Using Multi-Level Role Based Access Control for Wireless Classified Environments

Daniel E. Burgner, Luay A. Wahsheh, Aftab Ahmad, Jonathan M. Graham, Cheryl V. Hinds,
Aurelia T. Williams, and Sandra J. DeLoatch
Information Assurance Research, Education, and Development Institute (IA-REDI)
Department of Computer Science
Norfolk State University
Norfolk, Virginia 23504

ABSTRACT
Wireless environments have been researched considerably over many years. Initially, such applications involve the use of radios but have later evolved into satellites, cellular phones and global positioning systems. One detail involving wireless environments is the need to have them restricted only to those who have a need to use a wireless environment. Such users would have a role with permissions needed to access the system. One example of a user in this type of environment could be a commander on a battlefield requesting real-time information on enemy movements operating in a foreign country. This paper discusses the potential of a multi-level role-based access control (RBAC) in a wireless classified environment. Areas covered include what RBAC is, how RBAC works in a wireless network, how RBAC works with wireless applications as well as multi-level RBAC application examples. This would show that multi-level RBAC would be suitable for use in a wireless classified environment. Our analysis shows that a Multi-Role Based Access Control can be used along with XML to implement an object-oriented approach to provide security for a wireless classified environment.

Keywords
Access control, wireless networks, multi-level RBAC, security.

1. INTRODUCTION
Wireless environments are a fact of life. Everywhere you go, you encounter a wireless environment in use, such as a cell phone, global positioning systems, wireless hotspots and satellite television. A need has arisen for certain wireless environments to be classified, restricted to those who have a need to access these environments. Examples of users who would have a need to access these environments would include military commanders on the battlefield requesting real-time information on activities of an adversary as well as doctors using personal digital assistants to enter medical information from a patient. These environments would require users to have a role with certain sets of permissions to access the system, which is inherent in a role-based access control (RBAC) system. This paper reviews RBAC, how it works with wireless networks, wireless applications using RBAC and multi-level applications of RBAC.

2. ROLE-BASED ACCESS CONTROL (RBAC)
RBAC is an access control approach that is used in large systems that use roles to define responsibilities and objects to define resources with permissions to access them. This section reviews the definitions, hierarchies and benefits associated with using RBAC.

2.1 Definitions
The role is the most important aspect of this approach since it is used to group subjects based upon certain properties. Users, another entity in this approach, are referred to as subjects. Each user has a set of roles that he or she can perform [7]. This set of roles is also known as permissions giving approval of users acting in a role to access resources in the system. Many-to-many relationships can be developed since users can be assigned to multiple roles, with roles having multiple permissions. Permissions can be assigned to multiple roles while roles can be assigned to multiple users. Let's start by using a set of sessions S. A user initiates a session in which he or she activates a subset of roles in which the user is a member of. Multiple roles can be established from S to roles (R). The user's permissions would be the union of permissions from roles initiated in a session. A single user is a part of a session, which remains a constant for the life of a session. A user can have multiple sessions open at once, with each in a different window on a workstation screen. A session can have multiple combinations of active roles. This means that multiple sessions can have multiple active permissions at once. Constraints can come into play to any preceding component. One example could be a mutually disjoint role, such as a purchasing manager and accounts payable manager, in which a user cannot have both roles [2].

The relationships between these entities can be best described as follows: Users initiate by sending accessing operations and requests and are subjects that data objects process operations. Permissions are privileges that certain data objects perform certain special operations. Data objects are objects of access control, accessed by calling programs or data accessing them. Roles are executable and operational sets in system's user, an important concept in RBAC. Roles are the bridge between users and permissions with multiple relationships existing between all three [8].

Another concept called context control is important in that it is based on location. The impact on RBAC's architecture is two-fold. First, it distinguishes activated and predefined roles for a particular user. Predefined roles are determined at registration time and based on user's credentials. A user's working context along with dynamic exclusion rules determined what roles can be

activated at session time. Secondly, user context knowledge becomes a contributing factor when permission assignment of roles is refined. This allows for dynamic allocation of permissions for particular roles based upon user context constraints [10].

2.2 Hierarchies

It is natural for a hierarchy to exist between roles and users. Role hierarchies can also exist among the roles themselves as certain roles can be subroles of other roles. Role hierarchies allow policy administrators to write generic access rules only once as opposed to once for every role as applicable. A company's RBAC policy could have the roles of President, Vice-President and Chief Financial Officer, which are subroles of the officer role [7].

