**Name**: Simon Clarke
**Version Number:** GSEC 1.4b Option 2 (case Study)
**Title:** Authentication - The simple things in life cannot be forgotten

## Summary / Abstract

There are hundreds of facets to IT security - system security, network security, physical security to name just a few. There is one common element that runs through them all – authentication - the simple act of verifying that the person that is accessing a system is what they claim to be and not, for example a worm that is using authentication as a means of propagation.

The following case study will outline how I as the newly promoted IT security officer, hired after a massive viral attack can substantially improve the IT security of my company by designing, implementing and reviewing system wide authentication processes. The case study has been written to share my experiences of how to improve the authentication process through weighing up cost versus risk.

## Before Snapshot

First day at my new job

It was my first day as an IT Security Officer at the Company. I reclined in my new chair, cupped my hands behind my head and thought back to my interview.

The interview for the newly created position of IT security officer had come about because the company had recently been hit very badly by the Deborm worm. The worm used a password cracking dictionary attack vector as a means for propagation. The company had been rather slap-dash when thinking about IT security up until this point so the worm spread rapidly through the Windows environment requiring hundreds of man-hours to remediate.

My musings were interrupted by a knock on the door to my office; the chief technology officer (CTO) poked his head round the door.

“OK, so how are we going to stop the next virus then”?

“Well”, I said, thinking back to the last IT security training course, “First thing we need is up-to-date anti-virus software, using a delivery mechanism to ensure systems are protected against the latest viral threats”.

“Done that”, said the CTO, “we got a security company in last year to install an anti-virus central console in our 24 by 7 operations centre. This allows us to roll out new anti-virus signature files or detection engines within minutes of them becoming available. Problem was by the time we had a signature file available, we had almost half of our Windows 2000 machines infected and you know that virus infected the systems so badly that it cost over $500,000 in desk side support costs to remediate”.

I nodded in a sympathetic way at the CTO; the CTO returned my nod with a look that would sour milk. I had better think of something better or my first day at the job could very well be my last, I thought.

The CTO’s facial expression turned a little warmer, “look, it’s your first day in the job, come back to me by the end of the week with an action plan”, he said.

Well, no pressure there then!

## Casing the joint!

Right, first things first, I needed to know more about the computer systems that the Company uses. I already knew that the company was mainly a Microsoft shop. Windows 2000 Professional was used as the standard operating system for about 5000 desktops and laptops. The old NT 4.0 account domains had recently been migrated to a single Active Domain forest. Microsoft Exchange 5.5 was used as the corporate e-mail solution and the networks were based on Cisco kit. I was far less knowledgeable regarding the Internet gateways and the large 'mainframe' type systems that the company used.

After talking to a number of technical staff I discovered that the company used Sun Solaris servers running Solaris version 8 for the corporate finance and human resources (HR) systems and the two company manufacturing sites had a large single AS/400 system running a custom written application to handle the manufacturing process.

Time to talk to the Internet Service Provider (ISP). I had gathered earlier that the ISP provided a fully managed service to the company. After two hours worth of questions and answers with the ISP I discovered that the managed service consisted of two firewalls, one at the Internet side and the other at the company side. The external firewall was configured pretty securely and allowed only port 110, 80 and 443 sessions to be opened from the Internet. There was a caching proxy server with content filtering that we could modify via a web front-end. The Exchange bridgehead had anti-spam and anti-virus software. The web hosting ran on servers that were fully maintained. In short, this out-sourced deal seemed to provide a pretty secure service.

My goal at the moment was to come up with a plan of action that would offer fast improvements in this company's IT security. This ISP out sourcing deal looked like it offered a good level of perimeter security. I would still need to audit the service more carefully at a later date but it seemed good enough to leave it alone for now.

## Hooking a Worm

So armed with my greater understanding of the company's systems and network structure, the next port of call was to research how this worm had done so much damage.

