CRYPTOGRAPHIC MODELING IN SERVICE LEVEL AGREEMENT

Ahmad, Suleiman

Department of Cyber Security Science,

School of Information and Communication Technology

Federal University of Technology, Minna, Nigeria

ahmads@futminna.edu.ng

Abstract

Supporting business services through Electronic Service Delivery System (ESDS) as part of service-oriented architectures (SOA) involves business performance monitoring requirements, and their implementation results in developmental activities. A model-driven approach to the development of monitored of a well secured E-Messaging which focus on supporting the specification and transformation of information to an executable implementation in a secured order was designed.

Key words: E- Messaging, Cryptography, SOA, ESDS, PANDA, SBS, SLA

1. Introduction

Over the last few years, several approaches have been developed to support the monitoring of SLAs. Such approaches provide state of the art mechanisms for performing the basic checks of service compliance with SLAs but fall short of providing adequate support when replacements of the services deployed in a service based system (SBS) occur at runtime when SLA providers are directly involve with their clients. A SLA consumer for instance, might not be able to provide the runtime events required for monitoring some of the terms in an SLA. Also, after changes in the deployment infrastructure and composition of an existing service, it might no longer be possible to provide the events and monitors for checking the established SLAs for the service.

With the advancement in E-Messaging media, automation of the negotiation process has gained much attention[1]. With the advent of Service Oriented Computing (SOC), researchers have turned their focus to negotiations for e-Services. A negotiation server for e-commerce was proposed by [2], to perform bargaining-type negotiations automatically. Each negotiating party registers with a negotiation server and provide their goals, contexts, requirements and

priorities, and the servers then conduct negotiation automatically using constraint satisfaction, rule-based conflict resolution, and event [3]. A policy-based negotiation broker framework was proporsed by [3] similar to the NB to perform partially or fully automated negotiation of QoS parameters for service selection. However, the negotiating parties need to have knowledge about the strategy models supported by the framework to mention their choice of strategy and parameters in the policy specifications. [4] propose a scheme for negotiation of e-services under uncertainty using existing records of similar negotiations. In their scheme, a participant who is negotiating in uncertainty obtains assistance in the form of negotiation alternatives and offers made, from other reputable participants who have negotiated the same issue. [5] proposes Policy-Driven Automated Negotiation Decision-making Approach (PANDA), where a policy expresses a party's private negotiation strategy as a combination of rules and utility functions. In their approach, the decision making problem is decomposed into multiple aspects. Each aspect is handled by a separate Decision Maker (DM) framework, which interact with each other to jointly provide a solution. These steps are decomposing a user-defined process level utility function of overall preferences into lower level negotiation preferences for service selection; selecting a set of candidate services from a larger set of potential service providers, and finally negotiating with the set of candidate services to select the service that yields the highest utility value to meet the end-to-end process. The process repeats with an adjusted requirement set if no service can be selected. The approach uses regression analysis [6] for learning opponent's behavior and makes concessions accordingly to maximize its own utility.

Recent history in the telecommunications arena has shown us that just about anyone with sufficient financial means and relatively little expertise can build a network, bring in customers, and in most cases technically deliver a product or service to market. Nevertheless, as many companies have learned, products must be more than just technically deliverable to be successful [7].

It is not enough to have in placed the technical means, personnel, processes, and supporting infrastructure to accomplish operational tasks such as ordering, provisioning, network management, and billing [8].

From a business standpoint, it is a reasonable assumption that product delivery at or exceeding a reasonable and achievable volume will positively impact the bottom line. The key to whether or not a product can be considered deliverable most likely lies in the ability of the service provider to realistically optimize all the costs associated with the delivery of the product or service. The combined costs related to the technical means, personnel, and other infrastructure elements must be recoverable through the sale of the product at the defined level of volume [9].

2. Related work

2.1 Design and Implementation of Service Level Agreements at HEAnet

In [10] a propose Strategic Objective to monitor service levels in order to achieve excellence were outlined; setting up a benchmark operational performance on an ongoing basis; identify an appropriate set of operational benchmarks and service metrics to measure performance for clients.

In conclusion the HEAnet case study indicates that implementation of Service Level Agreements

towards the NREN's connected clients and/or towards their sponsoring/funding bodies can be implemented on both existing and new services, and can match and exceed those levels offered by the commercial sector.