Such a hierarchy allows for reflexivity, transitivity and anti-symmetry. Roles inheriting their own permissions are an example of reflexivity. The context of RBAC systems allows for transitivity to be a natural requirement. Ruling out roles inheriting from one another, or redundancy, is an example of anti-symmetry. For a multi-level RBAC system, a hierarchy can be built upon groups being separated into classes, which can be based upon clearance levels in the military, for example. Flow of information can be forced upward in terms of sensitivity in such a model [2].

2.3 Benefits

Many benefits exist from using RBAC systems. Authorization administration is simplified since a system administrator needs only to revoke and assign appropriate role memberships should users change job functions. RBAC is also policy neutral by supporting security policy objectives as well as offering flexibility regarding different security policies [4]. The access control policy would evolve over the course of the system life cycle, modified to meet changing needs. This policy, embodied in RBAC components, determine whether users are allowed access system data [2]. This also means that role and role hierarchies can mirror an organization's structure easily, resulting in well-structured access control policies making sense in the organization's context. Lastly, it supports delegation of access permissions in the event of a user's absence [7].

3. RBAC AND WIRELESS NETWORKS

One use for RBAC is with wireless networks. A variety of factors may arise regarding roles and permissions prevalent for wireless networks using RBAC. These factors may include the location of the user as well as the implementation issues related to wireless networks. This section reviews the access control models, infrastructure and the use of XML.

3.1 Access Control Models

A traditional RBAC model allows users to be assigned roles and permissions connected to these roles. More flexibility can be achieved in a mobile setting as permissions are changed dynamically to a role that is based on a user's location. When a user changes locations, permissions may be added or deleted dynamically. This is the basis of the Spatial Role-Based Access Control (SRBAC) model. SRBAC is an extension of RBAC in that it has the components of sessions and locations. Locations are expressed by descriptions of location domains identifiable by a system. A wireless network can identify and verify location of any legitimate user with its network architecture. Hierarchies in SRBAC define inheritance relationships between roles with roles inheriting permissions from other roles if all permissions are connected dependent on location. This means that a role can have permissions that other roles have in a certain domain together with permissions assigned to that role directly. However, separation of duties can be enforced on roles that cannot be executed concurrently by a user. The SRBAC model allows for users to have mutually exclusive roles if they cannot be used in the same location [4].

Users are limited to what they can do on mobile networks via separation of duty. Wireless devices are limited by space with caching of events and services to be allowed on individual devices. Such a framework would consist of four components: user management (combination of profile and membership management), protocol management, policy enforcement and event service. This framework runs on all applicable devices. User credentials are maintained by the profile management component with users managing their credentials and device settings as well as the user's preferences. Membership management exposes the user management interface to application level, allowing for users to: start establishment of, searching for and joining communities. Users can register services provided to other participants. Membership management also checks authenticity of policies and enforces them by extracting and distributing policy instances to enforcement components. The event service mechanism collects events, aggregates them and forwards them to policy enforcement mechanisms. System events are handled by protocol management while discovery of new communities are handled by membership management [5].

3.2 Infrastructure

Memon [6] suggests a mobile network in which one architectural component being present to start a mobile network. Any joining device is to be authenticated by central servers owned by an organization. For the sake of interoperability, devices are to be kept simple and compatible. A multi-channel model is proposed to facilitate accessing of services and information interchange among users. Such channels would include the universal description, discovery and integration (UDDI) channel, session channel and the data channel. The UDDI channel would have registry information about each group, given by a central server and propagated by the coordinator device. The session channel has the description and executable code for each session with information indexed with a service key to enable access performance better. Data channels are used for data transfer among network devices. Coordinator devices have more features in its software component to facilitate needed communications with central server for authentication as well as creating software proxies for network devices. Other devices communicate within the network on the data channel and their proxies communicate via the session channel. New devices entering the network download UDDI channels and store them for later use. Proxies are software components running on central servers for each device on the network. Their main functions are access control decisions, logging of device actions, role versus access list, generating random keys for device sharing as well as interfacing with other proxies. Central servers must be able to control many

mobile networks as well as create multiple proxies at once. The role of databases involves the coordinator buffer sharing and caching data frequently used by all mobile users. Roles will partition database information into access contexts. Object oriented methods associated with database objects partition the object interface which provides windowed (or user interface) access to object information. Object interface distribution across roles is achieved when all database information is specified and held in database objects with methods authorized to roles [6].