After checking the McAfee anti-virus knowledge base[1a] and the Trend Micro Virus Encyclopedia[6] along with a few news boards the attack profile became clear. This worm used open Windows root file access to copy itself to the targeted PC. These are the steps the worm used to infect a PC: -

Extract from the MacAfee Virus Information Library (W32/Deborm.worm.gen)[1b]

## ***Early Variants***

*Initial variants of this worm consisted of a dropper which dropped and executed various other components. These included a batch script (for connecting to remote machines), an application to launch processes on remote machines (RemoteProcessLaunch application ) and an IRC bot (which is remotely launched on remote machine). The batch script drives propagation, attempting to connect to remote shares using various usernames and passwords. Example accounts used include:*

- *Administrator*
- *wwwadmin*
- *database*
- *user*

*With passwords such as:*

- *"" (blank)*
- *user*
- *admin*
- *admin123*
- *password*
- *administrator*
- *changeme*
- *123*
- *1234*
- *12345*
- *123456*
- *654321*
- *test*

## ***Latter Variants***

*Latter variants do not rely upon a batch script for connecting to remote machines. When the worm is run on the victim machine, it sets the following startup hook on the victim machine:*
*HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run*
*"NAV Live Update" = (path to worm )*

*The worm will drop (and execute) other malware on the victim machine, for example IRC-Sdbot , BackDoor-JZ ("BackDoor.Litmus"), or ProcKill-AF . For example, the following files are dropped by one variant:*

- *IRC-Sdbot : %SysDir%\EXPLORER .EXE (12,832 bytes)*
- *BackDoor-JZ : C:\WINNT\LITMUS\SVCHOST32.EXE (17,440 bytes)*
- *ProcKill-AF : C:\WINDOWS\Winlogon.exe (17,410 bytes)*

*Such files dropped in testing were already detected by McAfee products using the specified engine/DATs (or greater).*
*Additional system modifications associated with the dropped malware will also occur on the victim machine - see the separate descriptions for such startup hooks etc.*

*Network Propagation*

*The worm scans the local network (via sweeping contiguous IP addresses) for machines present on the network. Once a system is found, the worm tries to connect to the 'IPC$' and/or 'C$' and/or 'C' shares on that machine (variant dependant). The following accounts are used for the connection (with no passwords):*

- *Administrator*
- *Owner*
- *Guest*

*NOTE: The virus assumes the privileges of the currently authenticated user. If a domain administrator logs on to an infected system, virtually all accessible systems on the LAN may be vulnerable to share propagation.*
*If successful, the worm will copy itself onto that share in one of the following locations (ie. Windows startup folder):*

- *C:\WINNT\Profiles\All Users\Start Menu\Programs\Startup*
- *C:\WINDOWS\Start Menu\Programs\Startup*
- *C:\Documents and Settings\All Users\Start Menu\Programs\Startup*
- *\WINNT\Profiles\All Users\Start Menu\Programs\Startup*
- *\WINDOWS\Start Menu\Programs\Startup*
- *\Documents and Settings\All Users\Start Menu\Programs\Startup*

*Finally, the worm attempts to execute the copied file by calling the NetScheduleJobAdd function.*

## During Snapshot

### The Truth is Out There

Now that I understood how the virus worked, I needed to understand how the Company got hit so badly. 'Time for a little experiment', I thought.

I found the machine name of the person in the next office and asked him if he minded my trying to test his PC (permission is the difference between a hacker and an IT security person after all).

I typed 'net use \\PC0354\c$ password /user:pc0354\administrator' – No that didn't work.

'net use \\PC0354\c$ administrator /user:pc0354\administrator' – Still nothing.

'net use \\PC0354\c$ "" /user:pc0354\administrator' – Bingo.

After repeating the experiment on a few more PCs I was beginning to have an idea how this worm spread so quickly through the company. It was looking like a great number of Windows 2000 workstations and laptops had a blank local administrator password. There's my first action point for the CTO – we need to change the local administrator password on all Windows 2000 workstations and laptops.

