Communications and Network, 2013, 5, 473-477
http://dx.doi.org/10.4236/cn.2013.53B2087 Published Online September 2013 (http://www.scirp.org/journal/cn)

A Secure Approach to Educating a Mobile World-Class Military

—A Mobile Secure Concept for Accessing the Classroom from Around the World

Terry C. House
Thouse Technology Research and Development, Fayetteville, NC, USA
Email: thouse@methodist.edu

Received April 2013

ABSTRACT

The "Mobile Secure Role Base Access Control Device" (MS-Ro-BAC) Device and database is a single unit system with the ability to instantly connect to secure databases around the world through Low Earth Orbit Satellite (LEO) using VPN wired communications. The capabilities provided by the MS-Ro-BAC device would support the "Global War on Terrorism" and increase the security of US force and Department of Defense Personnel around the world. Information dissemination in an austere environment is the focus of this seminal research; combat forces and DoD personnel depend on timely strategic information before making life threatening decisions on the battle field. This manuscript provides the framework and a prototype to improve the information dissemination process in the modern day information scenario.

Keywords: Wireless; RBAC; Computer; Networking; Security; Secure; Education; Military; US; DoD

1. Introduction

A Military service member attending college, who deploys away from the United States is required to communicate with their education provider before leaving the country to figure out how they will continue their education once they are no longer in USA. Most soldiers will depend upon the local nation's Internet to connect to the university's servers and educational resources while they are deployed; however, this form of communication platform is very unstable and unreliable for most university classroom activities. The 21st Century military is required to use some of the most advanced technological systems in the world to fight the enemy; therefore, these men and women are now required to think fast, react to all types of data and information in a professional manner. To execute their wartime mission, they must be not only highly educated in the art of war, but also in the world of general knowledge at the scholastic level. These individuals are required to interact with different personalities around the world, and having a solid college education is one way of ensuring our men and women in the military a solid foundation in how to conduct themselves in any setting they are in while defending the United States of America.

2. Problem Statement

Military students constantly struggle to complete their education while deployed. The current communication approach used in the military does not support an approach to educate their members while deployed. The current systems are not very good at sending communicating with non-military network systems in an educational secure ad-hoc manner around the world as well. In a global war scenario, there is not a strategic communication process in place assist the fighting men and women to effectively complete their online courses from anywhere in the world and submit their assignments in a timely manner. When students cannot complete or continue their educational aspirations while deployed, it becomes a significant drain on their morale. This drop in enthusiasm and passion soon turns into a lack of desire to stay in the military and support the commander's combat mission [2] (Steven Greenwald).

3. Prior Research

The motivation to conduct this research was inspired by "*Role Based Access Control on the Web*" [4] (Ravi Sandhu). The journal introduced various methods of implementing RBAC in a secure environment. Different drawing and data structures suggested a variety of client and server architectural designs. However, the journal did not produce a persuasive remedy for unifying the various techniques to support an approach to educating military forces deployed around the world. Software

businesses are attempting to solve the RBAC issues by embedding the role implementation process within the software. Many companies use proprietary RBAC software, which has impeded RBAC standardization on a larger scale. Dr. Strembeck [3] designed xoRBAC software, which provides a flexible RBAC service. Due to the nature of combat and the type of information sent around the world, all security objects must fit in the same access architecture in order to communicate effectively and allow students to access their college classrooms across different platforms [2] (Steven Greenwald).

4. What is RBAC?

Role Based Access Control is the use of generated templates of access authorizations and agreements applied to a specific student or professor. In the past, network administrators dealt with change after change; each new user required a profile designed for their access authorities. This new form of access control is a proven alternative to traditional discretionary and mandatory access control. RBAC technology has been around since 1990 as a trusted way to manage databases and network access in large corporations. The network administrator ensures that each patron has access privileges to their information area only. RBAC supports three essential security principles: information hiding, least-privileges and separation of duties. In **Figure 1**, the "Role" is a semantic concept forming the basis of RBAC positions. The administrator's initial necessity is to build "Role" [7] (Sandhu R).

