Unique User Identification

GIAC HIPAA Security Certificate (GHSC)
Practical Assignment - Version 1.0

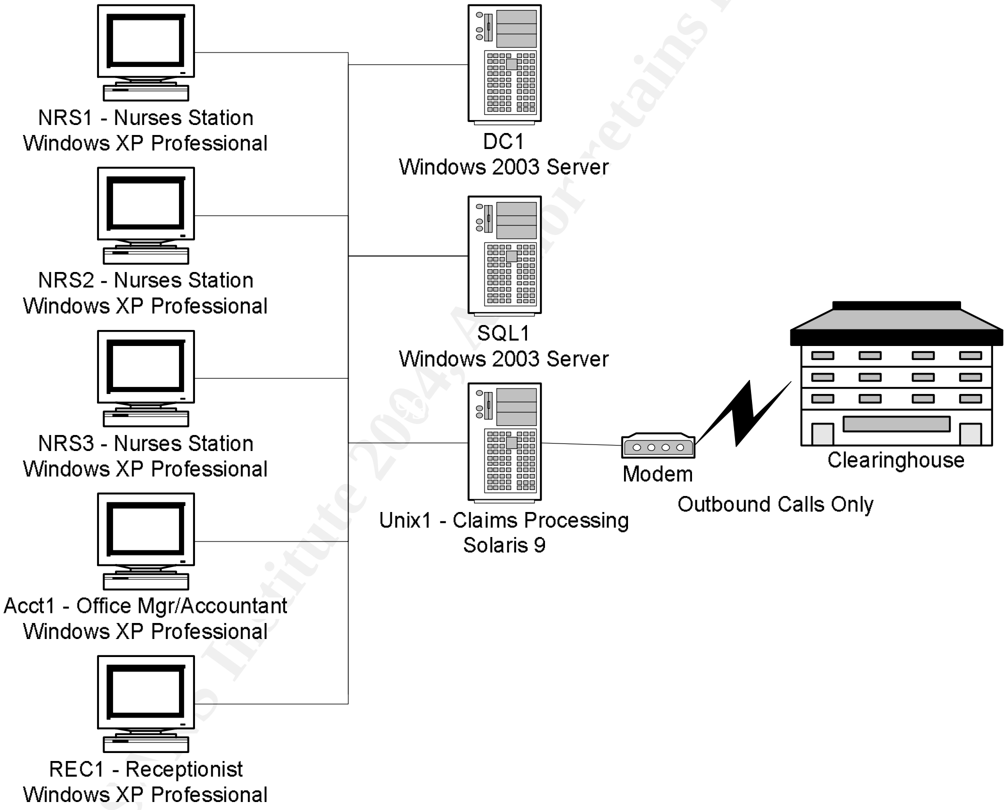
T. Brian Granier

Abstract

This document discusses the Unique User Identification implementation specification that is part of the HIPAA Security Rule federal regulation. A sample covered entity, GIAC Health, is defined as a small clinic that is used as a point of discussion for this document. Next, an explanation is provided to explain the Unique User Identification requirement. This is followed by a sample policy that could be implemented to help ensure compliance with this requirement. Finally, audit procedures are provided that can be used to ensure GIAC Health is in compliance with the stated implementation specification.

Assignment 1 - Define the Environment

GIAC Health is small clinic consisting of four doctors, eight nurses, an office manager/accountant and a receptionist. The networking for GIAC Health is a Windows 2003 Active Directory environment. They also have a single Unix based operating system that is used for processing claims information. This system is accessed via SSH only. GIAC Health uses a Windows 2003 SQL Server for storing the majority of their PHI information. The SQL application uses Windows 2003 user account information for authenticating and restricting/permitting access to the information it stores. The Unix system does not currently integrate with the Windows 2003 user accounts. There are no remote access or VPN accounts in use at GIAC Health. The network diagram is as defined below:



Assignment 2 – Explanation

Access Control Standard

The unique user identification implementation specification is part of the access control standard. The access control standard seeks to ensure that only authorized individuals have the ability to access the Personal Health Information (PHI) that is stored on a covered entities computer systems. Note that this standard is classified as a technical safeguard and is intended to be applied to electronic methods of access (as opposed to physical, which is covered in its own section).