3. Methodology

We propose a cryptographic approach of a SLA document based electronic plain text messaging, which introduces a SLA Executor that serves as an intermediary between SLA Provider and Consumer; this will ensure that a consumer gets a contract satisfaction under a well secured e-message platform. This SLA based project ensures a defined protocol (policy model) encrypted by the SLA provider, decrypted by the consumer via a well defined monitor base policy(SLA Executor) which ensures that consumers received the actual project under contract agreement section.

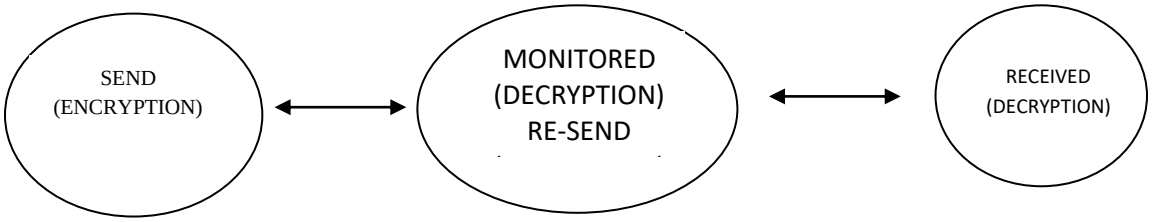
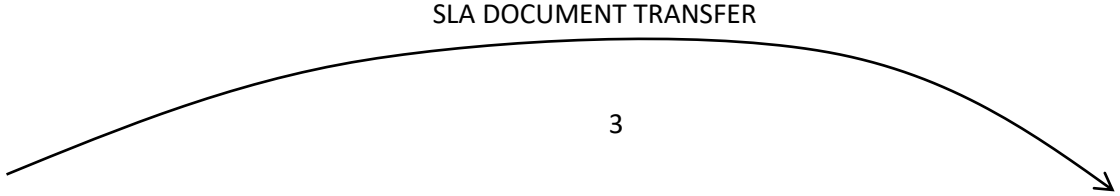


