and <ConnectionType> from|among <SourceIPAddress!..*> at <SourcePortNo|UserPortNo> to <destinationIPAddress!..*(optional)> at DestinationPortNo1 (optional)> with <PhBtype> and **<Sec-Prot>** with **<C-Algo parameters>** and **<A-I-Algo parameters>** and **<Tunnelling parameters>** and **<Seq-Number Length>**

Table 3. Network level policy for dissemination to the network elements

IF SourceIPaddress|UserIPaddresses = <SourceIPaddress|UserIPaddresses1..*> and SourcePortNo|UserportNo = <SourcePortNo|UserportNo> and DestinationIPAddress = DestinationIPAddress..(optional)> and DestinationPortNo = <DestinationPortNo (optional)> THEN SET at <InterfaceIPaddress> with <PhBtype> and <**Sec-Prot**> with **<C-Algo parameters>** and **<A-I-Algo parameters>** and **<Tunnelling parameters>** and **<Seq-Number Length>**

The element policy parameter <*InterfaceIPAddress*> represents the nodes where the policy must be enforced, i.e. the nodes crossed by the traffic for which the SLA is negotiated. This parameter can be directly deduced from the 'Topology unit' of the SLS, since this unit describes the SP domain access nodes.

5 SLS to policy mapping example

In this section we are only interested in the SoS parameters mapping from SLS to policy. Consider a End-User (EU) who wishes to secure its video-conferencing service. S/he expresses her/his requirements in qualitative terms and requires a security with a medium confidentiality and a high integrity/authentication. Therefore, the non-repudiation parameter receives the 'off' value and the protocol options (tunnelling and no-replay) will receive their default value. As for security protocol parameter, it will be derived from the result of the qualitative to quantitative parameters mapping. The obtained security SLS is depicted in Fig. 2.

QoS Unit		
SoS parameters	**Security protocol**	*not defined yet*
	Confidentiality	Medium
	Authentication	High
	Integrity	High
	Non-repudiation	*Off*
	Tunnelling	*Off*
	No-replay	*On*

Fig. 2. The EU negotiated security SLS with qualitative guarantees

These qualitative parameters must be derived into quantitative ones to be interpreted to configure and manage the SP network. The mapping tables described in Tables 4 and Table 5 are used. The grey lines represent the quantitative values associated to the specified qualitative ones.

These two tables are used to identify the algorithms associated to the negotiated security level. As for the column named 'Security protocol', it identifies the protocol that uses the algorithm.

We end up with the following alternatives. On one hand, the 'medium' level of confidentiality can be provided by the RC5 or Blowfish algorithms with ESP protocol. On the other hand, the 'high' importance of authentication/integrity can be provided by HMAC associated with the hash functions SHA-1 or RIPEMD-160, by using the AH, ESP or TLS protocols. The ESP protocol is therefore the only possibility since it is the only one proposing a 'medium' level of confidentiality.

Table 4. Example of a mapping table for confidentiality

Level	Name	Categ	Mode	Block size	Key length	Key rounds	Security protocol
High	AES	Block	CBC	128	128	9	ESP, TLS
	3DES	Block	CBC	64	192	48	ESP, TLS
	IDEA	Block	CBC	64	128	8	ESP, TLS
Medium	RC5	Block	CBC	64	128	16	ESP
	Blowfish	Block	CBC	64	128	16	ESP
Default	DES	Block	CBC	64	56	16	ESP, TLS
	RC2	Block	CBC	64	40	18	TLS
	DES	Block	CBC	64	40	16	TLS
No	NULL						

Table 5. Example of a mapping table for authentication, integrity and non-repudiation

Level	N-R Value	Auth Type	Auth Name	Auth key length	Hash function	Security Protocol
High	off	MAC	HMAC	128	SHA-1	AH, ESP, TLS
	off	MAC	HMAC	128	RIPEMD_160	AH, ESP
Medium	off	MAC	HMAC	128	MD5	AH, ESP, TLS
Default	off	MAC	HMAC	128	MD5	AH, ESP, TLS
No	off		NULL		NULL	

The network level policy will be created from the new data. The policy conflict verification and resolution will need to be done but its description is out of the scope of this paper. This policy is then derived in two element level policies. The Tables 6 and 7 present these policies where the negotiated security parameters are in bold. In these Tables, the sequence number length is set to '32'. It corresponds to the IPsec default value of this parameter [4].