The text from the final rule that describes access controls is as follows:

> (a)(1) *Standard: Access control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

The reference to § 164.308(a)(4) discusses that the access controls implemented are expected to be used to enforce the access permitted by the administrative safeguards. In short, this means that only individuals who have been given the administrative authority to view PHI are able to do so and that when accessed electronically, this access is enforced based upon the implementation specifications that the Access Control Standard requires.

Unique User Identification (Required) – Implementation Specification

The specification requires that users have a unique login account for electronic access to PHI. The text from the HIPAA legislation reads as follows:

> (i) *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.

The intent with this implementation specification is that each user has a unique login account. The point of doing this is so that electronic audit logs that identify PHI access can be tied to a single user to assist in identifying individuals who are attempting to or who have accessed PHI despite no administrative authority to do so and to be able to enforce this administrative authority. Related implementation specifications include termination procedures, log-in monitoring, password management, access authorization and access establishment and modification.

Assignment 3 – Policy

This policy is created with intent of matching the format used by policies found at http://www.sans.org/resources/policies/. This policy is specifically designed to comply with the unique user identification implementation specification for the HIPAA regulation but could be used in other organizations as well.

User account creation and access maintenance policy

1.0 Overview

User account names are just as important to computer security as passwords. Without unique user name accounts that can be associated with a single individual, auditing and access controls are difficult if not impossible. As such, all <Company Name> employees (including contractors and vendors with access to <Company Name> systems) who require accounts will have accounts assigned to them that conform to the guidelines below.

2.0 Purpose

The purpose of this policy is to establish a process by which all user accounts are uniquely identifiable to the individual or process that uses them.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account on any system that resides at any <Company Name> facility, has access to the <Company Name> network, or stores any non-public <Company Name> information.

4.0 Policy

All electronic user accounts are to be unique and each user account must never be used by another individual after creation. User account will remain with the individual throughout the entirety of their relationship with <Company name> and will not be assigned to future employees, contractors and vendors in the event of termination of relationship. Any access required on the network by each individual will require the usage of this unique user account and the associated authentication methodology. To further help ensure that these accounts are protected to reasonable standards, the password management policy found at http://www.sans.org/resources/policies/Password_Policy.pdf will be followed as well.

4.1 Single Sign-on

To assist in managing this process, single sign-on capabilities will be used wherever possible. This means that the account created for each user in the primary network operating system environment for <Company Name> will be used as the user account information for access to all third party applications whenever possible. In cases where this is not able to be done, this will be documented and all accounts created for the third party application must match the user account created under the primary network operating system environment.

4.2 Username format

Accounts will be created using the standard of at least the first four characters of the users' first name, followed by up to four characters of their last name and then a three digit number randomly assigned. For example, Tom Jones could have a user name of "tomjone294". All user accounts will have the users' full name included with the account so they can be uniquely associated with the specific individual for which the account was created.

4.3 Termination of relationship

Upon termination of relationship with <Company name>, the accounts for the user will be disabled, but not deleted, to ensure that the same user account id will not be used in the future.

4.4 Service Accounts

It is reasonable to anticipate that accounts will need to be created that are not uniquely associated with a specific user. These accounts are to be for special purposes, such as for running scheduled batch jobs, backups, service applications or the like. These accounts must be unique to the process or function for which they are intended and are to be clearly documented.

5.0 Enforcement

The responsibility for complying with this policy belongs to the personnel responsible for creating accounts. This includes network operating system accounts and accounts for third party applications. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Single sign-on – Single sign-on is a termed used to identify a process by which a user need only log in once for access to all information with a network. This is typically accomplished with some type of centralized authentication point to which all applications, including network operating systems, are able to verify the identity of the individual requesting access to the resources it controls.