Figure 3.1 A Platform for SLA plain text document transfer



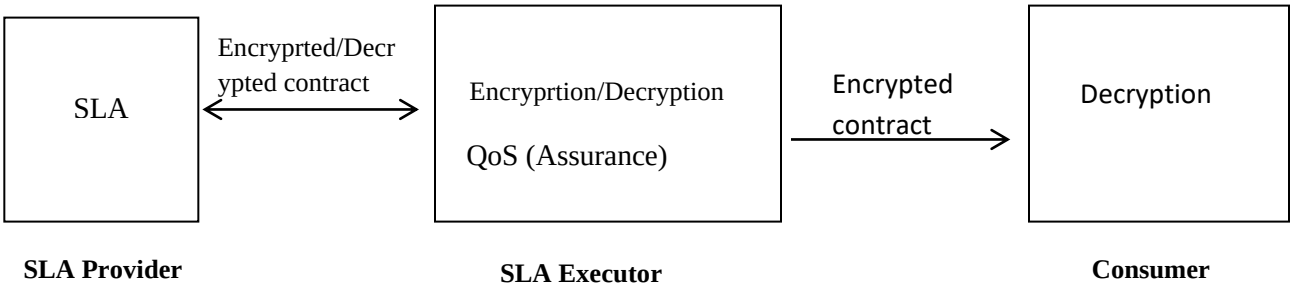


Figure 3.2 DSS – Through a unified protocol

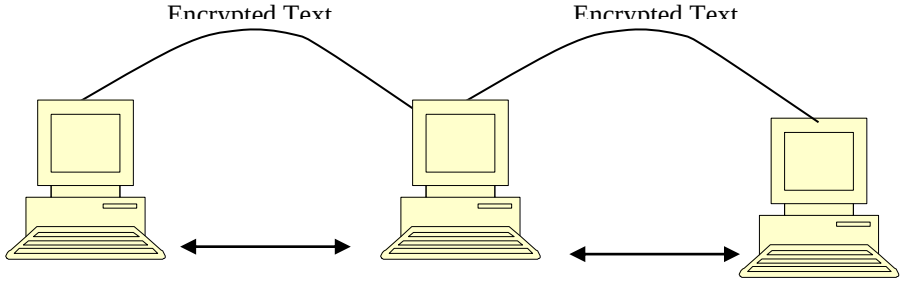


Figure 3.3 Connection mode

When a pair of users encipher the data they exchange over a network, the cryptographic transformation they use must be specific to the users. A cryptographic system is a family $\mathcal{T} = \{T_k : k \in \mathcal{K}\}$ of cryptographic transformations. A key k is an identifier specifying a transformation T_k in the family $\mathcal{T}$. The key space $\mathcal{K}$ is the totality of all key values. In some way the sender and receiver agree on a particular *k* and encipher their data with the enciphering transformation T_k. T_k is an algorithm whose input consists of plaintext $\underline{x}$ and key *k* and with ciphertext $\underline{y}$ as output.

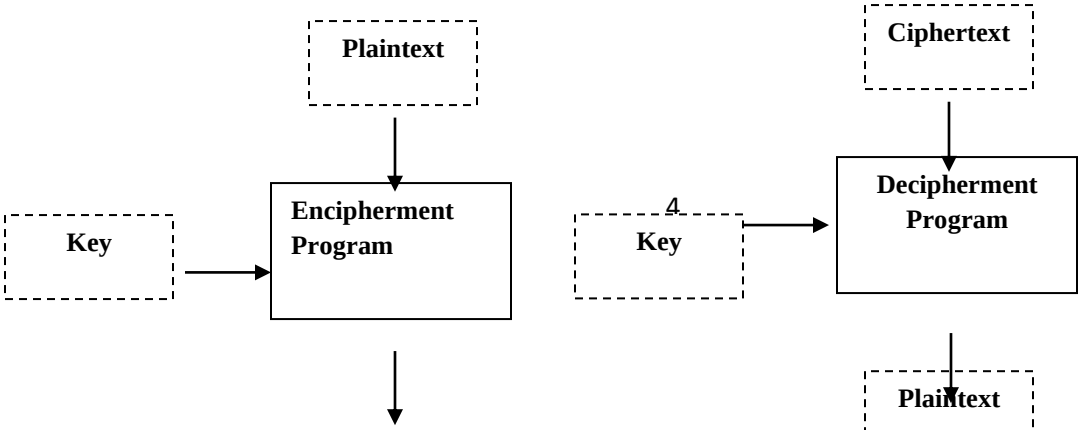


Figure 3.4 The software encipherment/decipherment processes

Proposition 3.1 (Boolean distribution ensemble)
Let ε be a public – key encryption scheme and let A be any ITM and let $\mathrm{RIND}_{\varepsilon,A}^{cpa,b}(k,z)$ *denote the random variable describing the output of the game in Fig*.3.6, *when the random bits used by A and the random b bits gen and enc are chosen uniformly at random. This defines a Boolean distribution ensemble* $\mathrm{RIND}_{\varepsilon,A}^{cpa,b}=\{\mathrm{RIND}_{\varepsilon,A}^{cpa,b}(k,z)\}_{k\in N,z\in\{0,1\}^*}$. *If ε is IND – CPA secure, then* $\mathrm{RIND}_{\varepsilon,A}^{cpa,0}\approx\mathrm{RIND}_{\varepsilon,A}^{cpa,1}$ *for all PPT A*

Formulation. Assume that we are given an adversary *A* for the repeated IND-CPA game. For $k \in$ N, $z \in \{0,1\}^*$ and $b \in \{0,1\}$, let $P^b(k, z) = \Pr[\mathrm{RIND}_{\varepsilon,A}^{cpa,b}(k,z)=1]$ and let $Q(k, z) = |P^0(k, z)-$

$P^1(k, z)|$. By the definition of repeated IND-CPA security it is enough to show that *Q* is

negligible. To formulate our model we construct an adversary *B*(*A*) for the IND-CPA game. Since *A* is PPT and has a running time k^c. This means that it makes at most k^c generate-requests and at most k^c test-messages-requests. The adversary *B*(*A*) runs in $\mathrm{IND}_{\varepsilon,B(A)}^{cpa,b}(k,z)$. Initially it is given (*k, z, e*). Then it generates two uniformly random integers *r, s* 2 Z_{kc} and runs a variant of the repeated IND-CPA game as follows:

1. Input (*k, z*) to *A*.

2. Let *R* = 0 and let *S* = 0.

3. Run *A* to receive an output *v* and proceed as follows:

(a) If *v* = (generate), then define a key e_R as follows:

• If $R \neq r$, then run $(e', d') \leftarrow gen(k)$ and let $e_R = e'$.

