Eleventh Int. Conf. on IFSs, Sofia, 28-30 April 2007
NIFS 13 (2007), 2, 48-53

Generalized Net model of SSL with intuitionistic fuzzy estimations

Ivelina Vardeva, Sotir Sotirov
"Prof. Asen Zlatarov" University, Bourgas-8000, Bulgaria,
e-mail: iveto@btu.bg, ssotirov@btu.bg

Abstract

At the article is examined one of the possibilities for security of data in TCP/IP based networks – the usage of SSL protocol.

It is developed generalized net model reflecting the work of building and transmitting confidential information between a client and server by cryptic tunnel. For better understanding we use intuitionistic fuzzy estimations.

Key words: Cryptography, Generalized net, Intuitionistic fuzzy set, SSL

Introduction

The fast entering of the computer communications and Internet in different spheres sets a multitude of questions bounded with the security in exchanging information. This is very important in transmitting confidential information by the network [8]. The investigation and analyzing of the processes bounded with the change of that kind information is exceptionally important and it could be a base for increasing the security of its transmitting.

At the article is introduced a model describing the processes of transmitting confidential information. About its development are used Generalized nets (GN, see [1]). They have powerful apparatus for modeling and analyzing such parallel flowing in time real processes.

The developed GN-model at the current article could be used independently or like additional module to others GN-models introducing the work of systems in which are transmit confidential data (example [10, 11, 12]), describing different processes in Internet of a university, [5] – GN-model of electronic payments. Computer networks are modeling with GN in [13, 14, 15].

One of the possibilities used for data security in TCP/IP based networks is the use of SSL protocol [2, 3, 4, 6, 7, 9]. It is based on cryptography with public keys. Some versions of SSL exist and they used 40/56/128/168 bit keys for crypt. In SSL the public key is called certificate. For realization of SSL are necessary a personal key and certificate.

The personal key is owned from the both parties – from the client and server. Each part owns two keys – one public and one private.

The server owns: server certificate, certificate for certificating authority (allowing to be done crypt of information) and the client certificate (it is received during the exchange of information with the client), Cipher Spec. The server certificate is used for attesting and generating keys for crypt of the session. Cipher Spec contains parameters for cipher and MAC address. The client owns: the client certificate (it is used for attesting the client), certificate from the certificating authority, ciphering algorithm, Cipher Spec. The certificate from the certificating authority of the client is used for verifying of server certifications assigned from this certificating authority but it do not contains the key of the certificating authority. The certificate of the certificating authority is used for verifying others certificates assigned from it (it do not participate in the transactions of SSL and do not contains a key of the certificate).

Work of SSL

The remote host (client) sets an inquiring to the server for realization of the crypt relation by sending its certificate. If the client certificate is authentic, the server backs its own certificate to contract the keys and crypt the session.

Every crypt session has dot a life finishing when the server send its serial message to the client that its serial data are received and are not received new data from the client of the server.

GN-model

All definitions related to the concept "GN" are taken from [1]. The GN, describing the work of the SSL, is shown on Fig.1.

