Construction of Network Security Architecture Based on Formal Specification in Digital Campus

Xiaole Li
Experimental teaching center, Guangxi University of Finance and Economics, Nanning, China
Email: leowing9@163.com

Ming Weng
Experimental teaching center, Guangxi University of Finance and Economics, Nanning, China
Email: 22582989@qq.com

Ying Wen
China Mobile Group Guangxi Company Limited, Nanning, China
Email: 47900047@qq.com

***Abstract*—With comprehensive analysis on security requirements of information transmission in digital campus, new primitives in asymmetric and symmetric cryptographic system are designed to describe essential security attributes. Secure information transmission is constructed with composition of the generated primitives and realized with common security technologies. And then, formal analysis shows that, secrecy, integrity, availability, controllability, non-repudiation and identifiability during information transmission can be insured by this architecture. At last, the network security architecture is verified by experiment based on Hadoop, with comparison data on the attacked rate in cloud environment.**

***Index Terms*—information transmission, composition, formal specification, network security architecture, cloud computing**

I. Introduction

Based on campus network, digital campus achieves the digitization of environment, resource, and activities, using the means of advanced informatization, with the purpose of building efficient, multifunctional process of education [1]. But as the spread of cloud computing, the security of digital campus is faced to more and more threats during information transmission, such as data forging, juggling or wiretapping. When the campus network is safe, digital campus can be equipped with various kinds of application systems. So it is important to construct a rational, active and systemic architecture for network security, satisfying secrecy, integrity, availability, controllability, non-repudiation and identifiability of information sender [2, 3]. It's the major problem how to realize date protecting, access control, and identify verification[4, 5, 6].

There are some researches in network security architecture during information transmission in cloud computing: a security transmission mode for Internet of Things is supported with trusted computing technology by Zhenqiang Wu [7]; based on the architecture and implementation of IacaaS, a security infrastructure of cloud computing is presented [8]; with consideration of confidentiality, authentication, integrity and non-repudiation in commercial environment, a secure data transmission model is researched and some useful expansion with both software and hardware is given [9]; with analysis on the cloud computing security threats under the comprehensive consideration of various factors, a cloud computing security architecture reference model is presented, including six modules for security transmission system [10]. There are some researches in security for digital campus [11], but cloud computing security framework is still insufficient [12].

In this paper, with a comprehensive analysis on security requirements of information transmission in digital campus, new primitives in asymmetric and symmetric cryptographic system are designed to describe essential security attributes, and a formal specification is given with composition method [13]. Based on this, a network security architecture is constructed, realized with common security technologies, such as firewall, access control, virtual private network (VPN for short), intrusion detection system (IDS for short), encryption and decryption, following principles of integrity, consistence, balance, operability, and multiple protections. And then, formal analysis shows that, secrecy, integrity, availability, controllability, non-repudiation and identifiability during information transmission can be insured by this architecture, as a common framework for development of various application systems in digital campus from the

Manuscript received August 3, 2013; revised September 3, 2013; accepted September 9, 2013.
Corresponding author: Xiaole Li
Email address: leowing9@163.com.
This research is supported by the Research Project on Science and Technology in Guangxi Colleges (No. 2013YB215).

doi:10.4304/jsw.9.4.952-957

viewpoint of information security. At last, the network security architecture is verified by experiment based on Hadoop, with comparison data on the attacked rate in cloud environment.

II. Security Requirements Of Information Transmission In Digital Campus

Construction of digital campus is related to many fields about universities, such as digital library, educational administration system, scientific research administration system, and management system, as shown in Fig. 1. These are important parts of whole management system in school, supplying information service of network resource, visited by users through the entrance of unified identity authentication.

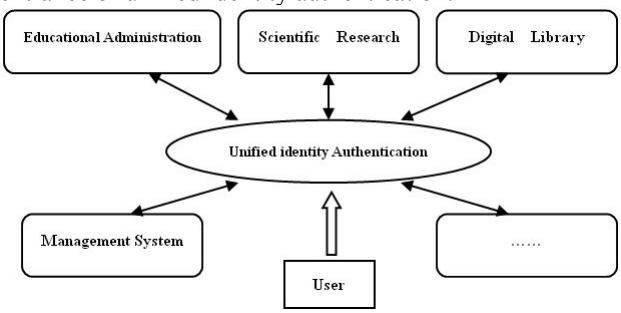


Fig. 1. The model for various application systems in digital campus.

