Global Information Assurance Certification Paper

Centralized management of users, access rights and security policies for call center applications in a mobile telecommunications operator's organization

Name: Corradino Corradi
Assignment Version: 1.4

Abstract

With the growth of mobile phone subscribers and GSM/GPRS services a large number of employees (especially call center operators) are supporting the customers using applications in a heterogeneous computing environment.
IT and Security departments of our organization are wrestling with the challenge of managing secure access to information and applications scattered across a wide range of internal computing systems. Furthermore, they have to provide access to a growing number of users (employees, contractors, consultants, temporary staff) without diminishing security or exposing sensitive information.
The management of multiple versions of user identities across multiple applications, the high-level employee turnover, the use of external staff for short periods of time (Christmas and summers promotions) makes the task even more daunting.
We achieved the goal of improving security and simplifying account management processes using an enterprise security management tool that can 'talk' to each platform from a single console and remote "tailored" agents. The identity management system provides a solid base for our call center organization's role-based access control; the security administrator can easily manage account and user rights and has more time to tighten security.

Description of the problem

In our large call center organization (more than 5000 people) we had a number of servers working on different platforms, each with its own administrator. In such an environment, setting up user accounts is a time-consuming process invariably accompanied with onerous paper work and large Excel files. Employees may require access to different applications, documents and data on each network's resources. In a worst case scenario, this could mean that new employees and contractors have to either wait for the appropriate access rights and user accounts to be set up by individual departments, or 'borrow' someone else's until theirs is ready.

The second solution has serious security implications. Users should only have their own ID but once allocated, the other 'borrowed' ID is often left in place. This leaves systems wide open to abuse.

Security literature reports that 80 per cent of data theft is generated from within an organization and not, as many fear, as a result of a hacker infiltrating the system; our company is not an exception.

A few call center applications are "sensitive"; there are special call center accounts with the power to visualize customers credit cards, assign points in loyalty systems, assign small amounts of money to customers with prepaid cards, see the historical traffic not older than three months.

A further problem arises from the security problems raised by contractors, consultants and temporary staff. We use a lot of consultants during the development and maintenance phases of IT projects and we use temporary staff during the campaigns to promote new services (like Multimedia Message System or wireless remote access to corporate networks).

How many former contractors and ex-employees still have valid IDs on company systems months (in some cases years) after they have left the organization? It can take weeks - even months - for the individual administrators to revoke these access rights and sometimes they are considered such a low priority matter that they are put to the bottom of the queue and then forgotten.

The following is a list of the applications that IT administrators and call center operators must access to perform their job:

- Operating system: Solaris, UP-UX, UNIX Digital
- Database: Oracle
- Legacy applications

Each application has its access control mechanism and specific non-sharable procedures.

To better control our call center systems, enhance the overall state of security and minimize system administrator workload we decided to start the identity management project for all call center accounts. We chose a step-by-step approach; the project has the following main phases:

1. User profiling and centralized control of user accounts
2. Password reset and password synchronization functionalities, extending user profiling to less critical systems
3. Single Sign On (SSO) and integration with the company's PKI

Here is a short description of the phase one requirements:

- Role-based access management
- Centralized access control
- Scalability across multiple platforms
- Centralized Security Alerts
- Audit and History Tracking
- Compliance with Italian privacy law (law 675/1996)
- Use of non-intrusive agents
- Agent already available for the most common platform (win2000, UNIX dialects, Oracle)
- Strong API and 4GL language for development of a tailoring agent or "general purpose" agents
- Support for password synchronization/reset
- Support for authentication tools, such as tokens and biometrics systems

- Security events notification by SMS or e-mail
- Secure communications: whenever possible centralized client and remote console must communicate in a secure way using a crypt channel

Here is a short description of the phase two requirements:

- Users must be able to reset their own passwords and unlock their accounts without the aid of a help desk. A user accesses a password reset application through a standard browser and/or a Windows client. In the first phase an access through a telephone (interactive voice response) is not necessary. Users must be authenticated by a set of questions to which only they should know the answers.
- Users must know just a single password across different systems and applications, reducing the chance that they'll forget one or more passwords.