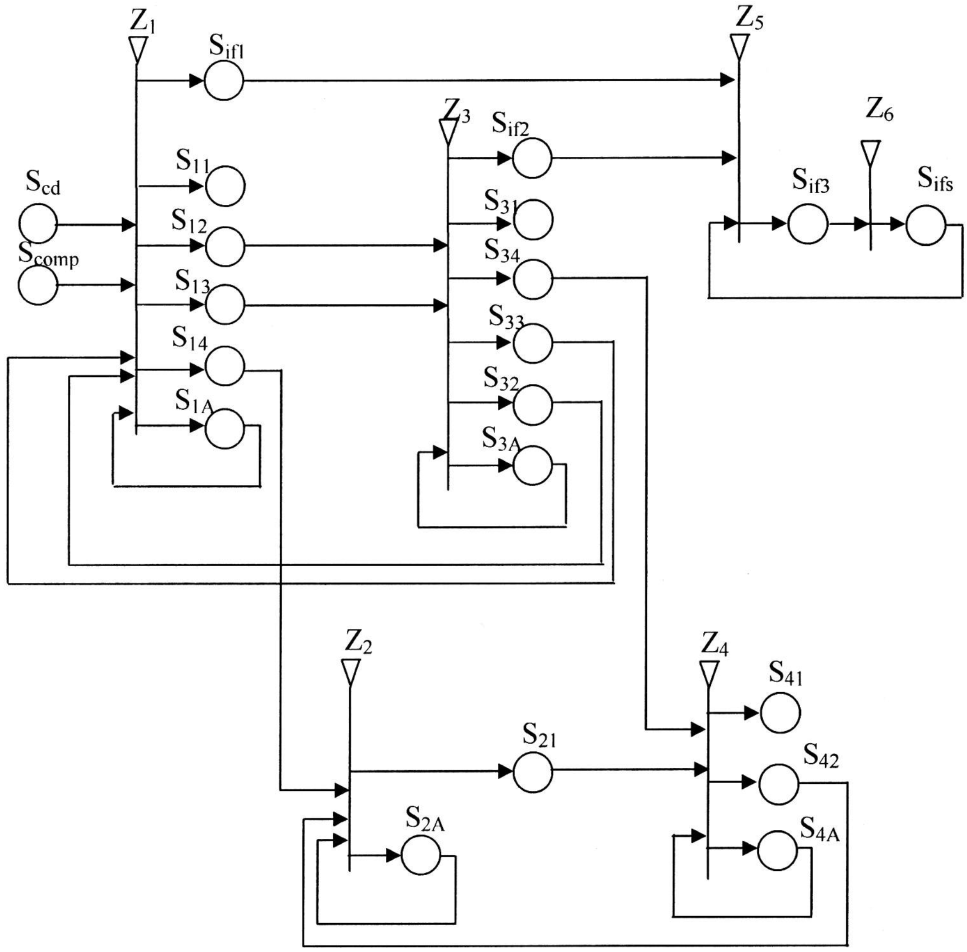

Fig. 1

Initially the α_{serv}-token stays in place S_{3A} with characteristic:

$x_0^{\alpha_{serv}}$ = "server certificate; certificate of the certificating authority; cipher spec".

It will be in its own place during the whole time which the GN functions. While it may split into two or more tokens, the original token will remain in its own place the whole time. The new tokens will be noted by $\alpha'_{serv}, \alpha''_{serv}$ and so on.

Initially the following tokens enter in the generalized net:

- in place S_{comp} - α_{cl}-token with characteristic:

$x_0^{\alpha_{cl}}$ = "client certificate, client key, certificate from the certificating authority, ciphering algorithm, client Cipher Spec";

- in place S_{cd} - β-token with characteristic:

x_0^{β} = "data for sending in secured channel".

Generalized net is presented by a set of transitions, where transitions describe the following processes:

Z_1 – sending information from the client;
Z_2 – sending information from the client in the crypt channel;
Z_3 – crypting and sending information from the server;
Z_4 – crypting and sending information from the server in the crypt channel.

$$Z_1 = < \{S_{cd}, S_{comp}, S_{32}, S_{33}, S_{1A}\}, \{S_{11}, S_{12}, S_{13}, S_{14}, S_{1A}\}, R_1, \vee(\wedge(S_{cd}, S_{comp}), S_{32}, S_{33}, S_{1A})>$$

$R_1 =$

	S_{11}	S_{12}	S_{13}	S_{14}	S_{1A}	S_{if1}
S_{cd}	*False*	*False*	*False*	*False*	*True*	*False*
S_{comp}	*False*	*False*	*False*	*False*	*True*	*False*
S_{32}	*False*	*False*	*False*	*False*	*True*	*False*
S_{33}	*False*	*False*	*False*	*False*	*True*	*False*
S_{1A}	$W_{1A,11}$	$W_{1A,12}$	$W_{1A,13}$	$W_{1A,14}$	*True*	$W_{1A,14}$

where

$W_{1A,11}$= "it is impossible to be realized the connection";
$W_{1A,12}$ = ""there is a request for version of SSL, cipher algorithm";
$W_{1A,13}$ = "it is confirmed the certificate of the client version of SSL and the cipher algorithm";
$W_{1A,14}$ = "Data exchange can start".