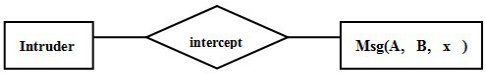
For intruder in the network environment, Dolev and Yao built the model as follows [14]:

(1) The intruder may obtain messages passing through the network.

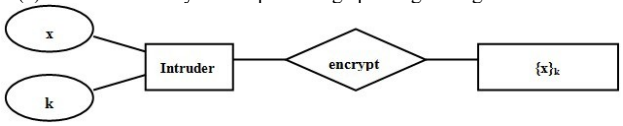
(2) The intruder is a legitimate user of the network, and can initiate a conversation with any other user.

(3) The intruder has the opportunity to be a receiver to any user.

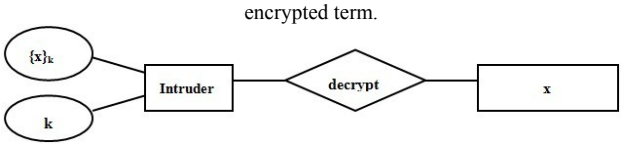
As a result, intrusion behaviors in digital campus can be described as follows:



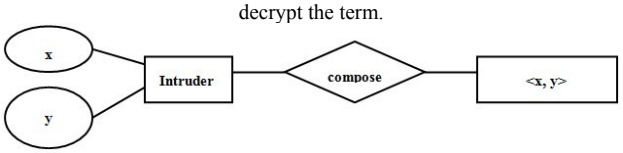
(a) The intruder may intercept message passing through the network.



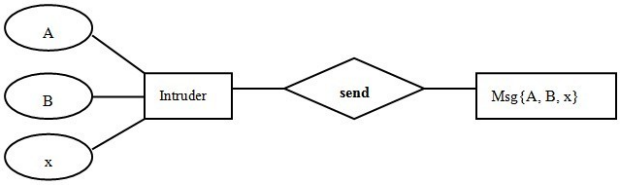
(b) The intruder owning certain term *x* and key *k* may generate an encrypted term.



(c) The intruder owning certain encrypted term $\{x\}_k$ and key *k* may decrypt the term.



(d) The intruder may compose different terms.



(e) The intruder may pretend to be a legitimate participant sending message.

Fig .2. 3. The model for intrusion behaviors in digital campus.

In order to avoid illegal stealing, altering or destroying of important information during transmission, the following security requirements should be satisfied:

- Secrecy-Important information, such as user name, password, and records about teaching, scientific research, or finance, should be encrypted during transmission.
- Integrity –Important information should be ensured from being altered, or perceived if altered.
- Availability-Important information should be available for unauthorized users.
- Controllability-Transmission process should be monitored and managed, avoiding illegal use.
- Non-repudiation-One party in a dispute cannot repudiate, or refute the validity of a statement or contract. The server must have unforgettable proof for the request of user; on the other hand, the user must have unforgettable proof for the information sent by server. All the proof for non-repudiation can only be used once.
- Identifiability of senders-The receiver could distinguish whether the information is sent by correct sender with effective measures.

III. Formal Specification On Network Security Architecture

Based on the security requirements, an information transmission model is built from the viewpoint of information security. According to Fig. 1, the formal specification can be divided into two parts: mutual authentication in asymmetric key cryptosystem, and distribution of secrets by the server in symmetric key cryptosystem.

A. Mutual Authentication in Asymmetric Key Cryptosystem

The goal of information transmission security protocol in asymmetric key cryptosystem (ITA for short), is to ensure the mutual authentication between *C* and *S*.

