

An Experiment of Reengineering Technology to Support Military Communication in a Strategic Environment

Terry C. House
Nova Southeastern University
hterry@nova.edu

Abstract

This research tested a reengineering approach to achieving Secure RBAC in a dynamic communication environment. In order to defend the United States against enemies foreign and domestic; it is crucial that scientist and combat operators collaborate to create innovative processes from existing technology and implement the best communication equipment available. 21 years technology experience in a military environment supports this research and contributes a collaboration of different systems that could revolutionize the existing government communication process. The Mobile Secure Role Base Access Control Network is a system composed of several other technologies designed to access secure global databases via wireless and wired communication platforms [2]. This research involved the development of a Database network, for wireless vs. wired access connectivity. Forty database access scenarios were tested during day and night hours, for performance analysis. After compiling the results of the experimental process, it was evident that the Iridium Satellite gateway was ineffective as a communication service to access the database in a global strategic environment.

1. Introduction

The “Mobile Role Base Access Control” (MS-Ro-BAC) Approach includes several systems reengineered as a seamless working process to promote an alternative technique to communicating on a global level. This process consists of a single unit system, databases, wireless satellite modems, wired servers and network connections. Each system supports the basic ability of a client to access strategic information from different databases anywhere in the world. [2]. Satellite technology was initially designed to support the National Oceanic and Atmospheric Administration (NOAA). This organization supported two systems of orbiting terrestrial bodies: Polar and Geosynchronous Orbits. The first satellite system known as Television and Infrared Observation Experimental Satellite (TIROS) propelled into space April 1, 1960. Later, the International Telecommunications Satellite Corporation (INTELAT) was founded by 11 nations to monitor the

development and design of global satellite communications systems. Soon after, in April 1965 the first communication satellite, INTELAT-I (Early Bird) was launched into space. This system was capable of carrying 240 voice channels with a life span of 18 years; however, the satellite became inactive after 3 years [8]. Today’s satellite technology is efficient and productive on an international level.

1.1. Satellite processes and background data

The most widely used satellite systems for communications are the Geosynchronous Orbit (GEO) and Low Earth Orbit (LEO) satellite constellation. During this investigation, the Inmarsat and Globalstar systems are the subjects of comparison and analysis for this study. The Globalstar satellite constellation system consists of 48 active satellites and 4 orbiting spares, at a height of 876 miles above the earth. This particular set of LEO satellites orbit the earth at 3.4 kms. Per second; however, the Inmarsat-3 constellation system consists of only five satellites [8]. Each satellite individually covers 1/3 of the earth’s surface at a height of 22,000 miles, while traveling at the speed of the earth’s rotation. Therefore, any satellite placed in geosynchronous orbit would appear from the earth as a stationary object. Two of the most powerful data systems available today are Globalstar and Inmarsat. Each system boast data rates of 56 – 64 kilo bits per second (kbs.), while connected to their various data gateway terrestrial stations [12].

2. Problem statement

The current WiFi approach used in the military, DoD and civilian sector does not incorporate a formal template and model to conduct GEO Satellite data transmission for client/server interaction using a Role Based Access Control (RBAC) interface. Such deficiencies create dangerous latency problems and security vulnerabilities when sending and receiving strategic information in a global setting. This is true particularly in the fight against terrorism, where a mobile global system may be the primary means of secure

communications in a covert and austere environment [4] and [7].

3. Current research significance

A credible standardized framework to access and submit information via LEO & GEO Satellite-ATM TCP/IP networks in a global environment is the relevance of this research. The significant contribution to the field of information technology is the development and implementation of a proven methodology designed to send data in a global client to server, secure RBAC framework. Many global communication systems can benefit from architectural design templates for hardware and software requirements that maximize the data quality and throughput with minimum latency; therefore, reducing the data transmission time and enhancing the throughput of information between the client and server [3].