The α_{cl}- and β-tokens entering in place S_{1A} (from places S_{cd} and S_{comp}) not obtain new characteristics. All tokens that will enter transition Z_1 will unite with original α_{cl}- token.
The tokens that enter places S_{11}, S_{12}, S_{13} and S_{if1} obtain characteristic respectively:

"not realized connection",
"version of SSL, ciphering",
"client certificate, client key, client Cipher Spec",
and $x_{cu}^{\theta_1} = "\langle Data\_CRC_T, Ack\_CRC_T \rangle"$.

The every transaction have CRC (Cyclic Redundancy Check) – received and transmitted. The Data_CRC$_T$ is for transmitted data, and Ack_CRC$_T$ is for acknowledgment.

α_{cl}- and β-tokens entering in place S_{14} (from place S_{1A}) merge in γ-token with characteristic:

$$x_{cu}^{\gamma} = "x_{cu}^{\alpha_{cl}}, x_0^{\beta}".$$

This is the whole necessary information for realizing of SSL tunnel and data for sending.

$$Z_2 = < \{ S_{14}, S_{42}, S_{2A}\}, \{S_{21}, S_{2A} \}, R_2, \vee (S_{14}, S_{42}) >$$

$R_2 =$

	S_{21}	S_{2A}
S_{14}	*False*	*True*
S_{42}	*False*	*True*
S_{2A}	*True*	*True*

The γ-token that enter place S_{2A} (from place S_{14}) not obtain new characteristics.
The β'-token that enters place S_{21} obtain characteristic

$x_{cu}^{\beta'}$ = "a current packet of crypt information".

$$Z_3 = < \{ S_{12}, S_{13}, S_{3A}\}, \{S_{31}, S_{32}, S_{33}, S_{3A}\}, R_3, \vee (S_{12}, S_{13}, S_{3A}) >$$

$R_3 =$

	S_{31}	S_{32}	S_{33}	S_{34}	S_{3A}	S_{if2}
S_{12}	*False*	*False*	*False*	*False*	*True*	*False*
S_{13}	*False*	*False*	*False*	*False*	*True*	*False*
S_{3A}	$W_{3A,31}$	$W_{3A,32}$	$W_{3A,33}$	$W_{3A,34}$	*True*	$W_{3A,34}$

$W_{3A,31}$ = "it is impossible to be realized the connection";
$W_{3A,32}$ = "it is confirmed the certificate of the client version of SSL and the cipher algorithm";
$W_{3A,33} = W_{3A,34}$ = "Data exchange can start".
The tokens that enter places S_{31}, S_{32}, S_{33} and S_{34} obtain characteristic respectively:
"unrealized connection with the client",
"certificate for the client, SSL version, ciphering algorithm",
"cipher spec"
and "certificate for the client, SSL version, ciphering algorithm, cipher spec".
Token that enter place S_{if2} obtain characteristic:

$$x_{cu}^{\theta_2} = "\langle Ack\_CRC_R, Data\_CRC_R \rangle" ;$$

The Data_CRC$_R$ is for received data, and Ack_CRC$_R$ is for acknowledgment.

$$Z_4 = < \{ S_{34}, S_{21}, S_{4A}\}, \{S_{41}, S_{42}, S_{4A}\}, R_4, \vee (S_{34}, S_{21}, S_{4A}) >$$

$R_4 =$

	S_{41}	S_{42}	S_{4A}
S_{34}	*False*	*False*	*True*
S_{21}	*False*	*False*	*True*
S_{4A}	$W_{4A,41}$	$W_{4A,42}$	*True*

where:
$W_{4A,41}$="there is an information by the crypt channel";
$W_{4A,42}$="there is a query for the next packet information".
The β'-token that enter places S_{4A} obtains characteristic:

$$x_{cu}^{\beta''} = x_{cu-1}^{\beta''} \cup x_{cu}^{\beta'}.$$

The tokens that enter places S_{41} and S_{42} obtain characteristic respectively:

"received information by the crypt channel",

and "query for the next packet information".

We must note that the input place priorities must satisfy the following inequality:

$$\pi_L(S_{34}) > \pi_L(S_{21}) > \pi_L(S_{4A}).$$

Initially, token θ has initial characteristic "<0 ,0>".

$$Z_5 = <\{S_{if1}, S_{if2}, S_{ifs}\}, \{S_{if3}\}, R_5, \wedge(S_{if1}, S_{if2}, S_{ifs})>$$

where:

$R_5=$

	S_{if3}
S_{if1}	*True*
S_{if2}	*True*
S_{ifs}	*True*

.