APG [15] is used to generate two protocol primitives used in mutual authentication:

P_1:

P_C->P_S:NONCE_C | New(NONCE_C);

P_S->P_C:E{C[NONCE_C,NONCE_S],PRIVKEY_P_S} | New(NONCE_S);

P_C->P_S:E{NONCE_S,PRIVKEY_P_C};

P_2:

P_S->P_C:NONCE_S | New(NONCE_S);

P_C->P_S:E{C[NONCE_S,NONCE_C],PRIVKEY_P_C} | New(NONCE_C);

P_S->P_C:E{NONCE_C,PRIVKEY_P_S};

It is assumed that the server is honest and competent. There are two participants: user C and server S. In asymmetric key cryptosystem, the ek_C and ek_S are the public key of C and S respectively; sk_C and sk_S are the private key of C and S respectively; in the $\beta_C=\beta_S=(C, S)$, β_C and β_S are the binding information of C and S.

P_1 and P_2 used in the process of protocol design can be transformed in the following:

P_1:

$M_1\ C\rightarrow S: N_C$

$M_2\ S\rightarrow C: \{ 1, \beta_C, N_C, N_S \}_{skS}$

$M_3\ C\rightarrow S: \{ N_S \}_{skC}$

P_2:

$N_1\ S\rightarrow C: N_S$

$N_2\ C\rightarrow S: \{ 2, \beta_S, N_C, N_S \}_{skC}$

$N_3\ S\rightarrow C: \{ N_C \}_{skS}$

Based on this, the design process by composition method [13] is as follows:

The sequence of events performed by agents can be determined:

$e+(M_1) < e-(M_1) < e+(M_2) < e-(M_2) < e+(M_3) < e-(M_3)$

$e+(N_1) < e-(N_1) < e+(N_2) < e-(N_2) < e+(N_3) < e-(N_3)$

$e+(M_1) < e+(N_1)$

$\beta = \beta_C \cup \beta_S = \{C, S\}$, so $P_1 \otimes P_2$ is obtained by composition as follows:

$C\rightarrow S: N_C$

$S\rightarrow C: N_S,\{ 1, \beta_C, N_C, N_S \}_{skS}$

$C\rightarrow S: \{ N_S \}_{skC}, \{ 2, \beta_S, N_C, N_S \}_{skC}$

$S\rightarrow C: \{ N_C \}_{skS}$

It should be ensured that two authentication goals in the same protocol run, avoiding replay attacks in multiple runs. So Term Binding $c=(C, S)$ is added:

$C\rightarrow S: N_C$

$S \rightarrow C : <c>_{skS}$

$S\rightarrow C: N_S,\{ 1, \beta_C, N_C, N_S \}_{skS}$

$C\rightarrow S: \{ N_S \}_{skC}, \{ 2, \beta_S, N_C, N_S \}_{skC}$

$S\rightarrow C: \{ N_C \}_{skS}$

To simplify the primitive protocol, the terms N_S in $\{ N_S \}_{skC}$ and β_C in $\{ \beta_C, N_C, N_S \}_{skS}$ could be combined or replaced:

$C\rightarrow S: N_C$

$S\rightarrow C: N_S,\{ 1, c, N_C, N_S \}_{skS}$

$C\rightarrow S: \{ 2, \beta_S, N_C, N_S \}_{skC}$

$S\rightarrow C: \{ N_C \}_{skS}$

At last, the c and β_S can be replaced by $\beta=(C, S)$:

$C\rightarrow S: N_C$

$S\rightarrow C: N_S,\{ 1, \beta, N_C, N_S \}_{skS}$

$C\rightarrow S: \{ 2, \beta, N_C, N_S \}_{skC}$

$S\rightarrow C: \{ N_C \}_{skS}$

The security protocol ITA is obtained by composition, by which mutual authentication between C and S is insured.

B. Distribution of Secrets in Symmetric Key Cryptosystem

The goal of information transmission security protocol in symmetric key cryptosystem (ITS for short), is to ensure the distribution of keys and secrets between A and B, sent by server S.