Table 6. Network level policy derived from the SLS parameters

IF UserIPaddress = *1.1.1.1, 2.2.2.2* and UserPortNo = *8000*
THEN CONNECT with *bi-directional* and *unicast* among *1.1.1.1, 2.2.2.2* at *8000* with *AF11*
and ***ESP*** with ***{(RC5, block, CBC, 64, 128, 16), (Blowfish, block, CBC, 64, 128, 16)}***
and ***{(HMAC, 128, SHA-1), (HMAC, 128, RIPEMD_160)}*** and ***off*** and ***32***

Table 7. Element level policies derived from the SLS parameters

IF SourceIPaddress = *1.1.1.1* and SourcePortNo = *8000* and DestinationIPAddress = *2.2.2.2* and DestinationPortNo=*8000* THEN SET at *1.1.1.0* with *AF11*
and ***ESP*** with ***{(RC5, block, CBC, 64, 128, 16), (Blowfish, block, CBC, 64, 128, 16)}***
and ***{(HMAC, 128, SHA-1), (HMAC, 128, RIPEMD_160)}*** and ***off*** and ***32***

IF SourceIPaddress = *2.2.2.2* and SourcePortNo = *8000* and DestinationIPAddress = *1.1.1.1* and DestinationPortNo=*8000* THEN SET at *2.2.2.0* with *AF11*
and ***ESP*** with ***{(RC5, block, CBC, 64, 128, 16), (Blowfish, block, CBC, 64, 128, 16)}***
and ***{(HMAC, 128, SHA-1), (HMAC, 128, RIPEMD_160)}*** and ***off*** and ***32***

The first policy in Table 7 is enforced by the network node 1.1.1.0 managing the IP address 1.1.1.1. The second policy is enforced at the network node 2.2.2.0 managing the IP address 2.2.2.2. These policies will secure the videoconferencing traffic between the IP addresses 1.1.1.1 and 2.2.2.2.
The network nodes where the policies are enforced can be edge routers of the SPs domains or device modems provided by SPs to the EUs. Those device modems are

integrating security mechanisms and allow the SPs to provide end to end SoS to their customers. Fig 3. illustrates where SLSs can take place.

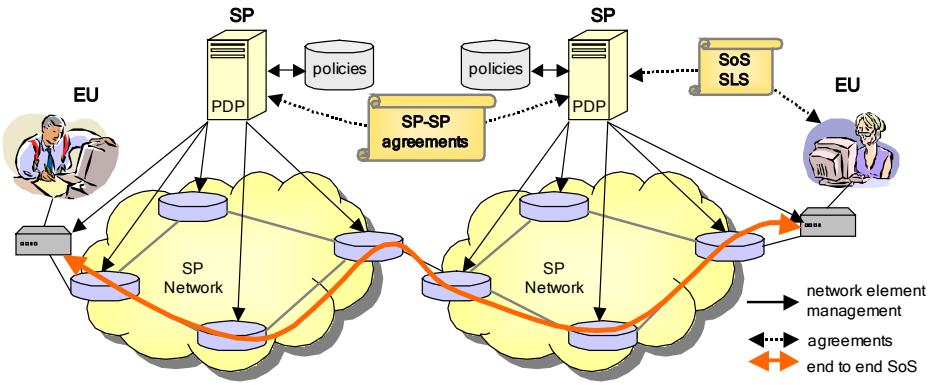

Fig. 3. End to end SoS with SLS enforcement

The mapping tables and policies presented in this section offer a choice among several SoS solutions, each having a different impact on the QoS.

6 Security influence on network and service performance

This section discusses the influence of security on network and service performance (in the context of our SLS for QoS and SoS). In our previous paper [4], we discussed how each SoS parameter affects the performance. The resources we studied are CPU, memory and bandwidth. For each resource two types of costs are distinguished: initialisation and streaming costs. The initialisation represents the initialisation phase of the security mechanism process (including the negotiation), and the streaming represents the data packet emission. In [4] we consider the resources (CPU, memory and bandwidth) and their associated costs with each SoS parameter specified in our SLS. We determine how each SoS parameter influences the different resources and therefore the importance of the impact. The figure 4 summarises this study with a down/top classification of resource consumption for our SoS parameters.

Fig. 4 (a) and (b) show the initialisation and streaming costs for CPU and memory. These resources are considered together since their consumption has the same origin. During the initialisation, CPU and memory costs are due to the initialisation of the no-replay sequence number and of the authentication and confidentiality algorithms. During the streaming phase the sequence number incrementation and checking, the creation of a new (tunnel) header for each packet and the processes of authentication/integrity and confidentiality algorithms consume also these two resources. Fig. 4 (c) presents the bandwidth costs while streaming. Our classification depends on the amount of data transferred for each specific SoS parameter. For example, the sequence number exchanged to ensure the no-replay is a 32 bits value, whereas the size of the added header for tunnelling is at least 20 or 40 bytes for

respectively IPv4 and IPv6, or more, the size of data when padding is added to enciphered data can reach 255 bytes. The initialisation bandwidth cost is not shown here. Only the protocol has an impact on it for its security context establishment (key generation, negotiation of used algorithms, etc.).

