INFORMATION
Volume 16, Number 1(B), pp.581-586

ISSN 1343-4500
©2013 International Information Institute

A Study on Security Grade Assignment Model for Mobile Users in Urban Computing

Hoon Ko*, Goreti Marreiros**, Sang Heon Kim***,
Carlos Ramos**** and Tai-hoon Kim*****

*GECAD (Knowledge Engineering and Decision Support Research Group),
ISEP/IPP (Institute of Engineering-Polytechnic of Porto),
Rua Dr. Antonio Bernardino de Almeida, 431, 4200-072, Porto, Portugal.
E-mail: *hko@isep.ipp.pt, **goreti@isep.ipp.pt, ****csr@dei.isep.ipp.pt
***Dept. of Global Culture & Contents, Graduate School,
Hankuk University of Foreign Studies, 230,
Imundong, Daongdaemungu, Seoul, Korea
E-mail ***shkim@gcrc.kr
*****Department of Multimedia Engineering, Hannam University,
Ojeon-dong, Daedeok-Gu, 133, 306-791, Daejeon, S. Korea
E-mail *****taihoonn@hnu.kr*

Abstract

This paper presents a study of the Security Grade Assignment Model (SGAM) and specifies the security level and the Cyber-Society Organization (CSO) according to their purpose to make the cyber-society secured through the SGAM decision. As a result, the SGAM have helped set each security value for all contexts and made the cyber-society more secured.

Key Words: Security, Grade, Ambient Intelligence, Context, Model

1. Introduction

The relation between the information/knowledge expression and the physical expression can be involved as one of items for an ambient intelligent computing [2][3]. Moreover, because there are so many contexts around the users/spaces during a user movement, all applications which are using an AmI for users are based on to the relation between user devices and environments [4]. The AmI gets their results by those contexts during user movement. In these situations, it is possible that the AmI may output the wrong result from unreliable contexts by attackers. Recently, establishing a server have been utilized, so finding secure contexts and make contexts of higher security level for safe communication have been given importance. Attackers try to put their devices on the expected path of all users in order to obtain users information illegally or they may try to broadcast their SPAMS to users. This paper is an extension of [11] which studies the Security Grade Assignment Model (SGAM) to set Cyber-Society Organization (CSO).

2. Security issues and Cyber Social Organization

2.1 Security Issues

In [7], the authors studied generation and management of identity about resource sharing based on distributed subscription, and they designed and implemented the system which provides remote network control over subscription of devices browser. Because a third-party authentication protocol was designed and employed to exchange security assertions among involved parties, the mobile users only should use the subscribed resource with only ID/Password. However, the way which used resource provider have to depend on an access control of IP based, that's why, it has flexibility problem, forcing off campus, and there are the disadvantage to moving user who uses a proxy server. In [8], access authority delegation have been studied and discussed. But they do not directly process the certification between servers and users, so it has weakness in dynamic changing. In [9], although they have tried to overcome flexibility of ACL processing in distributed location, still, they have problems about different security issues, for example, security grade delegation, flexibility. In [10], the authors have surveyed existing problems wherein the existing system has potentials of having security or privacy problems.

2.2 Cyber Social Organizations

The fig. 1 and the table 1 show the relationship among Security Factors [SF], Space Information [SI], and Service Based [SB] which includes each definition and interaction [6][11] [Table 2]. The cyber-society usually is composed by using the SB, by using the same SI, and by processing the same security components. With this situation, it is possible that they can share the same server or the same networks; also, they can get information if they want from the cyber-society.