APG [15] is used to generate two types of protocol primitives, including key establishment and an authentication server:

P_1:

P_A->P_S:E{NONCE_A,SYMKEY_(P_A,P_S)} | New(NONCE_A);

P_S->P_A:E{ NONCE_A,SESKEY_KAB,SYMKEY_(P_A,P_S)} | New(SESKEY_KAB1);

P_2:

P_B->P_S:E{NONCE_B,SYMKEY_(P_B,P_S)} | New(NONCE_B);

P_S->P_B:E{ NONCE_B,SESKEY_KAB,SYMKEY_(P_B,P_S)} | New(SESKEY_KAB2);

APG [15] is used to generate the primitive for secrets exchange:

P_B->P_A:C[E{NONCE_B,SYMKEY_(P_B,P_A)}, P_A] | New(NONCE_B);

P_A->P_B:C[E{NONCE_A,SYMKEY_(P_A,P_B)} P_B] | New(NONCE_A);

It is assumed that there are three participants: A, B, and S. S is an authentication server with faithful behavior. Either A or B shares a secret key k_{AS} (k_{SA})or k_{BS} (k_{SB})with S. Either a or b is a short-term secret between A and S or B and S, and either c or d is a secret distributed to A or B by S. In the $\beta_x=(A, S)$, and $\beta_y=(B, S)$, either β_x or β_y is the binding information of secrets k_{AB1} or k_{AB2}. $\beta'=(A, B)$, where β' is the binding information of secrets x. $\beta=(A, B, S)$, $c_{SA}=(a, c, \beta)$, $c_{SB}=(b, d, \beta)$, $c_{BS}=(a, b, \beta)$.

P_1 and P_2 used in the process of key establishment can be transformed in the following:

P_1:

$M_1\ A\rightarrow S: \{ \beta_x, a \}_{kAS}$

$M_2\ S\rightarrow A: \{ a, k_{AB1} \}_{kAS}$

P_2:

$N_1\ B\rightarrow S: \{ \beta_y, b \}_{kBS}$

$N_2\ S\rightarrow B: \{ b, k_{AB2} \}_{kBS}$

P' used in the process of secrets exchange can be transformed in the following:

P':

$M_1'\ B \rightarrow A : A, \{x, \beta'\}_{kBA}$

$M_2'\ A \rightarrow B : B, \{x, \beta'\}_{kAB}$

Based on this, the design process by composition is as follows:

The sequence of events which are actions performed by agents, can be determined:

$e+(M_1)< e-(M_1)< e+(M_2)< e-(M_2)$

$e+(N_1)< e-(N_1)< e+(N_2)< e-(N_2)$

$e+(M_1)< e+(N_1)$

So the $P_1 \otimes P_2$ can be obtained:

$M_1\ A\rightarrow S: \{ \beta_x, a \}_{kAS}$

$N_1\ B\rightarrow S: \{ \beta_y, b \}_{kBS}$

$M_2\ S\rightarrow A: \{ a, k_{AB1} \}_{kAS}$

$N_2\ S\rightarrow B: \{ b, k_{AB2} \}_{kBS}$

↓

M_1 $A \rightarrow B : \{ \beta_x, a \}_{kAS}$

NM $B \rightarrow S : \{ \beta_x, a \}_{kAS}, \{ \beta_y, b \}_{kBS}$

MN $S \rightarrow A : \{ a, k_{AB1} \}_{kAS}, \{ b, k_{AB2} \}_{kBS}$

N_2 $A \rightarrow B : \{ b, k_{AB2} \}_{kBS}$

The term binding information $<c_{BS}>_{kBS}$ is added:

M_1 $A \rightarrow B : \{ \beta_x, a \}_{kAS}$

NM $B \rightarrow S : \{ \beta_x, a \}_{kAS}, \{ \beta_y, b \}_{kBS}, <c_{BS}>_{kBS}$

MN $S \rightarrow A : \{ a, k_{AB1} \}_{kAS}, \{ b, k_{AB2} \}_{kBS}, <c_{BS}>_{kBS}$

N_2 $A \rightarrow B : \{ b, k_{AB2} \}_{kBS}$

To simplify the primitive protocol, the $\{ \beta_y, b \}_{kBS}$ and $<c_{BS}>_{kBS}$ can be combined:

M_1 $A \rightarrow B : \{ \beta_x, a \}_{kAS}$

NM $B \rightarrow S : \{ \beta_x, a \}_{kAS}, \{ c_{BS}, b \}_{kBS}$

MN $S \rightarrow A : \{ a, k_{AB1} \}_{kAS}, \{ b, k_{AB2} \}_{kBS}, <c_{BS}>_{kBS}$

N_2 $A \rightarrow B : \{ b, k_{AB2} \}_{kBS}$

The one-way authentication primitive P′ is added:

$A \rightarrow B : \{ \beta_x, a \}_{kAS}$

$B \rightarrow S : \{ \beta_x, a \}_{kAS}, \{ c_{BS}, b \}_{kBS}$

$S \rightarrow A : \{ a, k_{AB1} \}_{kAS}, \{ b, k_{AB2} \}_{kBS}, <c_{BS}>_{kBS}$

$A \rightarrow B : \{ b, k_{AB2} \}_{kBS}$

$B \rightarrow A : A, \{x, \beta' \}_{kBA}$

$A \rightarrow B : B, \{x, \beta' \}_{kAB}$

In Symmetric Key Cryptosystem, k_{AB1} is equals to k_{AB2}, so the final version is as follows:

$A \rightarrow B : \{ \beta_x, a \}_{kAS}$

$B \rightarrow S : \{ \beta_x, a \}_{kAS}, \{ c_{BS}, b \}_{kBS}$

$S \rightarrow A : \{ a, k_{AB} \}_{kAS}, \{ b, k_{AB} \}_{kBS}, <c_{BS}>_{kBS}$

$A \rightarrow B : \{ b, k_{AB} \}_{kBS}$

$B \rightarrow A : A, \{x, \beta' \}_{kAB}$

$A \rightarrow B : B, \{x, \beta' \}_{kAB}$

The security protocol ITS is obtained, by which the distribution of $k_{AB1}$and k_{AB2}($k_{AB} = k_{AB1} = k_{AB2}$), and secrets exchange between A and B are completed.

IV. Formal Verifications

The analysis shows that secrecy, integrity, availability, controllability, non-repudiation and identifiability of sender during transmission can be insured by this architecture.

$C \rightarrow S: N_C$

$S \rightarrow C: N_S, \{ 1, \beta, N_C, N_S \}_{skS}$

$C \rightarrow S: \{ 2, \beta, N_C, N_S \}_{skC}$

$S \rightarrow C: \{ N_C \}_{skS}$

- Secrecy- The information including key and secrets is secret during transmission by $\{ a, k_{AB} \}_{kAS}$, $\{ b, k_{AB} \}_{kBS}$ and $\{x, \beta' \}_{kAB}$.
- Integrity- The information $\{ 1, \beta, N_C, N_S \}_{skS}$ and $\{ 2, \beta, N_C, N_S \}_{skC}$ can only be generated by the participant owning sk_S or sk_C, while the binding information β can be used as verification for information integrity.
- Availability- The information including secret $\{ a, k_{AB} \}_{kAS}$, $\{ b, k_{AB} \}_{kBS}$ or $\{x, \beta' \}_{kAB}$ could be decrypted by authorized user(teacher, student, or administrator) using keys.
- Controllability- The participant could only use information in the designated way (sending or authentication) in the forms as $\{ a, k_{AB} \}_{kAS}$ or $\{ 1, \beta, N_C, N_S \}_{skS}$.
- Non-repudiation- The $\{ \beta, N_C, N_S \}_{skS}$ and $\{ \beta, N_C, N_S \}_{skC}$ can be used as a receipt.
- Identifiability of information sender- The authentication for identity of user by server: the user information could be obtained from the β decrypted from $\{ 2, \beta, N_C, N_S \}_{skC}$, by which the identity of user could be authenticated by server. The authentication for identity of server by user: the information sent by server could be obtained from the secret β decrypted from $\{ 1, \beta, N_C, N_S \}_{skS}$, by which the identity of server could be authenticated.