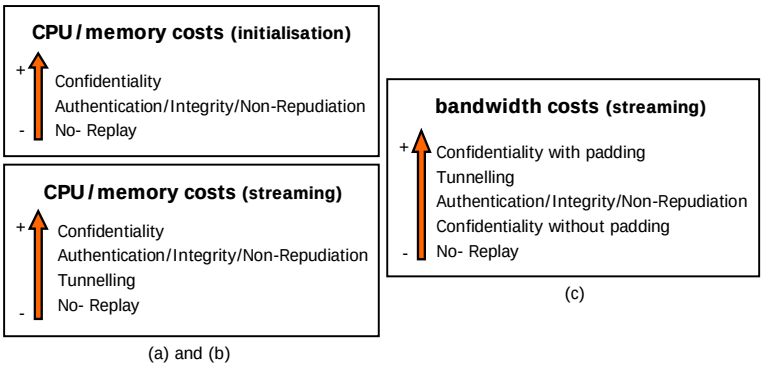

Fig. 4. Classification of SoS parameters resource consumption

To determine the precise impact of the choice of the protocol on the bandwidth, we did run some tests that applied the IPsec protocols for different levels of security. We used the Ethereal tool [6], a network protocol analyser, to value bandwidth costs for a MPEG video and a DVD sequence. The multimedia sequences are read with VLC (Video LAN Client) on a laptop from a desktop running on Windows OS and are secured with the Windows OS IPsec Policy Tool. The data are exchanged over a LAN.

The Windows IPsec Policy Tool provides confidentiality using 3DES or DES algorithms. The SHA-1 and MD5 algorithms associated with HMAC are available for authentication and integrity services. To measure the bandwidth costs, we did test two times for both multimedia sequences (MPEG and DVD) with all possible combinations of security protocols and algorithms (i.e. AH with SHA-1, AH with MD5, ESP with SHA-1, ESP with MD5, ESP with 3DES, ESP with DES, ESP with SHA-1 and 3DES, ESP with SHA-1 and DES, ESP with MD5 and 3DES and ESP with MD5 and DES). We can notice that the quality of the multimedia sequence, the level of confidentiality and the level of authentication and integrity do not have an impact on the bandwidth costs. Only the choices of the security services and of the protocol do have an impact.

Table 8. Bandwidth costs for UDP and IPsec protocols

Protocol		**Bandwidth cost during the initialisation (bytes)**	**Bandwidth cost while Streaming (bytes/packet)**
UDP		*not relevant*	1358
AH	Authentication and integrity	1688	1382
ESP	Authentication and integrity	1712	1382
	Confidentiality	1712	1378
	Confidentiality, authentication and integrity	1712	1390

The table 8 depicts the increase bandwidth costs before and after the inclusion of security. The bandwidth cost during the initialisation phase is expressed in bytes because it consists in the security context establishment (key generation, negotiation of used algorithms, etc.) and the number of exchanged packets is limited (10 for IPsec). While streaming, it is expressed in bytes per packets because it corresponds to the protocol processing, which depends on the multimedia file. Table 8 shows that the bandwidth initialisation cost depends only on the protocol. ESP consumes more resources than AH. During the streaming phase the bandwidth consumption varies according to the chosen security services apart from the protocol. Confidentiality consumes less bandwidth than authentication and integrity, which consume fewer resources than confidentiality, authentication and integrity. This confirms our classification in Fig. 4 (c).

We are now extending our tests to the other resources (CPU and memory), and for each SoS parameter.

7 Conclusion and future work

This paper has proposed a solution to improve the SLA based management of QoS for secure distributed multimedia services. It used the Tequila project SLS definition as a basis and extends it with SoS parameters.

We identified the essential SoS parameter to integrate in the QoS part of an SLS. It consists of a set of network specific parameters useful for network security protocols configuration and to evaluate the impact on resource consumption and consequently on the QoS. We also highlighted the necessity for EUs to provide higher-level parameters to the SLS in order to express their SoS requirements in terms they do understand. Then, we described the mapping of SLS parameters on policies and give an example of this mapping. Finally we discussed the influence of security on the performance of services and networks. It is essential to consider it to improve the QoS management. Our SoS quantitative parameters are useful to evaluate this influence.

Including security parameters in the SLS allows SPs to propose end to end SoS to their customers. The SLS can be used by the modem devices provided by SPs to EUs. These devices can integrate security mechanisms that can be dynamically configured by the SP.