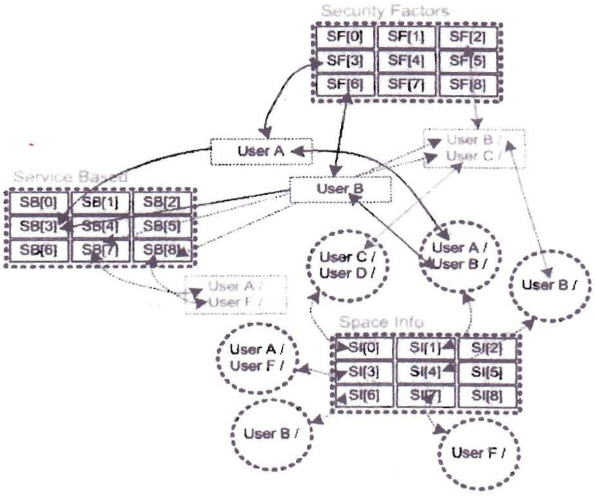

Fig. 2. Information of all users

In addition, it defines same 'SF [1]' as the SI with security viewpoint. Finally, it says that both of them can get the same security server with the same cipher algorithm and the same key length, and also the same security policy etc. Now, they may have little different information about the validation and the expiration dates. If it makes the cyber-society based on 'SF [1]', and then User A and User B shares their keeping security policy in the future. They usually get the same policy for the same composition that can make the related servers convenient. Finally, because there are many users who have different purpose in urban computing, this method is good and effective for this situation to control and to manage.

Table 1. Each Definition

User	SB	SI	SF
User A	SB[3],SB[7]	SI[1],SI[0]	SF[3] 0,2,2 SF[1] 1,2,2
User B	SB[3],SB[5] SB[8]	SI[1],SI[2] SI[1]	SF[6] 4,2,1 SF[6] 4,2,1 SF[2] 2,1,3
User C	SB[7]	SI[0]	SF[0] 0,0,0
User D	SB[6]	SI[3]	SF[0] 0,0,0
User E	SB[0] SB[2]	SI[3] SI[5]	SF[3] 0,2,2 SF[6] 4,2,1
User F	SB[6] SB[8]	SI[3] SI[8]	SF[2] 2,1,3 SF[1] 1,2,1

Table 2. Society composition

User	SB	SI	SF
[0]	User A	User A, User C	User C, User D
[1]		User A, User B*2 User F	User A, User B, User F
[2]	User E	User B, User F	User F
[3]	User A, User B	User E	User A, User E
[5]	User B		
[6]	User D, User F	User E	User B*2, User E
[7]	User A, User C		
[8]	User B, User F		

3. Security Grade Assignment Model

The Security Evaluation Model (SEM) is to evaluate the security of the users and the devices; wherein it needs to know the configured information in each device. The evaluated server can obtain and treat them as contexts. To securely estimate each objects, they will be divided into technology (f1) and operational (f2). The technology evaluation is estimated by the cipher algorithm status and the types of the devices or the network environment and the key size. The operational evaluation is made from an authorization, an authentication status from the security server for all devices, and the update time. It is defined in table 3. To evaluate the *SGAM, EA, KS, SS* and *UT* was defined in equation (1). Also, that model can be considered according to its security weight, which can be set based on its security status. The table 3 defines each *SEI* from(1). They evaluate the security evaluation as *EA* and *KS* belong to the technology evaluation items and *SS* and *UT* process for the operation evaluation items (1).

$$SGAM=[f1(EA,KS)\times f2(SS,UT)]=[(l_{ea}\times w_{ea})+(l_{ks}\times w_{ks})]\times[(l_{ss}\times w_{ss})+(l_{ut}\times w_{ut})]\times 1/100 \quad (1)$$

The *EA* step is for setting the grade (or point) to the security algorithm types, it can change the algorithm types according to the application. For example, the digital signature usually uses the public key algorithm; however, the application for user authentication may use the secret key algorithm. This lea is arranged following each security algorithm. The *KS* named the key size for encrypting provides each l_{ks} grade (or point). If the key size is bigger, it can make a stronger security. However, the processing will be delayed. The l_{ss} in *SS* gets them according to the security status. The security status means how many get an authen/an author from how many security servers.

Table 3. Security Evaluation Items (SEI)

Items	Point	Weight	Total
EncryptionAlgorithm(EA)	l_{ea}	w_{ea}	$l_{ea} \times w_{ea}$
KeySize(KS)	l_{ks}	w_{ks}	$l_{ks} \times w_{ks}$
SecurityStatus(SS)	l_{ss}	w_{ss}	$l_{ss} \times w_{ss}$
UpdateTime(UT)	l_{ut}	w_{ut}	$l_{ut} \times w_{ut}$
Total			*SEI(V)*

It can be defined if they get authen/an author from many security servers, they will be secured. It will be assigned according to the grade of the update time l_{ut} in *UT*. The object which has the latest update time gets the high grade. All grades can be defined based on each evaluated value. Finally, those values specify the *Security Grade Assignment (SGA)*.