V. Network Security Architecture

Based on formal specification, the network security architecture is constructed.

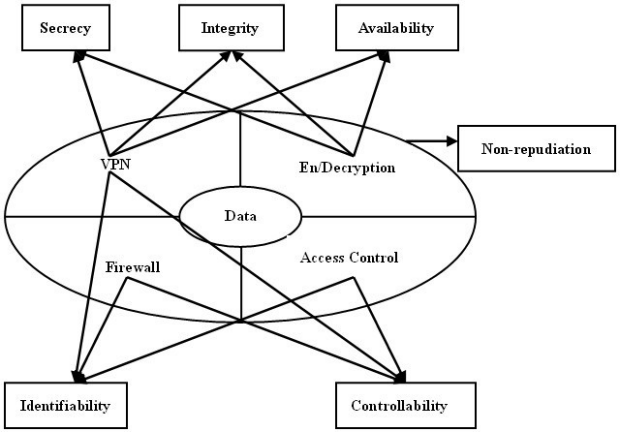


Fig. 3. Network Security Architecture.

Fig. 3 shows that secrecy, integrity, availability, controllability, non-repudiation and identifiability of sender during transmission can be insured by this architecture.

- Secrecy- The data could be secret during transmission with VPN, encryption and decryption.
- Integrity- Integrity of data could be insured with VPN, encryption and decryption.
- Availability- Availability of data could be insured with VPN, encryption and decryption.
- Controllability- Controllability of participant action could be insured with firewall, access control, encryption and decryption.
- Non-repudiation- The non-repudiation of participant could be insured with encryption and decryption, as the forms of $\{ 1, \beta, N_C, N_S \}_{skS}$ or $\{ 2, \beta, N_C, N_S \}_{skC}$.
- Identifiability of information sender- The authentication for identity of user and server could be insured with firewall, access control, encryption and decryption.

VI. Experiment Results

Combined with common security technologies, such as firewall, access control, VPN, IDS, encryption and decryption, following principles of integrity, consistence, balance, operability, and multiple protections, the

network security architecture can be realized as the following Fig. 4:

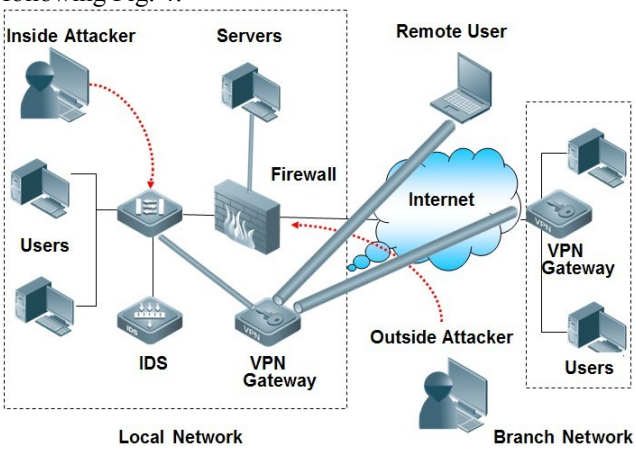


Fig. 4. Realization for Construction of Network Security Architecture.

And then, experiment for verification based on Hadoop which is open source version of the Google file Systems and MapReduce programming specification, is given. The new network security architecture is added into Hadoop as a simulation. The three most common attacks [16] including mandatory access attacks, SQL injection attacks and directory traversal attacks, are used to attack security architecture based on ITA and ITS. The comparison data is given in TABLE 1.

TABLE I.

THE COMPARISON DATA

Attacks	Attack number	No using ITA and ITS		Using ITA and ITS	
		Attacked number	Attacked rate	Attacked number	Attacked rate
Mandatory Access	10	7	0.7	0	0
	20	15	0.75	2	0.1
	40	31	0.78	3	0.08
	80	66	0.83	9	0.11
SQL Injection	10	8	0.8	3	0.33
	20	17	0.85	5	0.25
	40	35	0.88	5	0.13
	80	71	0.89	7	0.09
Directory Traversal Attacks	10	5	0.5	2	0.2
	20	11	0.55	7	0.35
	40	26	0.65	18	0.45
	80	56	0.7	33	0.41

As shown, the attacked rate of cloud environment, which using the network security architecture is much less than the one that no using.