Here is a short description of the phase three requirements:

- Users must have a single userID and password to access different systems and all call center applications

At the moment all the project one milestones have been completed (feasibility, analysis, development, test, deployment, maintenance); both my company and BMC have released the system in production and a 24x7x365 SLA has been defined and signed.
Project phase two has “passed” the feasibility milestone and the IT department is writing the functional requirements.
Project phase three is in feasibility; before we start the analysis a thorough review of the results of phase two will be needed; it will also be necessary to perform a new cost-benefit analysis.

Description of the solution for phase one

For the first phase, after defining the system requirements, we put out a tender for the identity management solution based on our requirements to the major Italian security companies. We tested the winner solution for a subset of our system (UNIX operating systems, Oracle databases); we signed a contract with the vendor not only for the installation and deployment of the tool but also for the agent customization and the training of users and administrators.

Identity management products with password self-service reset and password synchronization are offered to us in a wide range of options. The following are among the solutions that we recently evaluated:

BMC Software's (www.bmc.com) Control-SA provides user provisioning and role-based access control. Through a Web interface, users can request changes to security entitlements and manage, synchronize and reset passwords.

Tivoli (www.tivoli.com) offers Identity Director, a policy-based identity management suite that includes self-service password reset and synchronization.

PentaSafe (www.pentasafe.com) offers VigilEnt User Manager/ Password Manager, which includes password synchronization and reset functions. It runs on NT/2000 servers and deploys agent technology for password reset and synchronization across multiple platforms, including NT/2000, Unix, AS/400 midrange systems and Netware.

CA (http://www.ca.com/) eTrust Admin provides easy and cost-efficient administration of users and resources across enterprise security systems and directories. This powerful software solution simplifies the administration of complex environments, including Oracle, Active Directory, NT, Unix, NDS, Microsoft Exchange, and more.

Evidian (http://www.evidian.com) AccessMaster PortalXpert provides end-user access to all authorized resources with only one login name and password (Single Sign-On). When a user accesses a Web application that requires authentication, he does not need to supply authentication information himself. Instead, and on behalf of the user, PortalXpert provides the Web server with the user name and password requested by the application, without any modification of the Web application. AccessMaster security server is available on Windows NT 4, Windows 2000, Solaris 2.7, Solaris 2.8, and AIX 4.3.

During the feasibility step, from the beginning we discarded the idea of using web based SSO tool -- such as IBM Tivoli's Policy Director (www.tivoli.com), Netegrity's SiteMinder (www.netegrity.com), Entegrity's AssureAccess (www.entegrity.com), RSA Security's ClearTrust (www.rsasecurity.com), Oblix's NetPoint (www.oblix.com), Baltimore Technologies's SelectAccess (www.baltimoretechnologies.com) and Entrust's GetAccess (www.entrust.com) -- because a lot of critical call center applications are client/server and a few of them use proprietary user/right systems with a poorly documented API.

The product chosen was BMC Control-SA because it was the one that met almost all our requirements and was evaluated as offering a good balance among security, cost and business needs.