• If *R* = *r*, then let $e_R = e$, where *e* is the key initially received by *B*(*A*) from

$$\mathrm{IND}_{\varepsilon,B(A)}^{cpa,b}(k,z)$$

Store e_R, give e_R to *A* and let $R \leftarrow R + 1$.

(b) If *v* = (test-messages, e_ρ, m_0, m_1), where e_ρ has been stored and $m_0, m_1 \in M_{e\rho}$

then a ciphertext *c* is defined as follows:

• If $\rho < r$, then compute *c* = *enc*(e_ρ ,*m*1).

• If ρ = *r*, then

– If *S* < *s*, then compute *c* = *enc*(e_ρ ,*m*1).

– If *S* = *s*, then output (test-messages,*m*0,*m*1) to the game $\mathrm{IND}^{cpa,b}_{\varepsilon,B(A)}(k,z)$

and receive c' = *enc*(*e*,*mb*) = *enc*(e_ρ ,*mb*). Then let *c* = c' .

If *S* > *s*, then compute *c* = *enc*(e_ρ ,*m*0).

• If ρ > *r*, then compute *c* = *enc*(e_ρ ,*m*0).

(c) If *v* = (guess, *d*), then output (guess, *d*) and halt.

For $b \in \{0,1\}, let\ p^b(k,z) = Pr[\mathrm{IND}^{cpa,b}_{\varepsilon,\mathrm{B(A)}}(k,z)=1] \text{ and let } q(k,z) = \left| p^0(k,z) - \mathrm{p}^1(k,z) \right|.$

By the IND-CPA security of ε we have that *q* is negligible. We relate *q*(*k,z*) to *Q*(*k,z*). For $r,s \in Z_{k^c}$ and $b \in \{0,1\}$, we let $p^{r,s,b}(k,z) = Pr[\mathrm{IND}^{cpa,b}_{\varepsilon,\mathrm{B(A)}}(k,z)=1]$ when B(A) is using the fixed values r and s. It is straight forward to write that $p^{r,s,1}(k,z) = p^{r,s+1,0}(k,z)$ for $r \in k^c - 1 \text{and } s \in k^c - 2$. This gives us that;

$$p^{r,0,0}(k,z) - p^{\mathrm{r},\mathrm{k}^c-1,1}(k,z) = \left(\sum_{s=0}^{k^c-2} (p^{r,s,0}(k,z) - p^{r,s+1,0}(k,z)) + p^{r,k^c-1,0}(k,z) \right) - p^{r,k^c-1,1}$$

=

$$\sum_{s=0}^{k^c-2} (p^{r,s,0}(k,z) - p^{r,s,1}(k,z)) + \left(p^{r,k^c-1,0}(k,z) - p^{r,k^c-1,1}(k,z) \right) = \sum_{s=0}^{k^c-1} (p^{r,s,0}(k,z) - p^{r,s,1}(k,z))$$

$$= \sum_{s=0}^{k^c-1} (p^{r,s,0}(k,z) - p^{r,s,1}(k,z))$$

$p^{r,k^c-1,1}(k,z) = p^{r+1,0,0}(k,z)$.

This gives us that;

$$p^{0,0,0}(k,z) - p^{k^c-1,k^c 1,1}(k,z) = \left(\sum_{r=0}^{k^c-2} (p^{r,0,0}(k,z) - p^{r+1,0}(k,z)) + p^{k^c-1,0,0}(k,z) \right)$$
$$- p^{k^c-1,k^c-1,1}(k,z)$$

$$= \sum_{r=0}^{k^c-2} \left(p^{r,0,0}(k,z) - p^{r,k^c-1,1}(k,z) \right)$$
$$+ \left(p^{k^c-1,0,0}(k,z) - p^{k^c-1,k^c-1,1}(k,z) \right)$$

$$= \sum_{r=0}^{k^c-1} \left(p^{r,0,0}(k,z) - p^{r,k^c-1,1}(k,z) \right) \qquad (3.2)$$

$$= \sum_{r=0}^{k^c-1} \sum_{s=0}^{k^c-1} \left(p^{r,s,0}(k,z) - p^{r,s,1}(k,z) \right)$$