4. Iridium engineering experimentation

These research experiments involved Iridium satellite technology, in an independently funded laboratory in Fayetteville, NC. The experiments involved 20-year veteran military Special Operations personnel from Fort Bragg NC. Such experimentation proved the Iridium data communication system is incapable of supporting the bandwidth and communication requirements of MS-Ro-BAC Network. In Figures 2, 3 and 4. The results of the experimental tests illustrate the lengthy delay and time response for client server interaction. Figure 4. Depicts the higher quality of service (QOS) during the ‘day hours’ rather than the night. The outcome of the experiments are favorable for daytime transmissions, rather than in the twilight hours. These results represent the overall inefficiency of the Iridium satellite gateway for data communication service [6], [7] and [8].

4.1. Laboratory configuration

Components of the research laboratory consist of various software products: three servers, five desktop nodes, two mobile laptop computers, and two routers with wireless capability, private IP address, two hubs, DSL Internet capability, software, hardware for Inmarsat HSD and Globalstar Satellite connectivity. Each scenario incorporated in the research has become the standard template topology, of how to best use the technology to maximize the quality of service (QOS) over GEO & LEO satellite technology [7]. The researcher is a fulltime professor of computer science and has access to fully

operable technology center if the primary location wasn’t feasible or appropriate for the required experiments.

4.3. Industry engineering support

Design engineers of Iridium technology corporations, as well as US. Army Special Operations Communicators were instrumental in their support for this research [1].

The US Military is currently using Iridium SATCOM technology around the world, particularly in Iraq and Afghanistan; however, the data rate is approximately nine kbs. in addition, the quality of service is poor Professional interviews and real-world experience was very helpful when ensuring the experimentation and analysis process was rigorous and substantiated through the IT industry’s current professionals and end users [8].

4.2. Relational RBAC role inheritance

In Figure 1. The CMDR0 is the base model design for implementing a RBAC system. CMDR1 and CMDR2 both encompass CMDR0’s privileges; however, they both have independent features as well. The CMDR3 design adds the ability of inheritance to the overall model. This indicates roles can inherit permissions from other roles in the data base system as seen in Figure 7 and 8. [5] and [9].

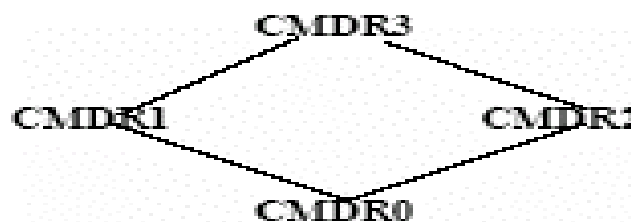


Figure 1. Relationship model of hierarchy

	WIRELESS ACCESS NIGHT				
	min.secs	quality	Errors	Attempts	Totals
Scenario 1	27.300	8.833	0.500	1.167	7.166
Scenario 2	17.700	9.000	0.000	1.333	7.166
Scenario 3	18.700	9.500	0.500	1.000	8.500
Scenario 4	18.310	9.500	0.167	1.167	7.833
Scenario 5	23.400	8.833	0.333	1.167	7.500
Scenario 6	21.800	9.167	0.000	1.133	7.500
Scenario 7	25.240	8.833	1.000	2.000	5.833
Scenario 8	19.600	9.167	0.333	1.333	7.500
Scenario 9	15.300	9.333	0.167	1.167	8.000
Scenario 10	21.170	7.667	0.667	1.167	5.300
AVERAGE	20.852	4.492	0.367	1.263	3.615
MODE	#N/A	8.833	0.500	1.167	6.875
MEDIAN	20.385	9.084	0.333	1.167	6.846
RANGE	12.000	1.833	1.000	1.000	6.680

Figure 2. Wireless ‘night’ data results

WIRELESS ACCESS DAY					
	min.secs	quality	Errors	Attempts	Totals
Scenario 1	19.550	8.833	0.500	1.167	7.166
Scenario 2	18.300	9.000	0.000	1.333	7.166
Scenario 3	21.100	9.500	0.500	1.000	8.500
Scenario 4	19.450	9.500	0.167	1.167	7.833
Scenario 5	23.400	8.833	0.333	1.167	7.500
Scenario 6	21.800	9.167	0.000	1.133	7.500
Scenario 7	25.240	8.833	1.000	2.000	5.833
Scenario 8	19.600	9.167	0.333	1.333	7.500
Scenario 9	15.300	9.333	0.167	1.167	8.000
Scenario 10	21.170	7.667	0.667	1.167	5.300
AVERAGE	21.391	8.492	0.367	1.263	6.815
MODE	N/A	8.833	0.500	1.167	6.875
MEDIAN	20.350	9.094	0.333	1.167	6.848
RANGE	8.940	1.833	1.000	1.000	6.686