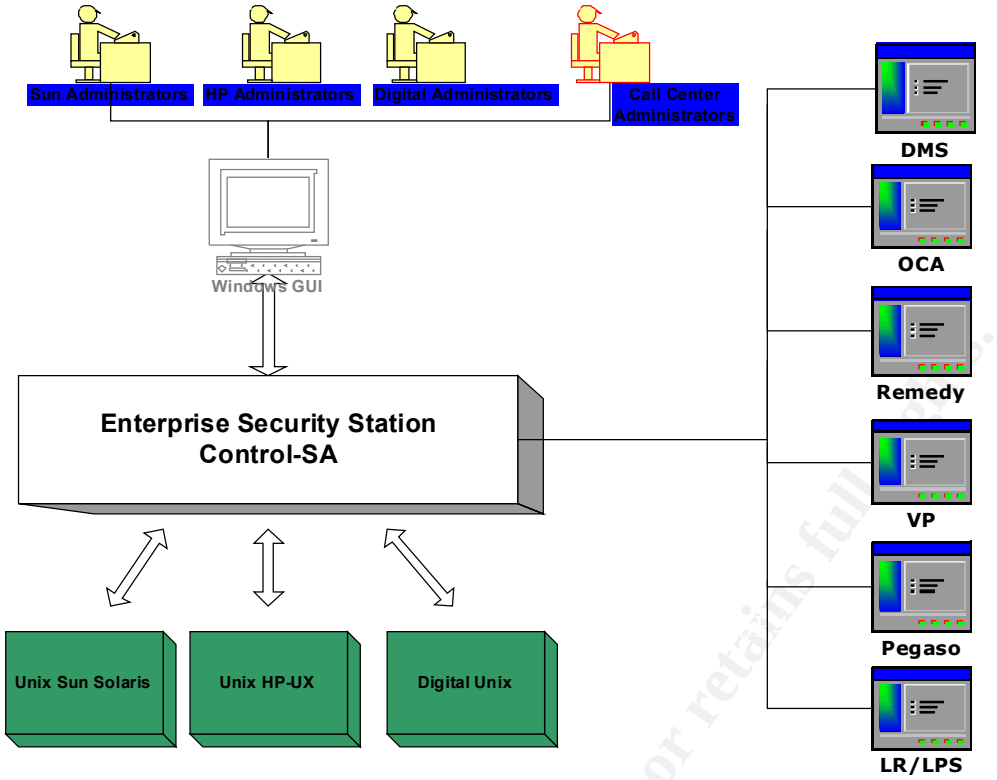
The CONTROL-SA server, with its central security repository (ESS), is the central point of control over managed security systems throughout the enterprise. CONTROL-SA/Agent software modules communicate between the CONTROL-SA server and the user databases of enterprise platforms and applications, providing real-time synchronization.
From the CONTROL-SA GUI, security administrators can monitor, control and audit authorized access to all managed systems.
Definable job-code entities represent groups of internal and external users that share similar business roles. Each entity (Enterprise user) consists of a set of cross-platform authorizations required for performing a specific role. Associating a user with a specific job code instantly produces user setup for resource access

privileges, leading to increased productivity. Role-based management automatically initiates immediate, accurate user agreements while providing a tightly controlled security environment.

Control/SA System architecture and settings

The Central Control/SA EES system is installed on a Sun V880 server running on Solaris 8 OS; EES uses an Oracle 8.1.7 RDMS.
The ESS system is installed in the internal production LAN and is protected from call center, development and test networks by a Checkpoint FW-1 firewall (http://www.checkpoint.com); ISS Realsecure NIDS sensor (http://www.iss.net) checks pattern signatures in production LAN.
F-secure Antivirus (http://www.f-secure.com) is installed on the ESS system and all servers that host call center applications.
Sun and Oracle have performed the hardening of EES servers (close or remove not necessary services) according to BMC requirements.
After a cost/benefit analysis we decided to use a standalone server and not a HA solution, however the critical components of the Control/SA server are redundant (CPUs, disks in RAID 1) to avoid single point of failure.
We have installed a HP Vantage Point system management agent (http://www.openview.hp.com) and a Legato NetWorker back-up agent (http://www.legato.com) on the EES system. An incremental backup of the server is done daily; a full back up is done weekly.
The installation of Control/SA was straightforward: to get EES and AIT agents up and running took 2 days.
Control/SA licenses are not related to the number of agents installed but are related to the number of platforms supported (Win, UNIX, Oracle); this policy reduces the cost in environments with applications distributed over a lot of servers.

Control/SA AIT agents are installed on a Win2000 SP2 server; data exchange between control/SA server, “broker” AIT agents” server and remote call center systems (Remedy, VP, DMS, etc) is handled by Oracle sqlnet and RPC calls.
The data exchange between Control/SA central system and administrative console is crypted using the BMC proprietary cryptographic solution.
After a risk analysis process we identified the following call center applications as the most critical from the security point of view: prepaid GSM SIM vouchers validation platform (VP), Customer Care and Billing System (CCBS), front-end for customer base (OCA), Document Management System (DMS), loyalty system (LR), crediting system (Pegaso), trouble ticketing system (Remedy).