Now that I knew that the virus spread using a blank local administrator password, the question was how could I change every single Windows 2000 local administrator password with the minimum of cost? Active Directory Global Policy Objects (GPOs) would allow me to enforce a password policy for both the domain and local Windows 2000 desktops. Unfortunately a local account policy only becomes active when a local account is used thus the policy would only be enforced when a user attempted to logon as local administrator. I also quickly discounted sending helpdesk personnel around to every Windows 2000 computer within the company (the expense would not please the CTO).

So after searching the Microsoft Knowledge Base I came upon a little command-line tool (Cusrmgr.exe[2]) bundled with the Windows 2000 resource kit that would allow me to remotely change the local administrator password to a random one thus scrambling the local administrator account.

Scrambling the local administrator account has two big security benefits and one big support issue. The first benefit is the local administrator account would have a strong password; so cracking it would be difficult to achieve. The second benefit would be each Windows 2000 desktop would have a different password, so compromising one desktop's security would not mean all desktops were compromised. The support issue is obvious; if no one knows what the local administrator account is, how does the desk-side support staff gain local administrator rights to perform their work? The answer to that is two fold; the desk side support staff can be given local administrator access to the desktop via active directory. Secondly if the desktop is unable to talk to a domain controller i.e. the desktop's network card has died, the support staff require a way to reset the local administrator account so they can repair the desktop, this was done by issuing a Linux boot disk called LINNT[3] which, when run reset the local administrator password.

### Scramble - Scramble

As an Enterprise Administrator, I intended to run the scramble process each week to insure all Windows 2000 workstations are contacted. To use the password-scrambling tool I needed first to gather a list of all the Windows 2000 desktops and laptops within the company. That information is listed in Active Directory so an export of the data to a text file was a simple process. I used the export feature in an administration tool called Hyena[4] to perform the computer name export. Next I created a little script to take the text file containing the list of Windows 2000 computers and run the password scrambling tool against each one, the script went as follows: -

```
@echo off

if not exist "%1" goto syntax

for /f %%i in (%1) do call :go_scram %%i
goto fin

:go_scram
echo Scrambling Machine %1
cusrmgr -u Administrator -m \\%1 -p
goto fin

:syntax
echo Syntax: SCRAMBLE {input file}
echo Example SCRAMBLE export.txt
goto fin

:fin
```

### A Brisk Morning Walk

The next morning I arrived early to work. I wandered around the open plan area of the finance department. 'Good grief'! Desk after desk had POST-IT notes with usernames and passwords on them. My biggest find was this note: -

> Hi Janet,
>
> I've changed the administrator password for the accounting system to 'pencil', hope you enjoyed your holiday – see you next week.
>
> Mike

'Didn't these guys see War Games[5]'?

I've got action point two - this company needed a password policy, signed for by the CEO, communicated to all staff and rigorously enforced.

<u>Creating a company wide password policy</u>

In my experience there are five simple rules to create a policy, they are: -

1. Make the policy as black and white as possible. This doesn't mean use only black ink on white paper – it means try to eliminate any points that could be misunderstood.

2. Make the policy as simple as possible. All personnel within the company have to be able to read it and understand it.

3. A technical policy, often required in IT security, should have two sections in it. Section one is written for non-IT people and section two for the IT folk. The reason for this is that a policy is useless unless everyone knows it, understands it and obeys it. Section two describes how the policy needs to be implemented on computer systems.

4. The policy has to be signed-off by at least the HR head and the technology head but preferably the CEO.

5. The policy has to have a way of waiving exceptions to the policy, a set review period and a way of enforcement.

OK, with my policy-writing rules firmly fixed in the back of my head I went about writing the policy. The company uses AS/400, Sun Solaris 8, Windows 2000 and Cisco systems. My first goal was to try to create a password policy that would work for all these systems.