Figure 3. Wireless 'day' data results

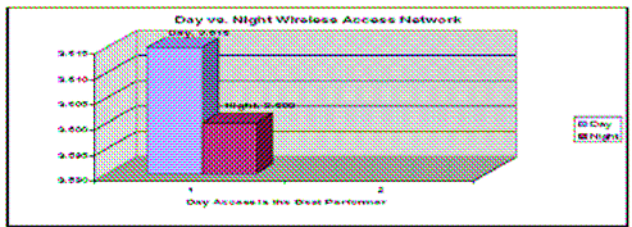


Figure 4. 'Wireless day vs. night,'

5. Summary of iridium reengineering

This research tested a different approach to Secure RBAC in a post 911 environment. In order to defend the United States against enemies foreign and domestic; it is crucial that combat forces are equipped with the best communication equipment available. 21 years technology experience in a military environment supports this research and contributes an ideology that could revolutionize the government communication process [5]. The "Mobile Secure Role Base Access Control" (MS-Ro-BAC) Network is a system designed to access secure global databases via wireless communication platforms [2]. This research involved the development of a (MS-Ro-BAC) Database, for wireless vs. wired access connectivity. Proprietary software was developed for authenticating with the server system. 40 database access scenarios were tested during day and night hours, for performance. The Iridium Satellite gateway was ineffective as a communication service to efficiently access the database in a global strategic environment. "in press. [6]."

5.1. Current Inmarsat & Globalstar research

The current research goals are to develop a standardized template and model to initiate data communications between a secure mobile-client and database server by satellite network. This investigation attempts to abstract the most efficient topology design and to maximize bandwidth and quality. By conducting comparison analysis research via the

Inmarsat and Globalstar technology, measurable data and results can ensue; thus, supporting the international community with reusable models and templates for any satellite-ATM system to send and receive data in a global environment [13]. Because of the various implementation techniques to mobile connectivity using GEO & LEO satellite data communications, the quality and throughput of either technology can possibly improve through rigorous testing and implementation techniques.

5.2. Research inquiries

Current experiments will satisfy a minimum of five questions in response to section II of this manuscript: 1. what is a credible standard for the client and server database configuration. 2. How will the client interface appear to the user while interfacing with the database? 3. What architectural model is used for hardware and software compatibility analysis? 4. What standard template(s) will measure the quality and throughput of each system? 5. What are the test scenarios for measuring the quality of GEO & LEO data communication system of the 21st Century? "in press. [13]."

5.3. System components and processes

The system case is 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 MEO satellite connectivity [12]. 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 with trusted personnel only. The immediate contribution to the computing community is the ability of this device to connect fellow users in an ad-hoc global network environment. To contact higher-level individuals, the lower level user can set flags for senior users to contact them in a hierarchical structure [13]. 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 [9].

5.4. The reengineered Interface device

Figure 5. Illustrates the MS-Ro-BAC device physical connection 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 MEO 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 MEO network and successfully authenticated their systems hardware and software. After a satisfactory handshake, the secure connection allows for a client-server exchange of data [6].

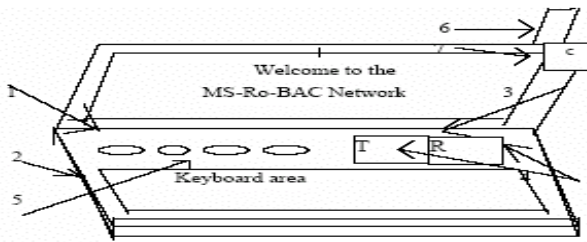


Figure 5. MS-Ro-BAC network device

This device has three modes: (1) Deployed independently for MEO satellite connectivity from any location in the world. (2) Configured for normal unsecured use not connected to a wired or wireless network. (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 7. Illustrates how each device activates and automatically authenticates through inheritance of junior roles where access is lower than the requestor’s clearance levels. Once initiated, the R-BAC infrastructure, the main DISCOM in Washington DC

is “Big Brother” (BB). Management of lower DISCOMs is the job of lower ranking Controllers. BB has authority over every DISCOM and its individual users. BB can 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 leaders. In Figure 7. Washington

user must submit a thumb and retina scan, and 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. After completing the system authorization process, the user will receive a graphical user interface that depicts all activated MS-Ro-BAC devices. “in press. [6].” Standard graphics and data come standard on every machine to decrease the message size, redundancy and increase the bandwidth speed during transmission [9].