We are currently continuing our tests on the other resources consumptions for each SoS parameter. The objective is to determine and add parameters that are representative of the resource consumption into mapping tables. It can be useful to choose the most suitable algorithm and security protocol. It will improve the QoS management by adapting and optimising the resource consumption for security.

References

1. Arcade Project Home Page: http://www-rp.lip6.fr/arcade/ [last accessed on 1st Aug. 2005]
2. Cortese, G. et al: Cadenus: creation and deployment of end-user services in premium IP networks. IEEE Communications Magazine, Jan. 2003, pp 54-60.

3. Dierks, T. and E. Rescorla: The TLS Protocol Version 1.1. IETF Internet Draft, May 2005. <draft-ietf-tls-rfc2246-bis-11.txt>
4. Duflos, S., et al: Integration of Security Parameters in Service Level Specification to Improve QoS Management of Secure Distributed Multimedia Services. In Proc. of IEEE INA'05 Workshop, Taipei, IEEE Press, March 2005.
5. Engel, T., et al: AQUILA: adaptive resource control for QoS using an IP-based layered architecture. IEEE Communications Magazine, Jan. 2003, pp 46-53.
6. Ethereal home page: http://www.ethereal.com [last accessed on 1st Aug. 2005]
7. Gay, V. et al: Policy-Based Quality of Service and Security Management for Multimedia Services on IP networks in the RTIPA Project. In Proc. of IEEE MMNS'02, Santa Barbara, LNCS Springer-Verlag, Oct. 2002.
8. Goderis D., et al.: Attributes of a Service Level Specification (SLS) Template. Internet Draft, Oct. 2003. <draft-tequila-sls-03.txt>
9. Irvine, C., et al: Security as a Dimension of Quality of Security Service. In Proc. of the Active Middleware Services Workshop, San Francisco, CA, Aug. 2001, pp 87-93.
10. IST Aquila Project Home Page: http://www-st.inf.tu-dresden.de/aquila/ [last accessed on 1st Aug. 2005]
11. IST Mescal Project Home Page: http://www.mescal.org [last accessed on 1st Aug. 2005]
12. IST Sequin Project Home Page: http://archive.dante.net/sequin/ [last accessed on 1st Aug. 2005]
13. IST Tequila Project Home Page: http://www.ist-tequila.org [last accessed on 1st Aug. 2005]
14. Jason, J., et. al: IPsec Configuration Policy Information Model. RFC 3585, Aug. 2003.
15. Kent S.: IP Authentication Header. IETF Internet Draft, Mar. 2005. <draft-ietf-ipsec-rfc2402bis-11.txt>
16. Kent S.: IP Encapsulating Security Payload (ESP). IETF Internet Draft, Mar. 2005. <draft-ietf-ipsec-esp-v3-10.txt>
17. Kent, S., Atkinson, R.: Security Architecture for the Internet Protocol. RFC 2401, Nov. 1998.
18. Koch, B. et al: IST Premium IP Cluster. IST deliverable, Mar. 2003.
19. Morand, P. et al: Initial Specification of Protocols and Algorithms for Inter-domain SLS management and Traffic Engineering for QoS-based IP Service Delivery and their Test Requirements. Deliverable D1.2, IST Mescal Project, Nov. 2003.
20. Mykoniati, E. et al: Admission control for providing QoS in DiffServ IP networks: the TEQUILA approach. IEEE Communications Magazine, Jan. 2003, pp 38-44.
21. Rajan, R., et al: Service Level Specification for Inter-domain QoS Negotiation. Internet Draft, Nov. 2000. < draft-somefolks-sls-00.txt >
22. Salsano, S. et al: Definition and usage of SLSs in the AQUILA consortium. Internet Draft, Nov. 2000. <draft-salsano-aquila-sls-00.txt>
23. Sevasti, A., Campanella, M.: Service Level Agreements specification for IP Premium Service. Deliverable D2.1 - Addendum 2, IST Sequin Project, Oct. 2001.
24. Spyropoulou, E., et al: Managing Costs and Variability of Security Services. IEEE Symposium on Security and Privacy, Oakland, California, May 2001.
25. T'Joens, Y. et. al.: Service Level Specification and Usage Framework. Internet Draft, Oct. 2000. <draft-manyfolks-sls-framework-00.txt>
26. Verma, D.: Service Level Agreements on IP Networks. Proc. of the IEEE, vol 92, no. 9, Sept. 2004.
27. Westerinen, A. et al: Terminology for Policy-Based Management. RFC 3198, Nov. 2001.
28. Yilmaz, V. et al: Gestion et déploiement de services de sécurité dans un réseau basé sur des politiques (In English: Management and Deployment of Security Services over a Policy-based Network). SAR 2003 Conference, Nancy, France, June 2003.