I first talked to the AS/400 manager (Yes AS/400, not iSeries, I had already discovered that this system is pretty old)

“So what password policy do you use?” I said.
“We have a small number of administrator accounts on the system, over and above that the manufacturing application talks to the operating system using hard coded service accounts – you’re not going to ask me to change them are you? That would mean a re-write in the code! The cost would be tremendous.”
“No we’ve got a waiver process for these type of accounts – but would it be possible to enforce a change in the administrator passwords on a regular basis?” I said.
“Yes – that shouldn’t cause a problem”, the AS/400 manager said.

Next on the list was the Unix manager.

“So what password policy do you use?” I said.
“None at the moment but we can implement whatever you wish – just tell me the settings, minimum password, account lockout setting etc.”, the Unix manager said.
“Cool – before I publish the password policy I’ll run it by all the system managers for their approval”, I said.

Now time to talk to the Network manager.

“So what password policy do you use?” I said.
“Well we use a password to access the Cisco kit, Oh and we have enabled the secret function”
“Oh good, at least the password file is not stored in plain text”, I said.
“Look, lets be honest here, the network team consists of three people – all based in the same office. What do you want us to do?”
“Would it be a problem to change the privileged mode password periodically?” I said.
“What on over 200 Cisco devices! You’ve got to be joking. We wanted to buy a TACACS+ server to allow us to centralize this sort of thing but the funds were never available”.
“OK, thanks for your help, I’ll see what I can do”, I said – writing the words TACACS+ and Cisco in my ‘things to do’ list.

Final port of call, I talked to the Microsoft products manager.

“So what password policy do you use?” I said.
“Well, its like this – we migrated from an old NT domain structure to Active Directory last year and we were, well are going to implement a strong password policy but it’s sort of slipped down the priority list a bit”
“What about the local administrator account being blank on the workstation and laptops?” I said.
“That’s not my fault, when a new workstation is delivered to a user we give them a sheet of paper that includes instructions on how to change the local administrator password”

“But the password change isn’t enforced?” I said
“Well – No”

After a few iterations I had a draft password policy. The publishing process would be an e-mail sent to all employees with an acceptance button, a laminated copy of the policy sent to every employee and a copy of the policy included in the new employee training pack.

## Information Technology Password Policy

### AUDIENCE AND SCOPE

This Policy applies to all Individuals within the Company who use any company computing equipment.

### THE POLICY

- A username and password are required to gain network access to any computer system.
- A user account should be restricted so that it only has access to the areas within computer systems that the user requires to perform his or her duties.
- Temporary user accounts (e.g., for contractors) should be set to expire on a predetermined date.
- User accounts should be disabled after a 90-day period of inactivity.
- User accounts must be disabled upon termination / suspension of the user.
- Users must not share usernames and / or passwords without express written permission from the IT Security Officer.
- Client-based automated processes (e.g., an automated logon script containing username and password) that by-pass user manual access control mechanisms should not be used without express written permission from the IT Security Officer.

## POLICY IMPLEMENTATION

| Description | Policy |
|---|---|
| Password history (a password may not be reused within a set period) | 10 passwords |
| Maximum password age (the period of time a user may keep using the same password) | 120 days |
| Minimum password age (the period of time a user has to wait before changing their password) | 1 day |
| Minimum password length (the minimum number of characters allowed for a password) | 8 characters |
| Password complexity requirement | A mixture of alpha-numeric and non-alpha numeric |
| Bad Logon Attempts (the number of logon attempts before a account is disabled) | 5 logon attempts |
| Reset account lockout counter (the elapsed time before the bad logon attempts counter is reset) | 30 minutes |
| Account lockout duration (the time a user has to wait before their account is reset after the account is disabled) | Manual – the account has to be reset via a manual process i.e. by the helpdesk. |

## WAIVERS TO THE POLICY

Any exception to this policy has to be agreed to by the IT Security Officer. Any agreed waiver will be active for no longer then one year.

## ENFORCEMENT

Any of the Individuals found to have violated this policy maybe subject to disciplinary action in accordance with prevailing IT and HR policies and procedures in force. For Individuals who are not employees of the Company, they will be subject to discipline according to the terms and conditions of the agreement with the contracted service provider.