4. Experiment

This section describes the experiment for this scenario. All users have their nodes and the node will be linked to each other as shown in fig. 2. Also, each node has their own security values and these values can be dynamically changed according to their updates.

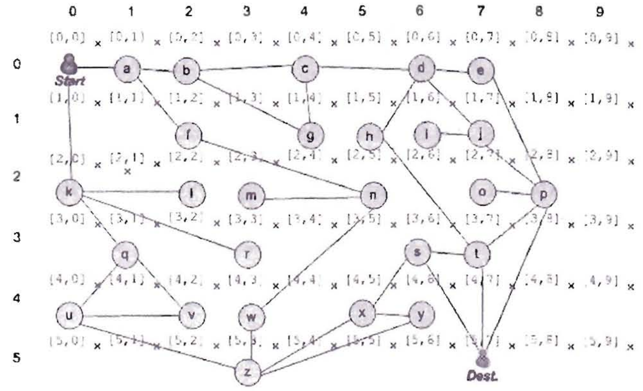

Fig. 3. Network model for Simulation

$$GRADE = [(l_{ea} \times w_{ea})+(l_{ks} \times w_{ks})] \times [(l_{ss} \times w_{ss})+(l_{ut} \times w_{ut})]$$
$$= [(EA_s \times W_s)+(EA_a \times W_a) + (EA_h \times W_h)] +(KS \times W_{ks}) \times (SS \times W_{ss})+(UT \times W_{ut}) \quad (2)$$

These values are substituted into equation (2) which is defined for security grade of each node. The equations (1) and (2) derive the results shown in table 4. As a result, all users set their good nodes shown in table 6. Table 6 shows the best node from source to destination for the User. This next paragraph describes the story. On the basis of *SGAM*, Users (Start) make the optimized nodes involving security factors to get the destination [6, 7]. This *SGAM* does not aim to find both the highest adjacent node and the similarity node for security configuration, but just to find the most optimized node. The number of cells for experiment are 45, and available nodes in those cells are 26 [Fig. 3]. *EA* may get difference algorithms, Symmetry Encrypt Algorithm EA_s, Asymmetry Encrypt Algorithm EA_a and Hash Algorithm

E4, according to each user or each device. Each configuration of 26 nodes for experiment was defined into table 4. The values in the table are *GRADE* from the expression (2). The degree of strength was composed by *[Security value, Consumption]*.

Table 4. Degree of Strength *([Security Value (SV),—SV-Source Value—, Consumption])*

Start	Consum. 1.26	Start	Consumption	Start	Consumption
a[0,1]	[3.77,2.51,0.8227]	k[2,0]	[6.50,5.24,0.9986]	u[4,0]	3.60,2.34,0.7768]
b[0,2]	[2.55,1.29,0.5758]	l[2,2]	[2.24,0.98,0.5233]	v[4,2]	[2.40,1.14,0.5398]
c[0,4]	[1.76,0.05,0.3869]	m[2,3]	[3.60,2.34,0.7768]	w[4,3]	[3.45,2.19,0.7672]
d[0,6]	[9.57,8.31,0.9994]	n[2,5]	[2.97,1.71,0.6679]	x[4,5]	[3.48,2.22,0.7639]
e[0,7]	[1.87,0.61,0.4218	o[2,7]	[3.78,2.52,0.8275]	y[4,6]	[0.68,0.58,0.1748]
f[1,2]	[1.20,0.06,0.2722]	p[2,8]	[5.00,3.74,0.9979]	Z[5,3]	[0.45,0.81,0.1516]
g[1,4]	[2.31,1.05,0.5303]	q[3,1]	[1.20,0.06,0.2722]		
h[1,5]	[4.83,3.57,0.9978]	r[3,3]	[3.63,2.37,0.7945]		
i[1,6]	[0.84,0.42,0.2032]	s[3,6]	[1.68,0.42,0.3684]		
j[1, 7]	[0.60,0.66,0. 1669]	t[3,7]	[0.24,1.02,0.1252]		