In summary, a typical mobile network requires authentication and database server devices present to facilitate its formation. Devices would have to be authenticated by a server with data buffers being used to improve cache retrieval. The buffer's secondary objective involves sharing and caching data frequently used by all users on the network. This results in reduction of disk accesses and invalidates obsolete buffer data [5].

3.3 XML

Extensible Markup Language (XML) could be used as a means to implement RBAC for a wireless network. For a database application, roles can be defined and functions can be identified for each role [5]. A role graph will emerge that defines a structural relationship among the roles in the application. The resulting hierarchy would show that the higher roles in the hierarchy have more roles than those lower in the hierarchy. The set of privileges is disjoint for any two roles not part of the same chain. Examples of constraints could include: the maximum number of users for a given role is one; certain roles cannot be assigned to the same user as certain roles cannot be activated or enabled at the same user session. A Document Type Definition (DTD) is later defined, representing the schema for the chosen RBAC model, which captures the actual data in a conforming XML document. DTDs provide logical tag organization used in an XML document. Issues involving DTD definition are: expressiveness, flexibility and document readability. Expressiveness refers to capturing semantic of various RBAC model constructs. Flexibility refers to generic DTDs describing most common RBAC models. Document readability refers to the XML document being readable such that the RBAC implementation program's logic is not overly complicated. Many commercial XML processors would be sufficient to validate conformance to the XML schema. A Java application can be used to read data in an XML document that can generate the internal Document Object Model (DOM) tree representation of an XML document. The DOM tree is navigated to extract data related to roles, relationships and constraints by navigating to the nodes in question. SQL queries would be generated to create roles, specify structural relationship or constraints involving previously created roles. SQL queries are passed as parameters to appropriate methods for implementation on a resource server.

4. RBAC APPLICATIONS

A variety of existing applications use RBAC. They range from group communication systems in a grid environment to algorithms used in conjunction with the RBAC model to role-based protocol for wireless networks. This section will cover an example of each.

4.1 Mobile Ad Hoc Networks

Mobile ad hoc networks have security issues unique to them in that they operate in an uncontrolled medium, have a topology that changes dynamically and lack not only centralized management but also a means to defend it. This requires a new means for which communications are to be protected within a mobile ad hoc network. Barka and Mohamed [2] propose using a protocol that controls access to a mobile ad hoc network via node credentials as well as access to information exchanged within the group on basis of access level of different nodes. The protocol is based on a multicast Ad Hoc On-Demand Distance Vector Routing (MAODV) algorithm. The protocol's main functions are group formation and data access. Group formation and member access are done with node roles with privileges assumed by these roles. Data dissemination is dependent on a role-based access policy. All control packets generated in this method are applicable to this method with the following modifications: RREQ packet, which has two additional fields, one for the role of requesting node with the other being authentication information for this node; RREP packet, which has an additional field containing the key allowing requesting node to access information according to its privileges; and NACK packet, a new packet used to inform requesting node it cannot access multicast group for insufficient credentials [2].

4.2 RBAC Algorithm

Younis and Ebrahim [11] propose an algorithm which is used in conjunction with the RBAC model that reduces information transferred during a multicast session deemed redundant. Active nodes in a multicast tree filter data packets that are forwarded to the receivers according to information contained in packet header. This results in minimal redundancy of transmitted data and overcomes inefficiency issues related to using network resources when one multicast group is used for each role of different participants in a multicast session. Application layer message headers introduced with this algorithm should not be encrypted since the message belongs to roles that are forwarded downstream should be encrypted by shared keys for corresponding set of roles. Source nodes have the ability to distribute representation of functions during key exchange process assuring that these functions are transferred securely [11].

4.3 Group Communication Systems in Grid Environments

Group communication systems allow for efficient communications between processes organized into groups, communicating via multicast in asynchronous environments [13]. Secure group communication is a key component for collaborative applications. Grid computing is emerging as an effective means to pair geographically distributed resources, solving large-scale computational issues related to wide-area networks, resulting in collaboration being brought to a new level. Integrating both of these technologies is appropriate for providing support for collaborative applications in a grid system. RBAC and attribute based approach is introduced to define security policies for group authentication and authorization. A general authentication and authorization framework for group communication uses an identity provider, a service provider, a Policy Decision Provider (PDP), group management, group policy, and a group member. Identity providers play the role of authentication and

authorization authority. Security providers verify the users' identities and attributes. PDP determines whether users can be allowed to take group management functions. Group management provides group related management functions, which include group maintenance and key management. Group communication systems have many types of group management policies. Once groups are created, group policies are built based on policy template and context, the former is formed before the group is created. Many types of group members exist for group communication systems. Roles would have to be defined for each kind. Grid collaborative applications require group management policies to be defined before a group is created, with policies being registered to a domain or information server.