VII. CONCLUSION

According to the mutual model during transmission of digital campus in cloud computing, security requirements are obtained with formal specification. Based on this, the network security architecture is constructed, integrated with common security technologies, such as firewall, IDS, VPN, encryption and decryption. The analysis shows that secrecy, integrity, availability, controllability, non-repudiation and identifiability can be insured.

From the viewpoint of information transmission security, there are security requirements in the constituent parts of digital campus, such as digital library, one card solution, educational administration system, scientific research administration system, financial administration system. In order to avoid the illegal stealing, altering or destroying of important information during transmission, such as user name, password, personal information, and records about teaching, scientific research, or finance, the network security architecture can be used as a common framework for information transmission security in digital campus.

ACKNOWLEDGMENT

This research is supported by the Research Project on Science and Technology in Guangxi Colleges (No. 2013YB215).

REFERENCES

[1] Yuan-jiao Zhu, Ke-qin Zhou. Design and Realizing of the Digital Campus Security System, WCSE 2009, vol. 4: pp 305-309.
[2] Backfield J, and Bambenek J. Network Security Model, SANS Institute; 2008.
[3] Top Threats to Cloud Computing V1.0. Cloud Security Alliance. 2010.
[4] Yang Xu, Xiaoyao Xie. Modeling and Analysis of Security Protocols Using Colored Petri Nets. Journal of Computers, vol. 6(1):19-27, 2011.
[5] Xiaoqiang Zhang, Guiliang Zhu, Weiping Wang, Mengmeng Wang and Shilong Ma. New Public-Key Cryptosystem Based on Two-Dimension DLP. Journal of Computers, vol. 7(1):169-178, 2012.
[6] Chunguang Ma, Jiuru Wang, Peng Wu, Hua Zhang. Identity Authentication and Key Agreement Integrated Key Management Protocol for Heterogeneous Sensor Networks. Journal of Computers, vol. 7(8):1847-1852, 2012.
[7] Zhenqiang Wu, Yanwei Zhou, Jianfeng Ma. A Security Transmission Model in Internet of Things. Chinese Journal of Computers, vol. 34(8):1351−1364, 2011.
[8] Leshen Guo, Naijing Zhang, Jingang Shang. Security Infrastructure of Cloud Computing. Netinfo Security, vol. 7:61−64, 2009.
[9] Chengqiang Xu, Qinghua Shi. Research and expansion of commercial model used in data transmission. Computer Engineering and Design, vol. 26(10):2619−2620, 2005.
[10] Chunle Duan. Key Technologies of Cloud Computing and Realization of System Case. Computer Knowledge and Technology, vol. 7(26): 6344-6345, 2011.
[11] Weijian Xiong, Xiaole LI, Yongjun Luo. Design and Verification of Security Protocol of Information Transmission for Teaching Affairs Administration System. Computer Applications and Software, vol. 8(26):113-114, 2009.
[12] Dengguo Feng, Min Zhang, Yan Zhang, Zhen Xu. Study on Cloud Computing Security. Journal of Software, vol. 22(1):71−83, 2011.
[13] Hyun-Jin Choi. Security protocol design by composition. PhD thesis, Cambridge, UK: University of Cambridge, 2006.
[14] Dolev D, Yao A. On the security o f public-key protocols. IEEE Trans on Information Theory, 1983, 29 (2): 198-208.
[15] A. Perrig and D. Song. A first step towards the automatic generation of security protocols. In Proceedings of the Symposium on Network and Distributed Systems Security, 73-83, 2000.
[16] http://www.softwarehouse.com.cn/news/show/101593.html.

Xiaole Li (1982.8-), Master, mainly engaged in network security, cloud computing.

Ming Weng (1976.12-), Doctor, mainly engaged in logistics and supply chain management, distributed information system.

Ying Wen (1983.11-), Master, mainly engaged in communication technology, network optimization.