All these systems have proprietary mechanisms to manage users and user rights; therefore we developed 6 AIT agents using the Control-SA Links tool, based on TCL scripts).
At the beginning we inserted 3 administrative profiles in the system and we created 14 user profiles (UNIX administrators and DBAs), then we loaded all the call center users in the system using a dump of the Human Resource database. BMC created scripts for bulk operations.
For call center applications we created one call center administrative profile and 9 user profiles; we enabled the auditing functionality of Control-SA to log at least the administrator's activities.
We configured the system to handle at least two bulk operations at year (Christmas and summer period) to enable a large influx of external staff (more or less 1000 people) for a short period.
We created reports that showed us account type vs. application, attributes time vs. application, list of all accounts with idle time longer that three months, list of suspended and deleted accounts, list of accounts that have a different status (not synchronized) in different applications. The reports helped the Control/SA administrator during system and application troubleshooting and call center managers during the control of user accounts and call center activities.
The development and rollout phase of the project took 5 months; the implementation team met the deadline, but not without some difficulty. The main complication found was the development of tailored agents for our legacy system. For a few subsystems the development of the agents was related to proprietary API, this mean that the middleware had to be realized together with the tool supplier just to respect the contract and have the necessary maintenance.

We also found a problem during definition of the different statuses supported by the call center applications (user active, deleted, duplicated, suspended, pending or waiting an authorization). VP doesn't support the suspend account; which means that if we decided to suspend an account on Control/SA, the command is propagated to all the agents that support the functionality but it is not possible to execute it in VP because it has no correspondence on the system.
If it is necessary to suspend an account pending authorization before reactivating it later, and the call center application supports the "active" and "deleted" states but not "suspended", rather than create inconsistencies, we preferred to have the suspend operation in the systems including it trigger an error message. In this way, with the "suspend account" command sent by the central system to peripheral systems, we will have a subset of the systems in which this command is executed correctly and another subset of systems in which the accounts remain active; for the latter, a suitable error message is displayed by the system for the Control/SA administrator.
User status vs. central system commands is still an open issue and has pros and cons that need to be evaluated each time system by system.

Results of phase one

The administrator really appreciates the possibility of registering users on the different systems and associating with the Enterprise User a specific Job Code in a single mouse click. Besides the possibility of modifying a job code and automatically changing account of all Enterprise users connected to this Job Code considerably reduced the time spent by system administrators in managing users and user rights.
Nevertheless, even if the control/SA console is available for all system administrators, sometimes UNIX admin and Oracle DBA still use the old command and exploit only a subset of the functionalities of the security enterprise console.
The time spent in the integration among system helps our company, particularly the IT and Customer Services departments, to understand each other's needs better and improve the infra-department process and information flow.
After 3 months we performed a security assessment of user accounts for all call center applications; we noticed that applications migrated under Control/SA central console have no more idle or inactive accounts. Applications not part of Control/SA still have a lot of unused accounts or have accounts without user attributes.
During the Control/SA settings we spent some time importing user attributes from external sources; even if the tool is flexible, it lacks an easy data import functionality ; together with BMC developers we created a few scripts to fix this problem.

After a few months of service operation, we have no system down time; Control/SA uses Solaris and database resources in the right way.
For the release of new features in call center applications we created specific accounts; Control/SA administrator suspends these accounts only after a successful drop in production of the new functionalities; in our company we have a major installation in production every two months.