5.5. Communication and authorization process

Figure 6. 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 [6].

The access control relation is then simply the composition of these relations:

$$AC := PA \circ UA,$$

i.e.,

$$(u,p) \in AC \iff \exists role \in Roles: (u, role) \in UA \wedge (role,p) \in PA.$$

To further reduce the size of these relations and support additional abstraction, RBAC also has a notion of hierarchy on roles. Mathematically, this is a partial order \geq on the set of roles, with the meaning that larger roles inherit permissions from all smaller roles. Formally, this means that the access control relation is now given by the equation

$$AC := PA \circ \geq \circ UA,$$

Figure 6. RBAC Inheritance formula [8].

The proprietary software instantly reads the RBAC information of other devices and places each device in the hierarchy structure in which they have access. Therefore, if four users logged in and the head Governor (D1) was not there, each user becomes a peer-to-peer connection. In a MS-

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 [3].

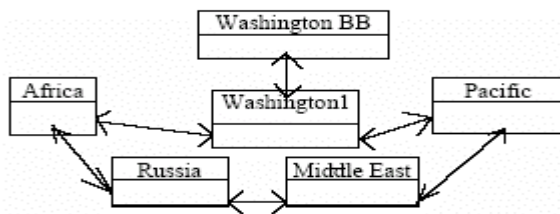


Figure 7. B. Brother Conferencing with controllers

6. System hardware and software

The MS-Ro-BAC Device will include various types of proprietary middleware, firmware and authentication programs to ensure file transfers are secure. Each device incorporates a retina and finger print scanner to identify the device user. 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 senders of secure 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 [3].

The software allows the senior most roles to acquire the permissions of their junior users. However, this ideology extends beyond inheritance of permissions. 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]. 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. Washington [9] and [7].

Figure 8. Illustrates the Middle East DISCOM and four local stations within its command sector. *D1.0* is an instance of *D1*. In the diagram, a one directional arrow symbolizes the ‘no write up’ rule for preventing covert channels to unauthorized devices: *D1*. There is a two-way communication channel, depicted by a two-headed arrow, between *D1* and its instance *D1.0*. This illustrates the

required procedure for *D1* to receive information from subordinate objects. Objects *D1.1*, through *D1.4* are examples of other countries in theatre: Iraq, Iran, Kuwait and Jordon [4].

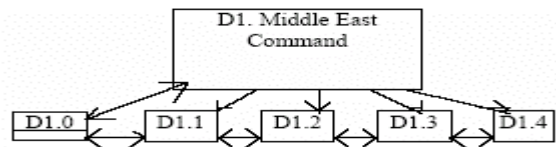


Figure 8. A MEO network with four subordinates.

6.1. Reengineering advantages

At the time of this manuscript’s publication, there is not a communication system and network, which provides the operability of the Mobile Secure Role Based Access Control Device. The conventional and Special Operations community has not incorporated such a device as well. There are existing systems that support one or two aspects of the MS-Ro-BAC implementation; however, they are not capable of instantly linking individual users in a Virtual Private Network around the world. This device will not require a constellation of new celestial bodies; it will correlate with existing government MEO or civilian network satellites that are presently in orbit [11]. Information security through hardware and software authentication provides a sound way to ensure only authorized devices can receive and send data. The MS-Ro-BAC Device incorporates AI biometric systems to maintain the integrity of the authorized and unauthorized users [4].