In **Figure 2**, the instructor is the base role of the classroom process, from this position of authorization, the students and administrators are implemented into the classroom as either learner or supporting entity to the mobile classroom system.

A New Vision for Secure RBAC

In a normal access controlled process, each user receives approval to access specific information, based on the level of trust placed in the user. In order for the administrator to grant access to certain levels of information, the user must have met certain attribute requirements. Those attributes of the user are role, access identity and group or clearance level. The ideology of students connecting through secure authenticating hardware and software is a vital design methodology of the MS-Ro-BAC system. The device consists of three major concepts: Secure hardware, software and satellite communications from anywhere I the world. The user connects to secure LEO satellites by network browser SHTTP connection. A network intelligent agent controls the actual roles assigned to the users in any domain [9] (Thomsen D).

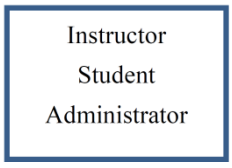

Figure 1. Example roles in a MS-Ro-BAC system.

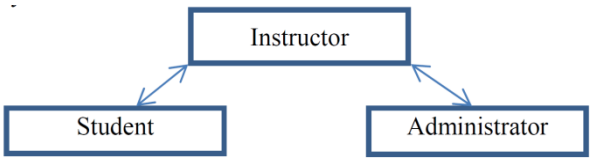

Figure 2. Relationship model of hierarchy.

5. The Mobile Secure RBAC Network Ideology

The thought process behind this Device is to take the server-pull technology design above and implement it directly into a (firmware) product that is small and mobile. This device concept would be directly in line with a VPN concept that is supported by the Universities that are part of the network of schools committed to supporting our Military forces around the world. The device could resemble a laptop or tablet; however, it could also be a "System on Stick"; meaning it could be a USB device active system that makes any device compliant with the software needed to communicate with those institutions that are part of the global VPN connectivity system. On the university end of the connection process, would be a high-speed network designed to support satellite long-range communications with their students. The institutional side of the network would ensure that there is always a VPN and server that control the data communications in proximity of the student. In a MS-Ro-BAC Network environment, there are no dedicated hubs, servers, special hard-drives or local administrators. The Network system will instantly provide users with the ability to transmit data, instant message and conduct live conferences while participating in a Distributed Compartment (DISCOM) RBAC secure environment [3] (Greenwald S).

Software and Hardware Aspects

The university could create a system that is completely self-contained, as it pertains to the hardware and software needed to communicate directly to their institution's satellite network. The system case could be lightweight and very durable where field use is applicable. A small keyboard and GUI is available to send and receive data. There are two USB ports to assist with uploading and downloading of files. A proprietary operating system (OS) that is similar to the *Microsoft* Pentium 4 processor New Generation Secure Computing Base (NGSCB) will control the mobile device. A wireless network radio will sustain LEO satellite connectivity. Biometric thumbprint

and retina scan requirements are part of the access authorization process when initiating the boot process. The device is capable of connecting directly to a static computing base that is not secure or as an independent system. Standard Wi-Fi communication electronics are standard in the hardware architecture; this authorizes the user to communicate with other MS-Ro-BAC users through satellite connectivity. This device should remain in a secure location that is accessible by the student only. However, if such an environment is not available, it is possible to view information through a secure viewing apparatus. Encrypted software and hardware technology in the device require authentication with the operating systems at all times during data transmission. The proprietary software will support chat abilities, instant messaging and file transfers through secure VPN encrypted format [3] (Greenwald S). **Figure 3**. Illustrates the MS-Ro-BAC device physical attributes. The case measures approximately 132 sq. inches and 1.5 inches thick. Position 1 indicates the rear panel input areas for network and fiber optic connections. Position 2 indicates the USB ports. Position 3 indicates the areas for an external monitor and keyboard connection. Position 4 designates the thumbprint (T) and retina scan (R) location. Position 5 indicates various system indicators and control buttons. Position 6 depicts the satellite antenna for LEO Satellite device operations. Position 7 (C) portrays a digital camera. In the future, field commanders can securely network with higher headquarters and subordinates as soon as each individual's device has entered the LEO network and successfully authenticated their systems hardware and software. After a satisfactory handshake, the secure connection is made.