Lessons learned:

- Security is a process and not a product; the use of an enterprise security tool in a large organization is not just a technical issue, it fits into the culture of the organization
- 80% of the time spent during the project was dedicated to the understanding of access and user mechanisms of legacy systems and to the development of tailored specific accounts; to avoid reworking and reducing the lifecycle of software development it is important to insert security requirements in all the company projects right from the beginning.
- More than "sensational new features" a security management system must be able to interface easily with other applications through strong APIs and easy to use programming language; the development of a tailored agent was faster for legacy systems with well documented APIs and a user management system based on RDMS tables
- Creating an authorization logic that spans a heterogeneous enterprise requires a thorough understanding of how business flows through the organization. This is best done through use cases. In simple terms, this means sitting down with users representing various business roles and documenting workflow.
- An enterprise security management tool has bugs and requires support; it is important to select a supplier taking into consideration the maintenance activities, the availability of local technical support and mother tongue help desk, the speed in release of a hot fix or customized solutions.

Feasibility and functional analysis for phase two

To complete the work done in phase one it is necessary to roll-out password reset and password synchronization functionalities and complete the training of end users and administrators.

We create Control SA AIT agents for the remaining (less critical) call center applications: customer contact management (CCM), credit card system (CCS), Phone Lock (system used by call center operators to block stolen mobile phone IMEI), on line services back-end system.

Modules that may be added, such as SA-Workflow, increase the usability of this software by providing a web-based interface that will allow departments or individual users to request changes. These may be for new user IDs or for

applications that they do not presently have access to. The requests go to a designated person and if these changes are authorized, control/SA may be utilized to provide the new permissions, which then flow back to the users. Where requests are not answered within a specified time limit, the request will be forwarded to the next person or department administrator on the Workflow list. This ensures that the process runs smoothly with as little delay as possible.

Feasibility for phase three

SSO can be considered a step up from password synchronization, nevertheless SSO implies a drastic change to a company's existing IT infrastructure and cost. To have a successful evolution from Control/SA to a more powerful and complex SSO infrastructure we are investing time in architectural analysis and design.

To understand how to integrate Control/SA and SSO we considered the key architectural elements of our IT infrastructure for users and user rights:

- Legacy data integrity, Data relationships, LDAP schema and namespace design
- Middleware components, Back-end security systems integration, Control/SA integration

A first analysis of applications that will come under the SSO umbrella will reveal common data elements and authorization decisions (Enterprise user attributes); to integrate these application in the SSO system, we need to extend our LDAP schema and directory service repository based on Baltimore technology (http://www.baltimore.com).

Control/SA AIT agent development showed how important it is to create standard interfaces. Like Control/SA, many SSO solutions provide security APIs to enable applications to invoke security functionality beyond what you get out of the box. But these aren't standard APIs. More importantly, the application itself will be bound to that API, so the application code must be rewritten if one SSO solution is replaced with another, or if the application/platform is upgraded to a new release.

Creating an application isolation layer via standard interfaces will reduce the need for costly and time-consuming re-engineering by shielding applications from vendor-specific code. An extension to the Java security model called Java Authentication and Authorization Service (JAAS) and Security Assertion Markup Language (SAML) addresses this issue.

Java Authentication and Authorization Service (JAAS) enables developers to implement authentication and access control functionality while minimizing vendor-specific coding within the application. This will allow customers to switch SSO vendors and/or upgrade their applications or platforms without extensive recoding. IBM/Tivoli and Netegrity already provide support for JAAS.

SAML is being sponsored by the Organization for the Advancement of Structured Information Standards (OASIS); it defines a common language for describing authentication and authorization "assertions.". Netegrity released a Java-based SAML developer toolkit called JSAML.

Almost all web based call center applications developed in my company use BEA's WebLogic Enterprise edition; this application server has is own native authentication and authorization security mechanisms. However, these mechanisms can only be leveraged by the applications written on the application server platform. Thus, other platforms, such as client/server and legacy systems, would still need to be secured and managed by yet another security solution. Application server authentication and authorization must be employed by SSO products to provide granular access control out of the box. Our goal is to integrate the application server's security system with an SSO solution to have in the end one centrally managed, policy-based security solution that allows a security policy to be applied and managed across Web-based, client/server and legacy applications. Examples of this kind of integration compatible with my company infrastructure are between Entegrity's AssureAccess and RSA's ClearTrust SecureControl's with BEA's WebLogic application server.

