International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:2, No:6, 2008

A Wireless Secure Remote Access Architecture Implementing Role Based Access Control: WiSeR

E. Tomur, R. Deregozu, and T. Genc

***Abstract*—**In this study, we propose a network architecture for providing secure access to information resources of enterprise network from remote locations in a wireless fashion. Our proposed architecture offers a very promising solution for organizations which are in need of a secure, flexible and cost-effective remote access methodology. Security of the proposed architecture is based on Virtual Private Network technology and a special role based access control mechanism with location and time constraints. The flexibility mainly comes from the use of Internet as the communication medium and cost-effectiveness is due to the possibility of in-house implementation of the proposed architecture.

***Keywords*—**Remote access, wireless networks, security, virtual private networks, RBAC.

I. Introduction

One of the most important business requirements of our age is always-available computing. Providing anywhere, anytime access to corporate resources for mobile employees turns out to be an inevitable need for enterprises of next decade since majority of key business processes (80% according to Gartner [1]) will involve exchange of information with remote workers. Extending the office for employees to their home, their cars or anywhere they have Internet connection, remote access brings in competitive advantage for corporations by enabling access to critical information at anytime. A case study conducted by Adesso Systems Inc. shows that a 30% improvement in the efficiency of key business processes can be achieved when suitable remote access architecture is implemented [2].

Despite the productivity gains and competitive differentiation brought by always-available computing, corporations seem reluctant in deployment of remote access systems. While one main reason for this is the excessive diversity of remote access technology alternatives which confuse IT managers about choice of the best solution, the other one is the concerns about security gaps which may arise when an organization opens its enterprise network to the outside. Although there are several companies which deliver turnkey remote access solutions for corporations which do not have enough IT expertise, the cost of such outsourcing solutions may outweigh the revenues gained by productivity increases that remote access provides.

In this paper, we present an architecture called WiSeR for implementing **Wi**reless **Se**cure **R**emote access to resources of enterprise network. The proposed architecture is product-independent. Corporations can use it to implement their own remote access system by using COTS (Commercial Off-the-Shelf) products. WiSeR combines the security of VPN (Virtual Private Network) technology with the flexibility of wireless access. Besides, it implements the Temporal and Spatial Role Based Access Control (TS-RBAC) model proposed in [3] and therefore, is able to provide granular access control to corporate resources. With WiSeR, corporations can enjoy the benefits introduced by remote access without being worried about whether they have chosen the appropriate and secure remote access solution among available alternatives. In addition, corporations do not have to endure high costs charged by turnkey remote access service providers since the only cost for WiSeR is of the required hardware and software.

The rest of this paper is organized as follows: In Section II, we first mention the business drivers behind remote access and then explain remote access technology alternatives with a particular focus on VPN. Section III illustrates how wireless technologies can be incorporated into VPN. Section IV introduces RBAC concept. In Section V, we present the proposed WiSeR architecture and in Section VI, we mention the implementation of it for Turkey's Banking Regulation Supervision Agency and give our experiences. Finally, in Section VII, our conclusions are presented.

II. Remote Access

Remote access means providing users who are away from the enterprise with the ability to access information resources residing in the corporate network. In this way, remote users can perform their job-related tasks from anywhere they have a network connection to their main site as if they are in the office. The convenience of having access to critical information by using a remote access infrastructure is an early form of ubiquitous computing [4] indicating the availability of information from anywhere and at any time.

In order to profit from the advantages of remote access, an appropriate method for the corporation should be chosen

Manuscript received September 15, 2006.

E. Tomur is with the Banking Regulation and Supervision Agency, Ankara, Turkey (corresponding author to provide phone: +90-312-4556726; fax: +90-312-4240877; e-mail: etomur@ bddk.org.tr).

R. Deregozu is with the Banking Regulation and Supervision Agency, Ankara, Turkey (e-mail: rderegozu@bddk.org.tr).

T. Genc is with the Banking Regulation and Supervision Agency, Ankara, Turkey (e-mail: tgenc@bddk.org.tr).

among several remote access technology alternatives. The selected method should satisfy the information needs of remote workers in a convenient and cost-effective way, and at the same time, it should not expose any security vulnerabilities for the information systems of the enterprise.