This device has three modes: 1) Deployed independently for LEO satellite connectivity from any location in the world; 2) Configured for normal unsecured use not connected to a wired or wireless network in the US; 3) The least favorable use of the device is coupling with non-trusted static computer peripherals; keyboards, monitors and external storage devices. The preferred implementation of the device is a standalone Satellite Virtual Private Network (VPN) communication system. **Figure 4**. Illustrates how each device activates and automatically authenticates through encrypted hardware and software technology. Once initiated, the user must submit a thumb or retina scan, then login to the interface with user-name and password. The network software will initiate the "tracker program" that will survey the entire network for fellow MS-Ro-BAC devices and begin the handshake process with other students in the same classroom for group meetings and seminars. After completing the system authorization process, the user will receive a graphical user interface that depicts all activated MS-Ro-BAC devices. Standard graphics and data come standard on every machine to decrease the message size, redundancy and increase the bandwidth speed during transmission [3] (Greenwald S). **Figure 4** provides insight into the methodology of the communication process and access authorization. This design ensures participants in one classification cannot penetrate data of higher authorization levels. In distributed Compartments (DISCOM) 1, 2 and 3 the letters stand for the following: s = Subject (users, databases), o = Objects (files, etc.), p = Privileges, r = Resource Pool (CPU, computing power), h = Handles (names or code names used for users). Notice that D1 has direct connectivity to D2 and D3; this gives direct control and access to both DISCOMs [3] (Greenwald S).

The proprietary software instantly reads the RBAC information of other devices and places each device in the hierarchy structure in which they have access, as it pertains to school, instructor, administrator etc. Therefore, if four students logged in and the head Governor (D1) was not there, each student becomes a peer-to-peer connection. In a MS-R-BAC infrastructure, the main DISCOM in Washington DC is "Big Brother" (BB), such as the University. Management of lower DISCOMs is the job of lower ranking Controllers, such as satellite campuses around the country. BB has authority over every DISCOM and its individual students and instructors. BB can

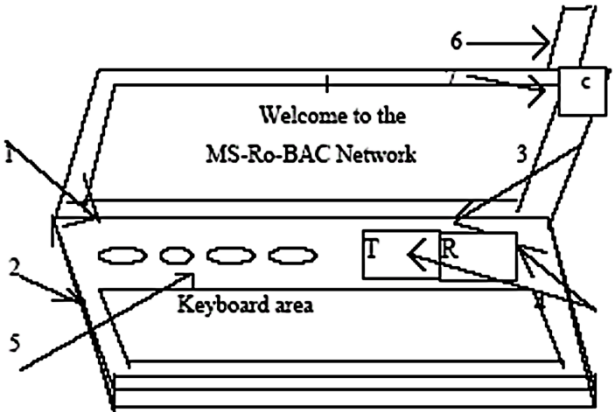

Figure 3. MS-Ro-BAC network device.

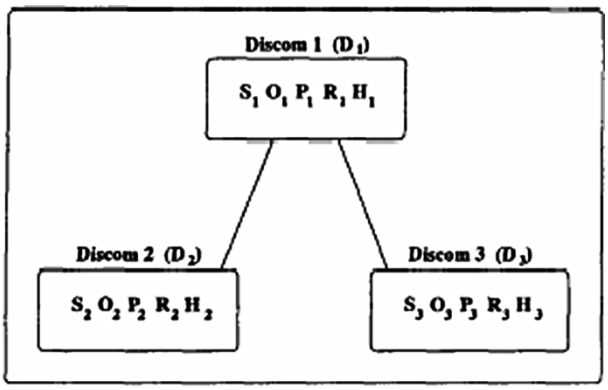

Figure 4. A LEO network with 3 DISCOMs.

immediately suspend any user's rights without the permission of their local DISCOM controller or governor. BB creates an instance of itself to share information and chat with subordinate schools. Washington, in **Figure 5**, resides in a monitoring position. The duplicate image of BB ensures covert channels do not exist to senior DISCOMs. This code design is transparent to the users. The different countries represent areas where students may be deployed around the world and pursuing their education [3] (Greenwald S).