5. MULTI-LEVEL RBAC

RBAC can even be extended to allow for multi-level usage. This section will cover examples of multi-level RBAC, such as: collaborative CAD, collaborative process planning system and multi-role based access control.

5.1 Collaborative CAD

A multi-level access control framework for a collaborative CAD system was proposed that implements an Extended Hierarchy Role-Based Access Control (EHRBAC) [3]. EHRBAC is integrated with a Layered Privilege Model (LPM) and Hierarchy RBAC (HRBAC) to facilitate hierarchical access control of collaborative feature modeling in component/part level and design feature level. EHRBAC is based on HRBAC, where roles are hierarchically partial ordered in a role hierarchy. Designers are affiliated with sets of roles via Designer Assignment (DA). Designer-Session is a one-to-many relation, mapping session to designer. Session-Role is a many-to-many relation, mapping roles to sessions. Separation of designers and sessions solves an issue caused by one designer with different account with different roles in different sessions. LPM facilitates multi-granularity access control by partitioning privileges into two layers, with Part-Privileges being the top layer and Feature-Privileges being the bottom layer. Part-Privileges can be defined as a tetrad *(p, m, f, v)*, where *p* is the target part, *m* is access mode, *f* is a flag representing part's default feature privileges and *v* is the additional value for this privilege. The flag can be set to access all features of the part in access mode or no features. Feature-Privileges operates on the same principle *(d, m, f, v)*, with *d* being the target design feature, *f* being negative or positive (representing privilege being negative operation or otherwise) and *m* and *v* being the same as in Part-Privileges. A token passing scheme is used to access design features that only one designer can use at a time. When a designer is finished with the feature, he or she returns the token and submits the changes to the feature. Each part and feature has a version entity. When the version is updated, it searched the related roles and assigned designers. All relevant designers will receive a message. Once a designer receives the message, he or she accesses the corresponding data from the server.

5.2 Collaborative Process Planning System

A process planning multi-level and dynamic access control (PPMLDAC) model was proposed for a collaborative process planning system based on the RBAC model [9]. This multi-level permission model is based upon a product and task decomposition level structure. This model features five permission states: dormant, hold, ready, running and accomplished. Dormant represents permission in non-activation. Ready represents validity conditions being satisfied and basic preparation work is completed. Hold shows the state that the permission is suspended because of waiting for system resources or permission constraints and also forced to suspend by the system in the running process. Running expresses that permission activated successfully is running. Accomplished is a representation that the permission is successfully implemented. The multi-level permission model also considers the level characteristics of products, composed of three levels: component, part and feature. Component-level permission is defined by 2-tuple in which the component object of permission operation is expressed by component and access control method by mode. Part-level permission works in the same manner as component-level permission with part representing the part object of permission operation. Feature-level permission works in the same manner as component-level permission with part representing the part object of permission operation. Task assignment is completed with a session of collaborative process planning according to structure characteristics of products and responsibilities of technologists' participation. The permission is defined first followed by defining and authorizing the role. User definition and authorization is the last step in this process.

5.3 Multi-Role Based Access Control (MRBAC)

MRBAC is an extension to the RBAC model that adopts the object-oriented concept to perform hybrid role hierarchy management and security rules/role administration [12]. This model enables sophisticated management on roles and their hierarchies as well as supporting temporal constraints and IP address restrictions. RBAC's security access control rule is defined as a three tuple $p = (Ru, x, m)$, where *Ru* represents a user role, *x* represents an object and *m* represents the accessing model. MRBAC's security access model is defined as a five tuple $p = (Ru, Ro, <Rt>, <Rs>, M)$, where *Ru, Ro,* <*Rt*>, <*Rs*> represents user role, object role, temporal role and spatial role, respectively and *M* represents the access mode (or permission) for objects represented by *Ro*. The object role replaces the traditional object, allowing for security permissions for sets of multimedia objects or other files. Temporal roles and spatial roles, which are IP-address based, are introduced so that controls can be put into place regarding temporal constraints and access computers. The access control mode's definition can be extended to handle multimedia data. The combination of all of these roles allows the security access policies to be defined as access control rules. MRBAC's role hierarchy theory considers temporal roles, spatial roles and object roles. User roles would have permission inheritance-only relations over each other on object *Ro* at time *Rt* using computer represented by *Rs*. In addition, they have role activation-only and general inheritance relations over each other at time *Rt* using computer represented by *Rs*. Temporal roles and spatial roles have inheritance relations over each other.