7.0 Revision History

Assignment 4 – Option A: Auditing

The auditing process defined below is specifically designed for GIAC Health as described in assignment 1. This audit process could be more or less detailed depending upon the environment, but these processes should be usable as a foundation from which similar audit routines for this implementation specification can be created.

Windows 2003 Environment

Windows accounts can be viewed from the Domain Controller using "Active Directory Users and Computers" to see it graphically or it can be extracted with a command-line utility. GIAC Health is a small organization, so graphically might be the most efficient way of doing it, but in a larger environment, the command line methodology would be better. To provide a process that would be usable in all Windows 2003 environments, we'll review the command line method as this can be used to facilitate an easy to use checklist in excel or in almost any database format. Issue the following command on a system with read access to the entire Active Directory database:

```
dsquery user dc=giachealth,dc=local | dsget user
```

This assumes that the Windows 2003 domain used in this environment is "giachealth.local".

The result will provide an output formatted as follows:

```
dn              desc            samid
```

DN denotes the distinguished name for the user account such as "CN=Andrew Manore,CN=Users,DC=giachealth,DC=local". "desc" specifies the description for the account, such as "Nurse" and samid denotes the username such as "andrmano438" for the specified user. Each line will denote a unique user account.

Each of these accounts should be reviewed to ensure that they conform to the policy. Individual workstations should be checked to ensure that they do not have any local accounts beyond the default Administrator and Guest accounts. To do this, access the local users and groups utility and view the local users.

Next, the list of applications being run on all the systems should be identified. This is for the purpose of identifying if any applications maintain their own user account list that need to be checked to ensure they conform with the policy. To view this list, from each system, view the Add/Remove Programs tab to list the applications that are installed. For GIAC Health, the only application that is expected to be found that fits into this category is SQL. If other applications are found that maintain their own user list, they will need to be checked according to the software documentation and any user accounts that aren't integrated with windows authentication need to be checked for compliance with the policy.

To ensure that SQL is using Windows Authentication, the Enterprise Manager application needs to be opened. From the Security > Logins panel, ensure that the "Type" column does not list the word "Standard" as this will indicate a SQL account as opposed to a Windows Authentication that will use the Active Directory user accounts. Windows authentication will be listed as either "Windows User" or as "Windows Group" depending upon how the configuration has been setup.

Unix System

The remaining system for GIAC Health is the Solaris system. To identify the users created in this environment, the /etc/passwd and /etc/shadow files should be reviewed. A sample /etc/passwd file might look as follows:

```
root:x:0:1:Super-User:/:/usr/bin/tcsh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
adammoor392:x:101:1:Adam Moor:/usr/users/adammoor392:/usr/bin/tcsh
mikepric221:x:102:1:Mike Price:/usr/users/mikepric221:/usr/bin/tcsh
shirvaug948:x:103:1:Shirley Vaughn:/usr/users/shirvaug948:/bin/sh
sshd:x:105:100:sshd privsep:/var/empty:/bin/false
```

Each user account needs to be reviewed to ensure compliance with the stated unique user policy. In this case, each of the user accounts should reflect the same username as they appear on the Windows Domain Controller. Note, just as in Windows, there are a number of "service" accounts that are not meant to be used by users. To ensure that these accounts are not in use, the user login logs should be checked. Typically, this is located in /var/log/authlog, but this may vary depending upon specific configuration done by the administrator. It is expected that SSHD is used as the only method of access to this system so, check to ensure that user account authentication is written to this file. If it isn't, find out where it is logged and view the file to ensure that only user accounts are logging into the system. For SSHD, check the "SyslogFacility" configuration in the sshd_config file and then the correlating syslog.conf file to determine where the specified syslog facility is written.

Checklist

The previous section explained each of the steps in detail. This section provides the same information in a short checklist format:

- Check Domain and local user accounts on all windows systems and ensure the unique user account policy is followed.
- Review list of installed applications on all Windows systems and check to see if any applications contain their own user accounts. If they do, ensure they conform with the policy.
- Check the users on the Unix system and ensure compliance with the unique user account policy.
- Check the login history and look for users logging into accounts they should not be (such as root).