Other SSO feature that we are going to analyze before concluding the feasibility of project phase three are:

- Handling multiple authentication options (e.g., user ID/passwords, digital certificates, authentication tokens)
- Support for several types of user repositories (LDAP, RACF, NT, etc.)
- Offer auditing services and intuitive Web-based interfaces for user and resource management
- Integration between SSO solutions and complementary security solutions such as intrusion detection solutions (e.g., ISS Real Secure, Tivoli Risk Manager).
- Increased functionality for delegated administration and password management.

Here is a list of products that we are going to evaluate:

- Computer Associates' eTrust Single Sign-On (www.ca.com)
- Passlogix's Single Sign-On (www.passlogix.com)
- Blockade Systems' Web Single Sign-On (www.blockade.com)
- Netegrity SiteMinder (www.netegrity.com),
- RSA ClearTrust Secure Control (www.rsasecurity.com)
- IBM Tivoli Policy Director (www.tivoli.com).

Conclusions

Using an identity management tool based on a security enterprise system helped my organization to:

1. Increase internal customer satisfaction because it reduces the time necessary for creating/modifying call center accounts and user rights/roles
2. Provide greater security both in prevention and detection activities because there is only one centralized console to handle all accounts for all applications and a centralized log system where all security events are stored;
3. Reduce security breaches because manual error and intervention are minimized and user access security policies enforced
4. Reduce the maintenance and support costs associated with user accounts, profile definition and access rights, because it automates routine management tasks and frees your IT staff to concentrate on larger problems
5. Increase integrity and confidentiality of the data exchanged between the client agent and the central system during authentication and authorization
6. Provide a stable security framework that can be used for integration with other security systems (PKI, strong authentication)

Acronyms:

API	Application Program Interface
DBA	Data Base Administrator
GSM	Global System for Mobile communications
GPRS	General Packet Radio System
IMEI	International Mobile Equipment Identity
NIDS	Network Intrusion Detection System
PKI	Public Key Infrastructure
OS	Operative System
RDMS	Relational Database Management System
SLA	Service Level Agreement
SMS	Short Message System
SSO	Single Sign On
VP	Validation Platform

References:

1. Rutrell Yasin. “Password Pain Relief: Self-service reset and password synchronization products reduce the burden and cost of help desk calls”.

Information Security Magazine April 2002. URL: http://www.infosecuritymag.com/2002/apr/cover.shtml
2. Rutrell Yasin. “What Is Identity Management?”. Information Security Magazine April 2002. URL: http://www.infosecuritymag.com/2002/apr/cover_casestudy.shtml
3. “Product Review: Control-SA”. Secure Computing Magazine February 2000, URL: http://www.westcoast.com/securecomputing/standalone/bmc/sc_controlsa_uk.html
4. BMC web site, Product description, “Control-SA”, “Control-SA Links”, “Control-SA WorkFlow” URL: http://www.bmc.com/products/proddocview/0,2832,19052_19453_22855_1587,00.html
5. Scott Sidel. “New security information management (SIM) products help you keep track of your "theater of operations"”. Information Security Magazine January 2002. URL: http://www.infosecuritymag.com/2002/jan/features_command.shtml
6. Russell L. Jones. “EAM ain’t easy”. Information Security Magazine January 2002. URL: http://www.infosecuritymag.com/2002/jan/features_eam.shtml
7. Scott Barman. “Writing Information Security Policies”. New Riders Publishing. November 2001. ISBN: 157870264X.
8. Russ Housley, Tim Polk . “Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure”. John Wiley & Sons. March 2001. ISBN: 0471397024
9. Julia H. Allen. “The CERT Guide to System and Network Security Practices”. Addison-Wesley Pub Co. June 2001. ISBN: 020173723X
10. Bruce Schneier. “Secrets and Lies: Digital Security in a Networked World”. John Wiley & Sons. August 2000. ISBN: 0471253111