The three tokens θ_1, θ_2 and θ that enter place S_{if3} unite in token θ that obtains characteristic

$$x_{cu}^{\theta} = \text{“}\left(\frac{s}{k};\frac{r}{k}\right)\text{”},$$

where:

- s is the number of coincidence packages;
- r is the number of non-coincidence packages;
- k is the number of all packages that are transmitted;
- k-s-r is the number of packages that are sent, but not received.

$$Z_6 = <\{S_{if3}\}, \{S_{ifc}\}, R_6, \vee(S_{if3})>$$

where:

$R_6=$

	S_{ifs}
S_{if3}	*True*

Token θ enters place S_{ifs} and obtains as (k+1)-th characteristic (for $k \geq 0$)

$$\text{“} < \mu_{k+1}, \nu_{k+1} > \text{”},$$

where

$$< \mu_{k+1}, \nu_{k+1} > = < \frac{\mu_k k + m}{k+1}, \frac{\nu_k k + n}{k+1} >.$$

It is estimated on the base of the previous sets from the formula mentioned above. Where $<\mu_k, \nu_k>$ is the previous evaluation, and $<m,n>$ is the estimation of the latest message, for m, n $\in$ [0, 1] and $m + n \leq 1$. The final estimation of the correctness of the information exchanged on the basis of the previous and the latest events

Conclusion

At the article is developed a model describing the work of SSL. The model can be used independently or like a component of others GN-models of different systems in which are transmitting confidential data.

The developed model can help examination, analyzing and optimizing the flowing processes in exchanging such data in Internet/Intranet.

References

1. Atanassov, K., Generalized nets, World Scientific, Singapore, New Jersey, London 1991
2. Bauer M., Security servers under Linux, O'Reilly, 2002
3. Jon Mountjoy, WebLogicThe Definitive Guide, O'Reilly, 2004
4. Kerry Plowright The Internet Business Resource Kit, http://www.awp.com.au/internet_business_guide.pdf
5. Kodoyannis V., S. Sotirov, A. Nenov, Modeling of electronic payment by generalized net, Concurrent engineering " The Vision for the future in Research and Application, Portugal , 2003, ISBN 90 5809 622 X, 1043-1046
6. Michael D. Bauer, Building Secure Servers with Linux, O'Reilly
7. Microsoft Internet Security and Acceleration server 2000, Redmont, Microsoft Press, 2001
8. Nenov A., S.Sotirov, "Protocols and standards in Internet payment" - International conference "Computer systems and technology" - KompSysTech'2000" in "Union of automatics and programming" , Sofia, Bulgaria
9. Professional programming: Java E-Commerce, Soft press
10. Shannon A., D. Langova-Orozova, E. Sotirova, I. Petrounias, K. Atanassov, M.Krawczak, P. Melo-Pinto, S. Mellani, T. Kim, Generalized net model of intranet in an abstract university, Advanced Studies in Contemporary Mathematics, 7 (2004), No 1, pp. 81-88
11. Shannon A., D. Langova-Orozova, E. Sotirova, I. Petrounias, K. Atanassov, P. Melo-Pinto and T. Kim, Generalized net model of information flows in intranet in an abstract university, Advanced Studies in Contemporary Mathematics, 8 (2004), No 2, pp. 183-192
12. Shannon A., D. Langova-Orozova, E. Sotirova, K. Atanassov, P. Melo-Pinto, T. Kim, Generalized Net Model of the University Electronic Archive, 15th International Conference of the Jangjeon Mathematical Society, S. Korea, August 5-7, 2004, pp. 88-92
13. Stoyanov P., Implementation of Generalized Nets for studying of a space switch for ATM computer networks "Electronics and Electrotehnics" – Vol. 5-6 / 2005, 41-47, (in Bulgarian).
14. Stoyanov P., G. Naydenov - Implementation of Generalized Nets for studying of conditional correct space switch for computer networks – Third International Scientific Conference Computer science, 12-15 October, 2006, Istambul, Turkey, Proceedings, 148-151.
15. Stoyanov P., G. Naydenov, Modelling of space switch and investigation of inside locks in real network traffic. Dolna Mitropolia, 21-22 April 2005, 22-32, (in Bulgarian).