There are several remote access options such as dialing-up into a remote access server (RAS), connecting over private circuits like leased-lines or utilizing Internet as the communication medium and providing security with VPN. We will briefly mention VPN since it is the remote access method used in our proposed architecture. More detailed information on VPN and other remote access technologies can be found in [5].

A virtual private network is a secure connection through an insecure public network, e.g. the Internet, where the confidentiality and integrity of the transmitted information is ensured by some tunneling protocols, which actually designate the public network as virtually private by encryption. As it can be used to set up a secure connection between two remote local networks over a public wide area network, VPN is also a very promising remote access alternative when compared to expensive leased lines or slow dial-up connections. VPN also offers great flexibility because the only prerequisite for connection is an entry point to the Internet. In next section, we will inquire the possibility of further increasing VPN's flexibility by using it together with wireless access.

III. VPN and Wireless Access

Lately, the wireless access technologies such as Wi-Fi wireless local area networks (WLAN) and WiMAX broadband wireless access have been very popular. The answer of the question about whether these wireless technologies can be utilized for making remote connections more comfortable by allowing non-tethered and mobile access from remote locations is yes. Since both Wi-Fi and WiMAX operate on the second layer of the OSI model, they do nothing more than providing link layer network connectivity just as a dial-up or ADSL connection does. More specifically, once a remote user gains access to the central site over Internet via a wireless hotspot, she can then make a VPN connection without any problem since VPN operates above the wireless link layer.

Nevertheless, there remains one more point to be clarified before one can use wireless technologies together with VPN as a remote access method without leaving any cause for concern: This is the well-known and documented insecurities of wireless access methods [6], [7]. Fortunately, security vulnerabilities particularly present in Wi-Fi do not jeopardize the strong security provided by VPN technology when configured properly. In fact, VPN can be used to protect IEEE 802.11 WLANs replacing the weak WLAN security protocols like WEP with robust authentication and encryption mechanisms of IPSec VPNs, as detailed in [8]. Therefore, the flexibility of wireless networks can be utilized in remote access when combined with the security of VPN technology since it protects the confidentiality and integrity of data in an end-to-end fashion from the client computer to the VPN gateway even for the data transmitted on the air by radio waves.

Although IPSec VPNs ensure integrity and confidentiality of data on the way both from client computer to wireless access point and from access point to the VPN gateway without any need to rely on WLAN security, some form of authentication is needed to prevent unauthorized clients from associating with the access points installed at remote sites where remote employees work. Since these access points are used as a means for Internet access of remote workers as well as remote access, unauthorized users should be prevented from accessing the Internet over those wireless access points. Strong VPN authentication mechanisms allowing only authorized clients to launch VPN connections to the main site do not provide any protection for war drivers having free Internet access over the wireless access point and therefore another authentication mechanism is needed for wireless access.

Strong authentication for 802.11 WLANs can be achieved by the employment of IEEE 802.1X standard [9]. 802.1X is a port based authentication framework, and when used with Extensible Authentication Protocol (EAP) in a wireless LAN, mutual authentication between clients and access points can be achieved via an authentication server. Several mechanisms such as EAP-MD5, EAP-TLS, EAP-TTLS or EAP-PEAP can be chosen as authentication method when 802.1X is used. Since it uses public key certificates for both the client and the server to verify their identities to each other, EAP-TLS is a very secure option and, that is why it is chosen as the wireless authentication mechanism of WiSeR. Despite the security advantages it brings in, deployment of EAP-TLS for wireless access systems installed at remote locations has some problematic issues due to the authentication servers required. Because it is not feasible to employ individual authentication servers at each remote access location due to scalability problems, a centralized solution is needed which utilizes a single authentication server at the main site to authenticate wireless clients at all locations. Our proposed architecture, WiSeR, incorporates such an authentication solution in addition to the VPN security and a special role based access control mechanism with time and location constraints. Before giving details of WiSeR, we summarize the basics of role based access control in the next section.