6.2. Reengineering disadvantages

The negative aspects of the MS-Ro-BAC system do not over-shadow the positive advantages of providing crucial information around the world in a timely manner. Lack of financial support will prohibit the adoption and full development of the global accessible system. The government’s desire for a new system to perform the task that four separate machines can presently accommodate, may not be feasible. Funding has always inhibited the progress of new evolving technology [7]. Another disadvantage is poor reception during electrical storms or the absence of a 24 hour satellite ‘foot print’. Such problems could prove disastrous for field agents or military maneuvering units. The required bandwidth and throughput to support the MIS-Ro-BAC Device would degrade the current satellite’s ability to support their existing communication tasks. Most importantly, if unauthorized individuals acquire the system, it is possible to freeze the current state of all registers and reverse-engineer some

aspects of the hardware and obtain classified information. However, AI security software will hopefully detect and defeat such attempts [11].

7. Conclusion

Continued research and development of the MS-Ro-BAC device is currently in progress, which includes proprietary software program design and testing. The significance of this research was to investigate different areas of RBAC, with the intent of producing a comprehensible proposal that will enhance the transmission and reception of information in a timely manner. The research has suggested a secure design and architectural framework for a Mobile Secure RBAC Device. The momentous principles of this manuscript are strategic security and information processing in a post 911 environment. The advantages of implementing a device with such operability would revolutionize the IT industry and secure combat forces and Department of Defense employees around the world. The MS-Ro-BAC Network will ensure portability and ease of data transfers within overt and covert government organizations or private corporations on a global scale. Critical areas of desired research and development are MEO satellite technology that will support Wi-Fi MS-Ro-BAC communications and a visual system for private viewing of classified information while in a non-classified environment [5], [7] and [11].

8. References

- [1] R.W. Baldwin, "Naming and Grouping Privileges to simply security" *Of the Symposium on Security and Privacy*, IEEE Press, Los Alamitos, Calif, 2002, pp. 116-132.
- [2] D. F. Ferraiolo, R. Sandhu, R, and Chandramouli. Proposed "NIST Standard for Role-based Access Control", *ACM Transactions of Information System Security*, , August 2001, Vol. 4, No. 3, pp. 224-274.
- [3] S. J. Greenwald. "A New Security Policy for Distributed Resources Management & Access Control", *ACM New Security Paradigm Workshop Lake Arrow Head CA*, 2001, pp. 4-6.
- [4] T.C. House, "An Analysis Format for Client-Server Performance Using GEO & LEO Satellite Networks (Inmarsat vs. Globalstar)" *Proceedings of the IEEE CISSE Conference TeNe05*. December 10-20, 2005.
- [5] T. C. House, Mobile instant secure role base access control (MIS-Ro- BAC) network, Presentation track C: *Proceedings of the IEEE Annual computer security application conference*. March 2004.
- [6] T. C. House, "Client Server Access: Wired vs. wireless LEO satellite-ATM connectivity; a (MS-Ro-BAC) experiment" *CIS 2005, Part II, LNAI 3802, IEEE*. pp. 719-724, December 2005.
- [7] T. C. House, "Mobile secure role base access control device", *Proceedings of the IEEE SoutheastCon: Mobile devices and communications track*. 2005, pp. 542.
- [8] M. Nynchama and S. Osborn. "Access Rights Administration in Role Based Security Systems". *Database Security, VIII: Status and Prospects*, 2000, pp. 37-56.
- [9] G. Neuman. "Design and Implementation of a Flexible RBAC-Service in an Object Oriented Scripting Language" *ACM Workshop on Role Based Access Control*, 2001, pp. 12-18.
- [10] Robert A. & Nelson, P.E. "President of satellite engineering research corporation". *Interview with a satellite engineering consulting firm*, Bethesda, MD. 23 April 2005.
- [11] R. Sandhu. "Role-Based Access Control", *Proceedings of the 10th IEEE, Conference on Computer Security Applications December 20*, pp. 3-6.
- [12] R. Sandhu, "Role Activation Hierarchies", *Of ACM Workshop on Role-Based Access Fairfax VA*, 2001, pp. 11-12.
- [13] R. Simon, And R. Zurko. "Separation of Duty in Role Based Access Control Environments", *New Security Paradigms Workshop*. 2001, pp. 11-17.
- [14] D. J. Thomsen, "Role-Based application Design and Enforcement", *Database Security, IV: Status and Prospects*, 2002, pp. 151-168.
- [15] S. J. Westfolds, E. Horvitz, S. Srinivase, 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*, 1992, pp. 19-21.