6. Proprietary Software Implementation

The MS-Ro-BAC Device will include various types of proprietary firmware and authentication programs to ensure file transfers, chats, and synchronized meetings are secure. Each device incorporates biometric scanner to identify the device and student using it. A login name and password is required to access the systems application environment. The device includes encrypted conferencing software with integrated middleware to ensure authorized users are the only recipients and course information. The highly encrypted Object Oriented Data Module (OODM) ensures the "no write-up" restrictions of subordinates' users are enforced. Public Key Infrastructure software will digitally sign and encrypt files automatically before transmission. This dynamic approach to satellite communications allows several devices to correspond at anytime without the supervision of higher level DISCOMs. An aggressive anti-virus defense algorithm will ensure the device maintains system integrity before initiating connectivity with other devices. Once the user accesses the network, secure tracking and discovery software locates other devices available in the system [1] (Baldwin RW) [3] (Greenwald SJ) [7] (Sandhu R).

The hierarchical model is responsible for the theory of Role-sets of authorized users and permissions. Role-sets are objects grouped together under one class that authorizes multiple role positions to the selected users of that set. The permissions assigned to that role are basic and dynamic as needed by the RBAC Governor or BB [7] (Sandhu R). The basic essentials in a Core RBAC interaction are: 1) Users (USERS); 2) Roles (ROLES); 3) objects (OBS), operations (OPS), and permissions (PRMS). Senior managers assign roles and permissions to each user. The user may be another device automatically working at the highest level in Washington [9] (Thomsen DJ) [4] (Nyanchama M and Osborn S) [7] (Sandhu R).

Figure 6 illustrates the Middle East DISCOM and four local stations within its command sector. *D*1.0 is an instance of *D*1. In the diagram, a one directional arrow symbolizes the "no write up" rule for preventing covert channels to unauthorized devices: *D*1. There is a two-way communication channel, depicted by a two-headed arrow, between *D*1 and its instance *D*10. This illustrates the required procedure for *D*1 to receive information from subordinate objects. Objects *D*1.1, through *D*1.4 are examples of other countries in theatre: Iraq, Iran, Kuwait and Jordon.

Advantages and Disadvantages

The conventional and Special Operations communities have not incorporated such a device to support the military forces continuing their academic program while deployed in other countries. There are individual systems that support one or two aspects of this process; however, they are not capable of instantly linking individual students in a Virtual Private Network around the world to conduct their classroom activities. This device will correlate with existing LEO network satellites that are presently in orbit. [1] (Baldwin RW). Information security through hardware and software authentication provides a reliable approach to ensure only authorized devices can receive and send data on this network. The MS-Ro-BAC Device will include several AI biometric programs to maintain the integrity of the authorized user.

The negative aspects of the MS-Ro-BAC system do not over-shadow the positive advantages of providing a quality education to soldiers who are defending the USA around the world. Due to many institutions experiencing a low in attendance, it can prohibit the development of such a network and system. Funding has always inhibited the progress of new evolving technology. Another disadvantage is poor reception during electrical storms or the absence of a satellite "foot print" that provides coverage for system users. Any network blackout can destroy the bandwidth and throughput to support the MIS-Ro-BAC Device and the LEO Satellites ability to support their existing responsibilities. Another disadvantage is

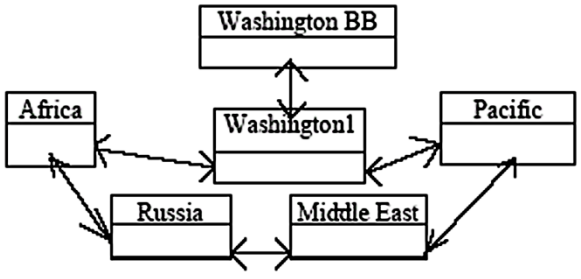

Figure 5. B. Brother conferencing with controllers.