IV. Role based Access Control (RBAC)

Role Based Access Control mechanisms, where the access rights to the data and resources are granted based on the job responsibilities, have been widely used for years. In RBAC, roles are created according to the job functions performed in an organization, permissions are granted to those roles, and finally, users are assigned to the roles in accordance with their specific job responsibilities and qualifications. Therefore, a role is a collection of permissions, and only those users who

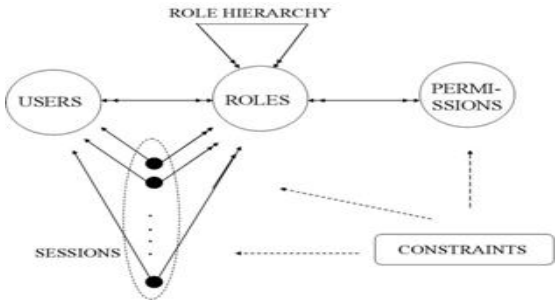

Fig. 1 The general RBAC model 1

are assigned to this specific role can perform operations on resources within the permission boundary of the role. In Fig. 1, this relationship is illustrated as proposed by the general RBAC model of [10]. RBAC is a remarkable alternative among access control methodologies. It supports three well-known security principles, namely, least privilege, separation of duties and data abstraction. In addition, since it suffices to revoke the old role and assign the new role when job function of a user is changed, burden on system administration is reduced. A final worth-mentioning property of RBAC is that it is policy neutral. However, it can be configured to enforce traditional models such as discretionary and mandatory access control as presented in [11]. Owing to advantages described in this paragraph, several practical RBAC applications have been implemented ([12], [13]).

There has also been research on several aspects of RBAC such as bringing formalism to RBAC models ([14], [15]) and providing other constraints like time and location for determination of role permissions. In [16] and [17], for instance, RBAC model is extended such that temporal constraints are taken into consideration while granting permissions to roles associated with users. In temporal RBAC models, considering the organizational functions and services with temporal requirements (e.g., part-time staff working only from 9 am to 2 pm or day doctors performing his/her duty only on certain days), role permissions are allowed to be active during certain time periods and non-active during others. This way, not only the role itself but also the time determines granting of permissions, and thus, performs access control.

On the other hand, with the widespread use of mobile equipment such as laptop computers and pocket PCs, users now access network resources from several locations in the enterprise. Hence, RBAC models are improved in such a way that role permissions are constrained also by spatial requirements as detailed in several studies such as [18] and [19]. In so-called spatial RBAC models, permissions not only depend on the role itself but also on the location of the role owner. Therefore, a single role has different sets of permissions for different locations. For example, a user with administrator role can have both read and write access to corporate database from his/her desk but have only read access from all other locations.

In our proposed architecture, we utilize both spatial and temporal role based access control models as presented in [3]. Therefore, level of access from remote site to corporate network resources is determined by the role of the remote user, his/her location and time of access request. Besides, method and strength of VPN encryption is chosen according to the role of the user.

V. WiSeR: Wireless Secure Remote Access

The proposed architecture of this paper, which is named as WiSeR, presents a common framework for providing secure access to information resources of enterprise network from remote locations in a wireless fashion. In WiSeR, network connectivity from remote locations to the central site is solely based on the Internet, that is, WiSeR can be used wherever a remote client has Internet access. The security of WiSeR relies on the strong data encryption and integrity preservation methods of VPN, a smartcard-based two-factor authentication scheme used in both VPN and wireless authentication, and the granular access control capability of TS-RBAC. The only required component of WiSeR is a VPN terminating module and its corresponding software. If remote clients reside at fixed designated locations, then a device that will provide Internet connectivity such as a wireless ADSL router is needed at each location. The WiSeR architecture is illustrated in Fig. 2.

As shown in the figure, enterprise network of the organization is positioned behind a firewall to permit remote inbound connections only in a strictly controlled way. The VPN gateway, either embedded into the firewall or standing as an individual module, is the termination point of all VPN connections from the remote sites. It handles encryption/decryption and integrity checking processes of all VPN connections as well as the authentication of VPN clients. The wireless authentication server is located in the DMZ (Demilitarized Zone) of the main site's network for not allowing yet unauthenticated connections into the enterprise network. Based on IEEE 802.1X protocol, this authentication server is used to validate the identity of clients attempting wireless access from remote sites. Authentication of both wireless and VPN connections are performed by public key certificates stored in smartcards and this constitutes a strong two-factor authentication mechanism which is much more secure than password-based schemes.

