Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 3 (2011) 801–804

Procedia Computer Science

www.elsevier.com/locate/procedia

WCIT-2010

Password management diffuculties in system and network management

Temuçin Huseyin[a*], Erzurumlu Kerem[a]

[a] *Hacettepe University Computer Engineering Department, 06532 Ankara, Turkey*

Abstract

In this paper, password management problems of network and system management will be handled.
In this concept, password management and its usage in systems and networks will be introduced. Then password management problems that occurs in such situations like employee change, internal or external password distribution, will be investigated. In this paper the determination of password management problems will be done and these problems will be introduced.

Keywords: Password Management, System and Network Management, Problems of password management, Centralized Password Management

1. Introduction

Corporations have to use software and hardware security policies to protect their systems and networks from miscellaneous threats. These threats can be caused by either authorized or unauthorized people. In network and system management; providing a secure connection for authorized employee to system and network devices with his authority, and protecting devices from unauthorized access is defined as user authorization. User authorization in multi-user systems is provided by user passwords which is associated to users or user groups. Passwords have different authorization levels depend upon associated user in system and network, and they are managed by password management systems. Password management systems are specialized and depend on the system's and device's hardware software features.

Password management softwares are assigned to provide security on login operations and store/manage passwords securely within operating system. Password management software provides services below [1] :

- Updating system passwords periodically
- Protecting passwords (Encryption, Backup etc.)
- Providing passwords to IT personnel, service and other applications.

In Unix and Linux family operating systems, the user "*root*" has all authorizations in system and can implement any operation on system without prevention. "*Administrator*" is equal to "*root*" in Microsoft Windows family operating systems. These kind of users are described as super users[2]. Similarly, database administrators(sysdba, dba etc.) have full authorization on databases[3].

Generally, besides the systems above, operating systems, DBMSs or network devices include a super user login and after this login super user has limitless, most of the cases uncontrolled power on system so he can apply

* Temuçin Huseyin. Tel.: +90-312-2977500; fax: +90-312-2977502
E-mail address: htemucin@cs.hacettepe.edu.tr

1877-0509
doi:10.1016/j.procs.2010.12.131

updates on system, can manage users, or change device configurations[4].

2. Password Management Difficulties

As described above, super users has limitless authority in the system they logged in. The IT personels and applications require super user privilege for system and network routines such as user management, debugging operations, updating and upgrading operations.

System administrators are responsible for system's accuracy and persistence, by managing hardware, network components and softwares which works on these components. These responsibilities makes it necessary to give system administrators super user privileges.

There are two ways to give system administrators super user authorities. First approach can be described as password sharing, that all system administrators share unique root password. With this method system administrators use root/Administrator user name, password pair to login for operations. Second approach can be described as separated user authorization. In this approach, each system administrator, more generally system power user, has own user name and password pair and these pairs are defined in each managed system. Then the IT manager defines each user's privilege in each system indipendently. In this way, super user password is not shared and system management operation continues. Separated user authorization is provided with "sudo" command in Unix/Linux and "Active Directory" in Microsoft Windows family operating systems.

Sharing super user privilege via passwords is required for system persistence but brings some password management problems. Paper's following parts will discuss these problems.

2.1. Employee Change Difficulties

Big companies and corporations networks' has a big number of users that works on systems which are distributed on many network devices and servers. These kind of systems cannot be handled by one system administrator alone. Commonly, a group of system administrators manage system and network in IT centers.

This team work is an advantage with the scope of distribution of duty. But this advantage turns to a problem that has to be handled when a member moves to another department from IT or quit company. This user's super user privilege must be revoked and this is essential for system security.

If super user privilege is provided via super user password sharing, hence the super user privilege is obtained by password of super user, revoking of super user privilege from a user means that stopping super user password's share with this user. This operation requires changing concerned password from all associated servers, database systems, network devices and operating systems. Also system have to be checked totally if diverged employee left any back door in system.

Since super user password is changed to obstruct diverged user login to system, new password must be unpredictable by this user. In this respect, new password's distribution and learning by remaining system administrators process is an another problem. These problems occur when a new member joined to group also[4].

In the case of super user privilege provided via separated user authorization, revoking a system administrator member from administrators group will result of user deletion from all associated devices and systems. These means username and password of the employee must be deleted from all active network devices, servers, operating systems and database systems which he is authorized. Similarly, when a new member joins to the administrator group, his user name and password must be added to all devices and systems that he is authorized.