Based on the information presented, we recommend that an MRBAC system be used that uses XML to provide security for a wireless classified environment. The MRBAC system provides for an object-oriented approach that would allow XML to be used to its fullest capabilities.

6. CONCLUSIONS

The research presented in this paper represents the usage of RBAC in a wireless classified environment. A number of uses for RBAC exist in wireless networks along with wireless applications. Multi-level RBAC applications are also presented to show the potential that it has for use in a wireless classified environment. In summary, an MRBAC system using XML would be better suited for implementation in a wireless classified environment since it uses an object-oriented approach to provide security in a wireless classified environment.

7. ACKNOWLEDGEMENTS

This material is based upon work supported by the Department of Energy National Nuclear Security Administration under Award number DE-FG52-09NA29516/A000. This paper was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

REFERENCES

[1] Barka, E. E., and Y. Gadallah. "A Role-based Protocol for Secure Multicast Communication in Mobile Ad Hoc Networks." *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference.* Caen, France. New York: ACM, 2010. 701-05.

[2] Barka, E. E., and E. E. Mohamed. "Securing Hierarchical Multicast Communications Using Roles." *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing.* Leipzig, Germany. New York: ACM, 2009. 101-05.

[3] Fang, C., W. Peng, X. Ye, and S. Zhang. "Multi-Level Access Control for Collaborative CAD." *Proceedings of the 9th International Conference on Computer Supported Cooperative Work in Design.* Coventry, United Kingdom: IEEE, 2005. 643-48.

[4] Hansen, F., and V. Oleshchuk. "Spatial Role-Based Access Control Model for Wireless Networks." *IEEE 58th Vehicular Technology Conference.* Orlando, FL.: IEEE, 2003. 2093-097.

[5] Memon, Q. A., and S. Khoja. "XML Implementation of Role Based Control in Healthcare Adhoc Networks." *IEEE 2007 International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications.* Hangzhou, China: IEEE, 2007. 1223-226.

[6] Memon, Q. A. "Policy Based Data Access in Wireless Adhoc Networks." *Advances in Hybrid Information Technology: First International Conference.* Jeju Island, Korea: IEEE, 2006. 112-16.

[7] Moyer, M. J., and M. Ahamad. "Generalized Role-Based Access Control." *Proceedings of the 21st International Conference on Distributed Computing Systems*. Mesa, AZ.: IEEE, 2001. 391-98.

[8] Qin, S., and Q. Zhao. "Application Research of the CAN on Role-Based Access Control." *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing*. Beijing, China: IEEE, 2009. 1-3.

[9] Su, Y., J. Wang, S. Liang, L. Tang, and W. Wang. "Research on Access Control in Collaborative Process Planning System." *Proceedings of the Second International Symposium on Intelligent Information Technology Application.* Shanghai, China: IEEE, 2008. 726-30.

[10] Wilikens, M., S. Ferti, A. Sanna, and M. Masera. "A Context-Related Authorization and Access Control Method Based on RBAC: A case study from the health care domain." *Proceedings of Seventh ACM Symposium on Access Control Models and Technologies.* Monterrey, CA. New York: ACM, 2002. 117-24.

[11] Younis, A. A., and G. A. Ebrahim. "An Efficient Role-Based Access Control Mechanism for Multicasting Environments." *Proceedings of the IEEE Sixth International Symposium on Multimedia Software Engineering.* Miami, FL.: IEEE, 2004. 142-45.

[12] Zhao, N., M. Chen, S. Chen, and M. Shyu. "MRBAC: Hierarchical Role Management and Security Access Control for Distributed Multimedia Systems." *Proceedings of the 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC).* Orlando, FL.: IEEE, 2008. 76-82.

[13] Zou, D., L. T. Yang, W. Qiang, X. Chen and Z. Han. "An Authentication and Access Control Framework for Group Communication Systems in Grid Environment." *Proceedings of the IEEE 21st International Conference on Advanced Networking and Applications.* Niagara Falls, Ontario, Canada.: IEEE, 2007. 547-54.