The clients at remote sites possess their smartcards where certificates are stored and these clients are equipped with laptop computers that have smartcard readers installed. If client-based VPN approach rather than SSL VPN is chosen, also VPN client software has to be installed on the client computers. Wireless Internet access gateways are set up at each pre-determined remote access location. As shown in the figure, for instance, remote sites A and B have wireless ADSL routers that connect remote employees residing at these locations to the Internet in a wireless fashion. Of course, an active ADSL line or any other active connection to the

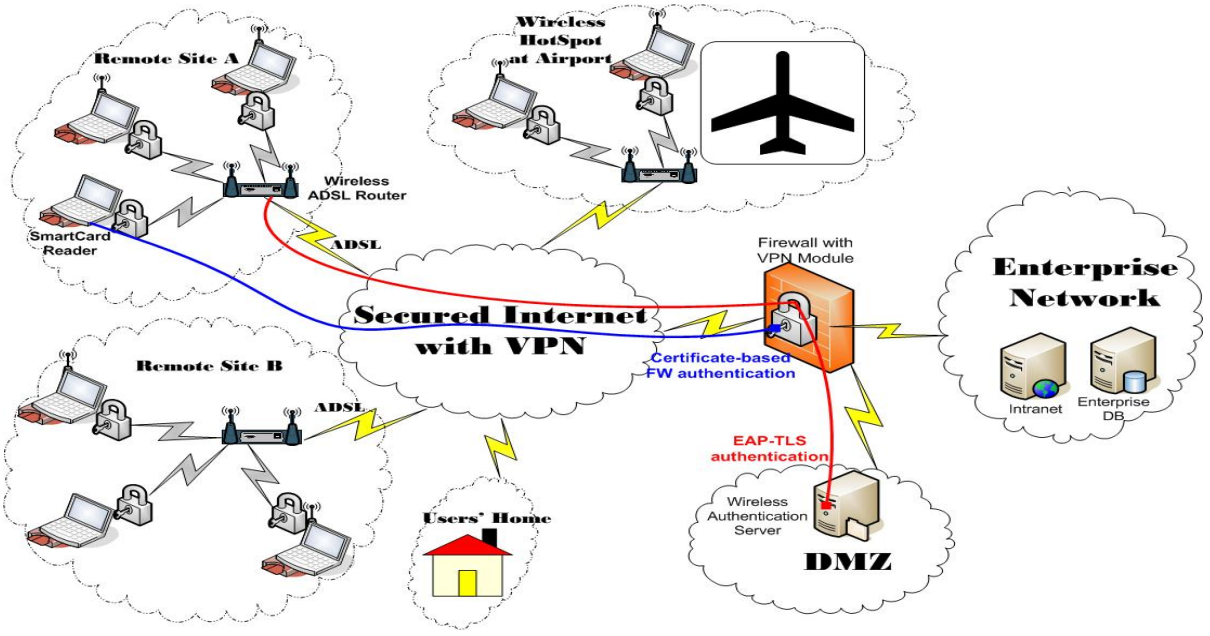

Fig. 2 Proposed wireless secure remote access (WiSeR) architecture

Internet should be present at these designated remote access locations. Besides, wireless Internet access devices like the ADSL router should be pre-configured for Internet access with service provider's settings and for 802.1X authentication. As mentioned before, not only the designated locations where remote employees are present at all times but also any other location where a user can access Internet can be used for secure remote access in WiSeR architecture. For example, wireless secure remote access using an 802.11 hotspot in an airport or a dial-up Internet connection from users' homes is possible as shown in Fig. 2. In that case, there is no need for wireless authentication since this should be handled by the service provider.

Another important property of our proposed architecture is the extra security provided by use of temporal and spatial role based access control. In WiSeR, the level of security (method and strength of encryption, and access rights) is determined by the triple *(role, location, time)*. The role is the same as the role concept in RBAC and refers to the organizational position of the remote user such as head auditor, auditor or support personnel. The location is the place where remote access attempt is initiated. We determine the location from the IP address information. We assume that the real IP addresses used for Internet access in designated remote sites are static and known. All IP addresses other than those known addresses are taken as a special category called "AnyLocation". And, the last element of the triple, time refers to the time of the day where access request is initiated.

When a user attempts to access a corporate network resource remotely, he/she is first authenticated and encryption method is chosen according to his/her role, then he/she is granted an appropriate access level based on both time of access and his/her location. This access control is performed by the firewall. The example rule base of a firewall performing this temporal and spatial role based access control is given in Table I. Here, "group1" and "group2" are two user groups where low-profile (support personnel) and high-profile (auditors) users are members respectively and "remote_sites" is a network object composed of known IP addresses of all designated remote sites.