## FRIDAY COMETH

I've had a week. My boss expects me to have a plan of action that will quickly plug the immediate security gaps in the company's IT infrastructure.

"Come in", said the CTO. "OK, what have you got for me?"

"Right, you asked me to prevent infection from the next virus. Since I don't know what the next virus will be, that's a pretty tall order, but what I can do is plug the gap that allowed this company to be decimated by the last virus. I've got two immediate action points that need to be implemented as soon as possible."

"I'm listening"

"Action point one; the vast majority of our standard desktops have a blank local administrator password."

The CTO's face turned a few degrees redder.

"The policy that this company has at the moment when delivering a new desktop to personnel is to instruct people how to reset the administrator password, but the nature of people being what it is, they are too excited about playing with their new toy to be concerned with the paperwork. All systems must have a complicated or strong password for the administrator account, and that password has to be set as mandatory. I've worked with the desktop engineering people to roll out a process that will automatically change the administrator password in the background," I said.

The CTO looked over at me, his eyes narrowed. "How much is this going to cost?"

"Well, the implementation cost is zero. We're going to use a free tool from Microsoft called 'Cusrmgr.exe[2]' to do the work and we will rollout via a weekly procedure. We've got about 5000 desktops and laptops to configure, and I'm sure that the helpdesk will have a number of extra calls regarding issues concerning the change of password, but I believe the fallout will be minimal."

"Very good, what's your second point?" said the CTO.

"A password policy. A simple set of instructions that can be given to everyone within the company telling them what they should and shouldn't be doing with regard to computer authentication."

"We do tell people about how to use the computer systems", argued the CTO.

"Is it a written-down policy of this company, signed off at the highest level and enforced?" I enquired.

"Not as such".

"Well it needs to be. People have to understand that when they sign on to a computer system it's like using their signature. It is a legal statement that they work they are carrying out under that authentication is their work. If we get into a situation that requires computer forensic evidence to prove a legal case, we won't be able to provide conclusive evidence to a court of law, and that's the sort of thing that is the difference between a profitable company and a bankrupt one.

"And, as the best celebrity chefs would say, here's one I made earlier". I handed my draft password policy to the CTO.

The CTO stood up and extended a hand. "Good work – I see I made the right choice when I promoted you to IT Security Officer".

## After Snapshot

It's one month later. I take stock of my first month in my new job. What has gone well and what has gone not so well and what things can I do over the next month that will improve the company's IT security still further.

First the good points: -

The password policy was signed off by both the CTO and CEO and then communicated to all personnel within the company. The communication process had been modified since my first draft. I used the company's e-mail system to send a copy of the policy to every e-mail address within the company. The e-mail had a voting button on it to confirm that the reader understood and agreed to the new policy. I wish I had not used my own mailbox account to send this message as I had an e-mail response back from some 5,000 users, which somewhat clogged my mailbox up! I also added the password policy to the new personnel starter pack along with a sign-off form. This meant that all new starters to the company had to read the policy and sign a form to say they agreed to it. In the end I didn't print and send a hard copy of the policy to all users as the printing cost would have been prohibitive. My final method of communication was to set-up an Intranet web site for IT security with a hyperlink to it from the company's home page, which would display all relevant IT security related information.

The local administrator password-scrambling tool had also worked well. After initial testing I started to run the tool on a weekly basis. The helpdesk received a number of calls after my first run, mainly from people who were using the administrator account to run services or scheduled tasks on their desktops. This led to a number of disgruntled users but after a few weeks the process settled down. Before my first run I had alerted both the helpdesk and the technology groups to check they were happy for me to proceed, but I was surprised to see just how many non-IT personnel were performing tasks that were affected by the local administrator password scramble. If I had to do this task again I would have probably sent out a company wide memo telling people what was about to happen.