Both cases which are described above requires configuration in systems' hardware, software and active network devices, no matter the situation is. Also some configurations can be skipped by fault in this "batch configuration" process, which will cause a serious system threat. Also super user password(s) can be confused by personnel when frequent employee changes occurs.

Thereby, inter-department and inter-corporation personnel changes gather serious extra loads for system administrators and password management systems. These routines' frequently repeatings may increase forgetting/skipping faults. These faults may accumulate in a stack manner and may arise one day(generally in a critic time) as a bigger threat to be handled quickly. This problem generally will be login error in a system/device, because its password was not updated in batch configuration process. In this situation system administrators have to

remember old password for device/system updating.

2.2. Misusage/Accident Detection Difficulties

It is obvious that all systems and database systems and network devices, even there is no hardware problem, will cause some errors and exceptions sooner or later. Super user privileged group is responsible for system and network components. This error can be caused by super user privileged user consciously or accidently (as a side effect of some operation). In password sharing manner, all system administrators use same user name and password in system. When a unexpected situation occurs in a device or system, it is hard to find responsible user via back tracking process because all devices, database systems and operating systems' session log files holds the same super user, which points all system administrators group.

In this case, the only back tracking way is to find responsible is human based searching, that all system administrators interrogated.

2.3. Out-Source Usage Difficulties

As it is known, corporations needs network, hardware and software components for work requirements such as reporting, storing records and connecting inter-department or external networks. Because softwares are "alive entities", they all need upgrading, updating and maintenance. In this concept, corporation's hardware components (servers and network devices) are also need routine maintenance.

In the situation of upgrading of a software which is serving the corporation, can be upgraded by the corporation's own software development department. But in case of corporation may not have a software development department, or it’s department may not have enough quality/man-power for developing required software, the corporation appeal to a out-source software company/employees for the development.

Similarly, if the corporation has not enough quantity or qualified employee for network management, the corporation may prefer a external network service company.

In the out-source usage case, the out-source providers needs to retrieve system, databases and network devices with super user privilege. That means out-source providers gain full access on corporation resources. This brings some problems together. First of all, especially software developing, upgrading and updating processes need permanent and careful observed. Also super user passwords have to be changed at the start and at the end of these processes.

If the software developer company is also responsible with management of software, password management becomes more complicated. Because software developer company employers have same privileges with system administrators, they also have to be included in pasword management. On the other hand, they have to be behaved as corporation employee and to be included the two processes introduced above. First, they also have to be included into error tracking processes when an unexpected situation occurs on the resource that software developers responsible, such as databases. Second, employee change routines for password management have to be applied when a employee left from project group of software company.

2.4. Embedded Passwords of Applications Difficulties

Corporations benefit software services for their routine office duties such as payrolls or backup. The software processes connect to system servers and databases during serving. These processes use username/password pairs to login, just like system users.

The password/username pairs that are used by software shouldn't be changed in normal conditions. In operations like inter-corporation migrations, re-planning and updating operations can harm these pairs by accident. These accidently occoured errors block software services and they cannot work properly.

3. Conclusion

In the scope notions above, super user passwords are required to be managed carefully regardless of corporation capacity, server park and active network device count. That means all domains need a password management

software, especially for super user management. It will be meaningful to expect that this password management includes the following features :

- Compatible with market's dominant operating systems.
- Compatible with market's dominant network devices.
- Compatible with market's dominant DBMSs.
- Keeping the Super User Passwords on itself.
- Creating a One-Time-Password for a single system when it is requested.
- The created OTP will work on given schedule with restricted time frame.
- Able to create passwords on server based or user based senarios.
- Detailed passowrd creation logs.
- Able to update all super user password of the systems periodically or on demand.
- Able to dump current passwords for unexpected situations.
- Able to train for undefined devices which operate on HTTP or SSH protocol.
- Has an API for batch processing softwares.
- Able to cancel a users all privileges when his account is suspended/deleted.

It is obvious that a centralized password management software with features above will facilitate employee business routines and will provide better security for the corporation systems and devices.

References

1. Tony Bautts, Terry Dawson, Gregor N. Purdy, Linux Network Administrator's Guide
2. Matt Bishop, Password Management, Department of Mathematics and Computer Science
3. Password Management Best Practices, Hitachi ID Systems
4. Priviliged Password Management, http://en.wikipedia.org/wiki/Privileged_password_management
5. Ali Saatçi, Bilgisayar İşletim Sistemleri