$$= \sum_{r=0,s=0}^{k^c-1,k^c-1} p^{r,s,0}(k,z) - \sum_{r=0,s=0}^{k^c-1,k^c-1} \left(p^{r,s,1}(k,z) \right)$$

$$= k^{2c} (p^0(k,z) - p^1(k,z))$$

If *r* and *s* are uniformly chosen from Z_{k^c} in such a way that $p^b(k,z) = k^{-2c} \sum_{r=0,s=0}^{k^c-1,k^c-1} p^{r,s,b}(k,z)$,

for $b \in \{0,1\}$. We observe that $P^0(k,z) = p^{0,0,0}(k,z)$ *and* $P^1(k,z) = p^{k^c-1,k^c-1,1}(k,z)$.

By Eq.(3.1), this gives us that $Q(k,z) = k^{2c} q(k,z)$.

From the fore going it is apparent to note that, designing a well secured e-message encryption key delivery is necessary to ensure that contract documents get to consumers under a well secured interface and with a high level of security.

4. Experimental Result

A monitored e- base approach is used which ensures that services be provided to customers under well-defined conditions (model) by specifying and agreeing to a Service Level Agreement (SLA) between the provider and the customer of a service under which a service should be delivered to a specific customer (or group of customers), monitored at runtime to ensure that the service provision fulfils it. Typically, this approach collects events during service executions and uses them to check whether the properties of service provision as specified in an SLA are satisfied through the service of SLA Executor.

4. Conclusion

A monitored - based approach was used which ensure that services be provided to customers under well-defined conditions by specifying and agreeing to a Service Level Agreement (SLA) between the provider and the customer of a service under which a service should be delivered to a specific customer (or group of customers), monitored at runtime to ensure that the service provision fulfils it. This approach introduce a SLA Executor Interface that collects events during service executions and use them to check whether the properties of service provision as specified in an SLA are satisfied.

From the existing literature, we realized that the consumer's requirements are only considered at the later stages (i.e during negotiation) of the SLA life cycle, at which stage the parties need to indulge in intense negotiations before an agreement can be reached. The degree of customization in SLA templates offered by service providers is limited. Consumers find it difficult to express their individual QoS preferences that allow them to realize classical SLA creation phase.

We, therefore, proposed a consumer-initiated SLA Executor framework that factors in the consumers request to select the most appropriate SLA template for that consumer through SLA Executor. The SLA Executor- initiated approach to SLA template selection is more appropriate in delivering flexible creation of SLAs and promotes increased consumer satisfaction as compared to the provider initiated approaches.

REFFERENCES

1. Anderson R. (2004). *Sun Microsystems Laboratories*. *An Introduction to the Web Services*

2. Cappiello C.(2007). *On Automated Generation of Web Service Level Agreements. Proc. of IEEE Int. Conf. on Advanced Information Systems Engineering (CAISE)*, Trondheim, Norway, pp. 264-278.

3. Chen R. (2002). *Architecture of an agent-based negotiation mechanism. In Proc. of Int. Conf. on Distributed Computing Systems Workshops*, Vienna, Austria, pp. 379-384.

4. Yee, and Korba, (2003*). Bilateral E-Services Negotiation under Uncertainty. In Proc. of the Intl, Symposium on Applications and the Internet (SAINT '03)*, Orlando, Florida, and National Research Council Canada.

5. Gimpel Z. (2003). *Specifying Policies for Automated Negotiations of Service Contracts. In Proc. of Int. Conf. on Service Oriented Computing (ICSOC'03)*, Trento, Italy. Orlowska, LNCS 2910, pp. 287–302, Springer.

6. Hou, C., (2004). *Predicting agents' tactics in automated negotiation. In Proc. of IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'04), Beijing, China, pp.127- 133.*

7. Su, E. (2001). *An Internet-based Negotiation Server for ECommerce, VLDB Journal*, Vol. 10(1), pp. 72-90.

8. Williams and Sawyer (2001). *Using Information Technology*. New York: McGraw Hill Inc., 3-5, 27-29.

9. Wireless Local Area Networks (2007) http://www.broadbandinfo.com

10. *Ann* Harding(2004). *Design and Implementation of Service Level Agreements at HEAnet*. *Ann*http://www.heanet.ie/about/HEAnet_Strategic_Plan_2004.pdf