Now the bad points: -

When I modified the active directory root GPO to reflect the new password policy I didn't think about the support issues around the resetting of passwords. The password policy states that 5 bad logon attempts will lock the account and if an account is locked out the account must be unlocked manually where as the old root GPO did not have an account lockout policy set. I was expecting only one or two accounts to be locked each day but when I changed the GPO to reflect the new password policy the helpdesk were overwhelmed with requests for account resets. It was so bad I had to change the GPO back to the old settings while I sorted the problem out. It turned out to be a company application that used NT authentication. What happened was that if a user had two machines, a desktop and a laptop for example, the user would change their password on the laptop, while the desktop was still logged on. If the user tried to run the application on the desktop, the application would try again and again to authenticate using the old password. This would, within a second lock the user account causing the call to the helpdesk.

Of course this issue caused a great deal of trouble and a very unpleasant discussion with the CTO. To fix this problem I sent a company wide memo out detailing that a user must logout of all their workstations before changing their password as well as working with the application developer to try to fix the application so that it will fail after only one logon attempt.

Looking to the future:

My initial work has concentrated around the Windows 2000 and active directory environment. When I have completed that work I need to start to look at the non-Microsoft technologies. The Sun Solaris systems should be a quick win, the UNIX manager seems very confident that the company password policy can be implemented with minimum effort. As for the AS/400 systems, I feel the authentication issues are best handled by a combination of waivers for the accounts that cannot be modified; such as embedded service accounts and a paper based AS/400 password policy dictating that the AS/400 administrators change their passwords according to the company password policy. The Cisco kit needs to have a central way of managing authentication. The network manager suggested that a TACACS+ server should be installed, this may very well be the best solution but before I start buying equipment I'll talk to a independent network consultant to get their thoughts on the pros and cons of a generic TACACS+ solution verses the Cisco Secure Access Control Server[7].

## Final Thoughts

Being an IT Security Officer is a job that requires technical expertise so that you know where the problems are and how to fix them, but more importantly you have to have both negotiating skills and a large portion of common sense. Never try to fix a problem totally – it is impossible to do. You need to understand the problem enough to evaluate the security risk verses the cost of remediation. It is no good proposing a $2 million solution to protect $1 million worth of assets. Always understand what the business requires, especially when it comes to people. And finally, do not try to change processes that have worked for years just because it will give you a small improvement in security at the cost of operational upheaval.

My company, like most corporate companies looked at IT security as an optional task. They had the opinion that as long as they protected their Internet perimeters and had anti-virus software they would be safe. This is a common misconception, one that cost them over $500,000. This case study I hope can be used as an example, not only as a guide for improving authentication security, but as a warning to other companies, not to think of IT security as an optional extra but as a fundamental part of today's Information Technology environment.

## References

1a) Network Associates Virus Information Library
http://vil.nai.com/vil/default.asp

1b) W32/Deborm.worm.gen description
http://vil.nai.com/vil/content/v_100143.htm

2) How to Use the Cusrmgr.exe Tool – MS Knowledge Base Article - 272530
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q272/5/30.ASP&NoWebContent=1

3) Windows Security - Useful security tools/utilities
To download LINNT click on 'NT Admin Boot Disk' under admin tools
http://www.windowsecurity.com/pages/article.asp?id=454#

4) System Tools – Hyena total system administration web site
http://www.systemtools.com/hyena/index.html

5) War Games – A film by MGM in 1983
http://www.mgm.com/title_title.do?title_star=WARGAMES

-) FOOTAGE FETISHES: "WARGAMES" by Pete Vonder Haar
http://www.filmthreat.com/Features.asp?Id=804

6) Trend Micro Virus Encyclopedia
http://www.trendmicro.com/vinfo/virusencyclo/

7) Cisco Secure Access Control Server for Windows
http://www.cisco.com/en/US/products/sw/secursw/ps2086/

-) Cisco Secure Access Control Server for UNIX
http://www.cisco.com/en/US/products/sw/secursw/ps4911/index.html