TABLE I
RULE BASE OF THE FIREWALL

Time	Source	Destination	Service	Action
Any_ Time	remote_sites	DMZ_Network	EAP	Accept
Work_ Hour	Group1@ remote_sites	Intranet	HTTP	Encrypt
Any_ Time	Group1@ remote_sites	Database_Server	SQL	Encrypt
Work_ Hour	Group2@ remote_sites	All_Corporate_ Network	ANY	Encrypt
Any_ Time	AllUsers@ AnyLocation	Mail_Server	SMTP	Encrypt
Any_ Time	ANY	ANY	ANY	DROP

When the security policy illustrated in Table I is enforced, a remote user can access (a) only from the location he/she is allowed, (b) only to network resources that he/she is allowed, (c) only for the services and applications he/she is allowed, (d) only at the time duration he/she is allowed and, (e) with encryption method and strength appropriate for him/her. First four items (a,b,c,d) are related to access control and determined by the triple (role, location, time) while encryption in the last item (e) is determined by the role of the user. For

instance, users of group2 can access any service from only the designated remote sites during only work hours whereas group1 users are allowed merely for Intranet and DB server access. All users are permitted to access their e-mail at any remote location and at any time.

In an organization that uses the proposed WiSeR architecture described above for wireless secure remote access, the order of events occurring when a client attempts to access enterprise LAN (local area network) from a remote location is as follows:

1) Client machine tries to associate with the wireless access point at the designated remote site where the employee is located. Authentication information for this wireless connection attempt is sent to the authentication server residing in corporate network DMZ over Internet on EAP port (the first rule of firewall permits this). If this EAP-TLS authentication is successful, remote client will be authorized for only Internet access over the wireless access point.
2) Using the authorized wireless Internet access at the designated location or any kind of Internet access at any other location, remote client establishes network connectivity to the VPN gateway.
3) VPN gateway challenges the remote client for access authorization to the enterprise network. If client successfully authenticates, VPN gateway permits access to enterprise network through the Firewall for allowed services based on the role, location and time information,
4) After VPN authentication, key exchange process is performed between the client and the VPN gateway. Using these exchanged keys, all traffic from the client machine to the VPN gateway is encrypted in accordance with the role of the client providing required level of confidentiality and integrity for transmitted data along the entire remote access path.

The WiSeR architecture whose operational steps are given above offers a very promising solution for organizations which are in need of a secure, flexible and cost-effective remote access methodology. In this proposed architecture, proven securities of VPN technology, role based access control and 802.1X authentication framework are combined. Several strong encryption methods such as 3DES and AES and integrity preservation schemes such as MD5 and SHA1, and any other method supported by employed VPN module can be utilized. Since both VPN and wireless authentications are based on a something you know (smartcard PIN) and something you have (certificate) scheme, the risk of having unauthorized connections is very low. On top of this, when client-based VPN approach is preferred, central security policies can be loaded into the remote client computers from the main site to mitigate attacks to client machines from the Internet, thus contributing to the sound security of WiSeR. Finally, employment of the temporal and spatial RBAC mechanism ensures that a remote user can access a network resource only if there exists a role that the user is a member of and that role contains a permission at the specific location and time. Therefore, TS-RBAC mechanism increases the security provided by WiSeR as formally verified in [3].

The possibility of making secure remote connections at any location where Internet is present makes WiSeR a very flexible remote access alternative. Wireless coverage areas set up at designated remote employee locations not only enable mobile connections but also remove the burden of cabling at remote sites in which cable installation may not be possible. The last but not least issue making WiSeR a very flexible solution is the convenience in its implementation using COTS products. In other words, WiSeR is not dependent on any specific product and can be implemented using any VPN hardware/software, smartcard or authentication server. Finally, WiSeR is an economical remote access solution since it does not involve any high outsourcing costs. It can be implemented in-house even in organizations with a limited IT know-how due to its simple and straightforward architecture.