When user moves to a[0,1], and it wastes 0.8227. If user moves to k[0,2], it gets 0.9986 as consumption [Table 4]. Therefore, to select a[0,1] is good for user. Eventually, user decides a[0,1] as one of via nodes to get to its destination. Certainly, Security value must first have to define the node which is consisted of hop count, bandwidth, delay, reliability and load etc. As it already mentioned, to decide the nodes from source to destination the routing algorithms have to consider Hop Count, Bandwidth, Delay, Reliability and Load. And then, if security configuration values are involved in node decision, it makes a strong node for safe using in urban computing. That value 17.51 from Source to Destination via a-b-c-d-p is the optimized node of all nodes.

5. Conclusion

This paper aims to provide a secured Urban Computing by adding security values to destinations. The urban computing aims to provide active and intelligent services between users and spaces. Therefore, in order to support its security aspects, individual users are able to select the security configuration in every stage of urban computing. However, there are different security configurations in various devices and networks and they need to reference the security configurations of adjacent notes in order to be evaluating by SGAM. As the paper already stated, SGAM involves the cipher algorithm, the key size, the security status and update dates to evaluate the security rates. Now, this paper only dealt with four issues. The detailed information of neighborhood node and the hiding of users' location should be inclusive in future work to make a stronger security.

6. Acknowledgments

This research was supported in part by a Grant-in-Aid for Scientific Research on Priority Areas (C) ‘Genome Information Science’ (No. 16014202) and a Grant-in-Aid for Scientific

Research (S) (No. 16109006) from the Ministry of Education, Culture, Sports, Science, and Technology of Japan.

References

[1] Carlos Ramos, Augusto JC, Shapiro D, Ambient intelligence the next step for artificial intelligence, IEEE Intelligent Systems, 23 (2008), pp.15-18.

[2] Carlos Ramos, Ambient Intelligence-A State of the Art from Artificial Intelligence Perspective, in Progress in Artificial Intelligence from Lecture Notes in Computer Science, (2007), pp.285-295.

[3] IST Advisory Group, Scenarios for Ambient Intelligence in 2010, EC, (2011).

[4] Rene Meiier and Vinny Cahill, Location-Aware Event-Based Middleware: A Paradigm for Collaborative Mobile Application," Computers and Security, (2006), pp.371-378.

[5] Hoon Ko and Carlos Ramos, A Study on Security Framework for Ambient Intelligent Environment, The fifth international conference on wireless and mobile communications, (2009), August 24-30, Velencia, pp.93-98.

[6] Hoon Ko and Carlos Ramos, A Survey of context classification for intelligent systems research for Ambient Intelligence, The fourth international Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing, (2010), February 15-18, Krakow, pp.746-75

[7] Mingchao Ma and Steve Woodhead, Authentication delegation for subscription-based remote network services, Computers and Security, 25 (2006), pp.371-378.

[8] Tuomas Aura, Distributed Access Rights Management with Delegation Certificates, Secure Internet programming: security issues for mobile and distributed objects, (2001), pp.211-235.

[9] David W. Chadwick, Alexander Otenko, and Edward Ball, Role-Based Access Control with X.509 Attribute Certificates, IEEE Internet Computing, 7 (2003), pp.62-69.

[10] Ludwig Fuchs, and Gunther Pernul, Digital Reducing the Risk of Insider Misuse by Revising Identity Management and User Account Data, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 1 (2010), pp.14-28.

[11] Hoon Ko, and Carlos Ramos, A Study on Security Status Matrix (SSM) in Urban Computing, ICITST2009, (2009) London, November 9-12, pp.134-140.

*Corresponding author: Hoon Ko, Ph.D.
Knowledge Engineering & Decision Support Research Group (GECAD),
Institute of Engineering-Polytechnic of Porto (ISEP/IPP),
R. Dr. Antonio Bernardino de Almeida, 431, 4200-072, Porto, Portugal
E-mail: hko@isep.ipp.pt