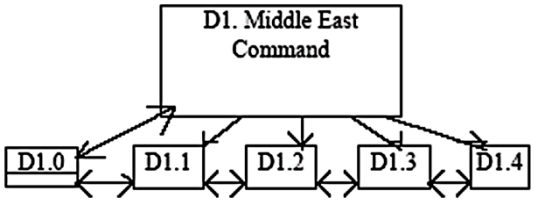

Figure 6. A LEO network with 5 subordinates.

device compromise. If unauthorized individuals acquire the system, it is possible to reverse-engineer some aspects of the firmware and destroy the integrity of the classroom process. However, AI security software will hopefully detect and defeat such attempts [4] (Nyanchama M and Osborn S).

7. Conclusion

Continued research and development of the MS-Ro-BAC device is underway in a private design approach, which includes proprietary software concepts and ideas. The significance of this research is to investigate different areas of RBAC, with the intent of producing a logical proposal that will enhance ability of deployed US military soldiers to seamlessly continue their education abroad. The research has suggested a secure design and architectural framework for a Mobile Secure classroom. The momentous principles of this manuscript are strategic security and information processing in a post 911 environment, where different universities and colleges can work together for the betterment of deployed military personnel. The advantages of implementing a device with such operability would revolutionize the IT industry, and change the way in which we view education in the military community. The MS-Ro-BAC Network will ensure portability and ease of data transfers from different schools on a shared platform. Critical areas of desired research and development are LEO satellite technology that will support Wi-Fi MS-Ro-BAC communication, and a VPN server connection agreed upon by different universities to communicate with all US. Military students around the world in order to achieve their educational goals while deployed [1] (Ferraiolo DF, Sandhu R, Gavrila S, Kuhn R, Chandramouli R) [3] (Greenwald SJ).

8. Acknowledgements

This research was sponsored and conducted by Dr. Terry C. House, in an attempt to bring education to US Military personnel around the world.

REFERENCES

[1] R. W. Baldwin, "Naming and Grouping Privileges to Simply Security," *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, 7-9 May 1990, pp. 116-132.

[2] D. F. Ferraiolo, R. Sandhu, and R. Chandramouli, "Proposed NIST Standard for Role-based Access Control," *ACM Transactions of Information System Security*, Vol. 4, No. 3, 2012, pp. 224-274. http://dx.doi.org/10.1145/501978.501980

[3] S. J. Greenwald, "A New Security Policy for Distributed Resources Management & Access Control," *ACM New Security Paradigm Workshop Lake, Arrow Head*, 2011, pp. 4-6.

[4] M. Nynchama and S. Osborn, "Access Rights Administration in Role Based Security Systems," *Database Security, VIII*: *Status and Prospects*, 2010, pp. 37-56.

[5] G. Neuman, "Design and Implementation of a Flexible RBAC-Service in an Object Oriented Scripting Language," *ACM Workshop on Role Based Access Control*, 2011, pp. 12-18.

[6] R. Sandhu, "Role-Based Access Control," *Proceedings of the* 10*th IEEE Conference on Computer Security Applications*, 20 December 1994, pp. 3-6.

[7] R. Sandhu, "Role Activation Hierarchies," *Proceedings of the* 3*rd ACM Workshop on Role-Based Access Control*, 2008, pp. 11-12.

[8] R. Simon and R. Zurko, "Separation of Duty in Role Based Access Control Environments," *New Security Paradigms Workshop*, 2011, pp. 11-17.

[9] D. J. Thomsen. "Role-Based application Design and Enforcement," *Database Security, IV*: *Status and Prospects*, 2012, pp. 151-168.

[10] S. J. Westfolds, E. Horvitz, S. Srinivase and C. Rouokangas, "A Decision-Theoretic Approach to the Display of Information for Time-Critical Decisions: The Vista Project," *Proceedings of SOAR-92 Conference on Space Operations Automation and Research*, Houston.