VI. Implementation of WiSeR

The WiSeR architecture presented in this paper is originally developed for providing the remote employees of Banking Regulation and Supervision Agency (BRSA) of Turkey with a secure remote access method. The proposed architecture has been fully implemented, and at the time being, auditors of BRSA working at more than 50 remote locations access to information resources of BRSA network in a wireless fashion. In this implementation, a Checkpoint firewall with VPN module, SecureClient VPN software and Microsoft IAS as the wireless authentication server are used. Each of these designated remote sites is provided with 512K ADSL Internet access and US Robotics wireless ADSL routers are installed at these sites for wireless coverage.

The described setup is successfully performing the expected functionality of remote access requirements of BRSA employees in a secure fashion. While auditors working at remote locations reach enterprise resources from their working area as if they are in the office, all other employees can also access to corporate network from any remote location.

VII. Conclusion

This paper presents an architecture called WiSeR to implement wireless secure remote access to information resources of the enterprise network of an organization. The key feature of the proposed architecture is the utilization of security of VPN technology and role based access control mechanism together with the flexibility of wireless access in a combined manner. Strong encryption methods of VPN technology, a very secure two-factor VPN authentication scheme based on public key certificates, temporal and spatial role based access control policy and the employment of 802.1X wireless authentication are important security aspects provided by WiSeR. Wireless access areas constructed at remote employee locations not only enable mobile remote connections but also provide great flexibility since it does not require any cabling at remote sites. Furthermore, WiSeR enables the possibility of making secure remote connections at

any location where any kind of Internet access is present. As a result, with WiSeR, corporations can enjoy the competitive business benefits of remote access without comprising any security risks and without enduring high outsourcing costs charged by turnkey remote access service providers.

REFERENCES

[1] W. Clark, "Enterprises Must Assess Impact of Mobile Applications", *Gartner Inc. Report*, 2003.
[2] Always Available Computing: Best Practices for Empowering Today's Mobile Work Force. Available: http://www.adessosystems.com
[3] E. Tomur and Y.M. Erten, "Application of temporal and spatial role based access control in 802.11 wireless networks", *Computers & Security*, vol. 25, no.4, pp 452-458, September 2006.
[4] M. Weiser, "Hot Topics: Ubiquitous Computing", *IEEE Computer*, October 1993.
[5] S. Harris, *CISSP All-In-One Guide*. McGraw-Hill Publications, 2004, ch.7.
[6] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11", *in Proc. of the Seventh Annual International Conference on Mobile Computing and Networking*, 2001.
[7] S. Fluhrer, I. Martin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4", presented at Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.
[8] E. Tomur and Y.M. Erten, "A layered security architecture for corporate 802.11 wireless networks", presented at 2nd Wireless Telecommunications Symposium, Pomona, CA, 2004.
[9] *IEEE Standards for local and metropolitan area networks: Standard for port based network access control*, IEEE draft P802.1X/D11, March 2001.
[10] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman, "Role-based access control models", *IEEE Computer*, vol. 29, no. 2, February 1996.
[11] S. Osborn, R. Sandhu, and Q. Munawer, "Configuring role-based access control to enforce mandatory and discretionary access control policies", *ACM Transactions on Information and System Security*, vol. 13, no. 2, February 2000.
[12] J. Barkley, K. Beznosov, and J. Uppal, "Supporting relationships in access control using role based access control", *in Proc. of 3rd ACM Workshop Role Based Access Control*, Fairfax, VA, October 1998.
[13] D. Ferraiolo, J. Barkley, and D. Kuhn, "Role-based access control and reference implementation within a corporate intranet", *ACM Transactions on Information and System Security*, vol. 2, no. 1, 1999.
[14] M.J. Moyer, and M. Abamad, "Generalized role-based access control", *in Proc. of 21st International Conference on Distributed Computing Systems*, April 2001.
[15] M. Koch, L.V. Mancini, and F. Parisi-Presicce, "A Graph-Based Formalism for RBAC", *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 3, 2002.
[16] E. Bertino, P.A: Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control model", *ACM Transactions on Information and System Security*, vol. 4, no. 3, 2001.
[17] J.B.D Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A Generalized Temporal Role-Based Access Control Model", *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 1, pp 4 – 23, January 2005.
[18] F. Hansen, and V. Oleshchuk, "Spatial role-based access control model for wireless networks", presented at Vehicular Technology Conference, 2003.
[19] M. Wilikens, S. Feriti, A. Sanna, and M. Masera, "A context-related authorization and access control method based on RBAC: A case study from the health care domain", presented at Seventh ACM Symposium on Access Control Models and Technologies, 2002.