SystemEXPERTS
LEADERSHIP IN SECURITY

A Perspective On Practical Security 2000

More Than You Ever Wanted to Know about NT Login Authentication

SystemExperts Corporation
Philip C. Cox & Paul B. Hill

Abstract

The login process is the user's entry-point to the computing environment, the best or perhaps only chance for real authentication. No authorization decision has any meaning absent authentication. Taking the rapid adoption of NT as a given, any organization must understand exactly how NT login authentication works if it is to determine whether or not NT login can meet the organization's needs. Otherwise, the choices are faith and luck.

This white paper describes an Interactive NT login and lays the groundwork for understanding the Network login. This information is current as of NT 4.0 Service Pack 5.

NT Login Authentication

There are no less than 5 types of "logons" in Windows NT, but only three are commonly used: Interactive, Network, and Service.

1. *Interactive* logons are for users logging onto the console and for processes that require "interactive" access. Interactive NT user authentication itself takes several forms:
   - Login with a locally defined user account — no network access is required; the account is authenticated by the machine you are logging into and only by that machine

Inside

- Under the covers for a local NT login
- NT & LAN Manager compatibility
- Password encryption within the Security Accounts Manager (SAM) database
- User Authentication Process
- Use of the LsaLogonUser API
- The groundwork for understanding network login.

SystemExperts Corporation

Boston New York Washington D.C Tampa
San Francisco Los Angeles Sacramento

Toll free (USA only): +1 888 749 9800
From outside USA: +1 978 440 9388

www.systemexperts.com
info@systemexperts.com

  - Login with a Windows NT Domain User account — requires network access; the account is authenticated by an NT domain controller
  - Third party login — authenticated by a third-party replacement for the user interface and the authentication package
2. *Network* logons are for accessing Microsoft Networking Printers and File Shares
3. *Service* logons are used for logging on of services, not users, during startup time

WHEN WINDOWS 2000 IS RELEASED, IT WILL INTRODUCE KERBEROS VERSION 5 AUTHENTICATION AS A METHOD FOR ACCOMPLISHING ANY OF THE ABOVE.

Normal Local NT Login

A normal NT Interactive Login presents you with a dialog box that prompts you for a User name, Password, and Domain — this via the Graphical Identification and Authentication (GINA) module `msgina.dll`. If the machine is not part of an NT domain, then the domain field will not exist and the login will be to the local account defined (only) on the local machine. Even if your machine is part of an NT domain, you can just login to a local account by entering the local machine name in the domain field.

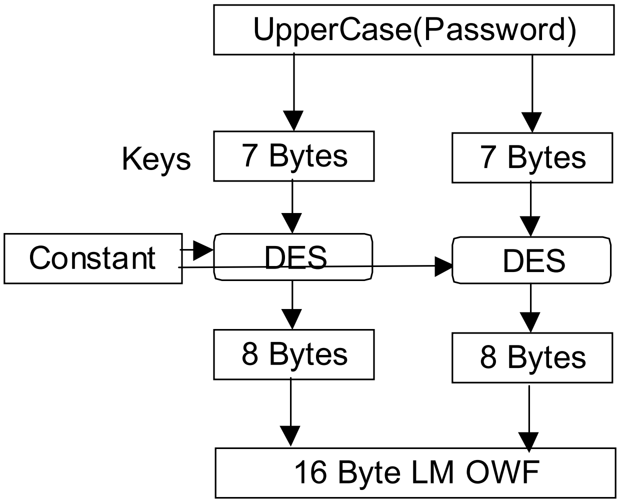
The Security Accounts Manager (SAM) Database

During an Interactive Login, account information is checked against the Security Accounts Manager (SAM) database. The SAM is part of the Registry (Microsoft's system administration database) and is implemented as a separate hive (table). The SAM database is usually located at `C:\WINNT\system32\config\sam`. The SAM database that will be checked is determined by the name in the Domain field of the login. If it is an NT domain name, then the account will be authenticated against that NT domain's SAM database maintained on that NT domain's Domain Controller, i.e., not locally. If the Domain field contains the local machine name or it is blank, the SAM database on the local machine is used.

Each user record in the SAM database can contain two encrypted representations of the user's Password (more explanation to follow). One of the Password entries is used for LAN Manager compatibility.* Prior to any encryption, the LAN Manager version of the Password is uppercased and then truncated or padded to 14 characters. The character set for the LAN Manager compatible password is limited to the OEM character set. The other password entry, referred to as the NT password, is based on the Unicode character set, is case sensitive, and can be up to 128 characters long (this is limited though by the User Interface, as described later).

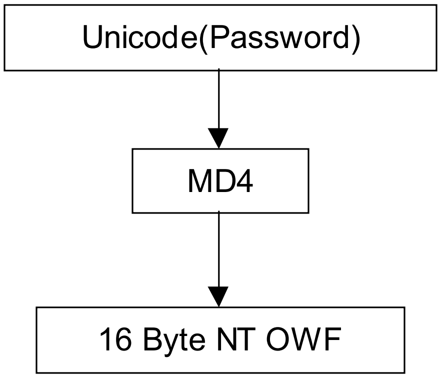
Each of these passwords is doubly encrypted within the SAM database. The first encryption is the result of applying a one-way function (OWF) to the clear-text password to generate a hash result, that is the clear-text password is scrambled to a fixed bit representation derived from, but not indicative of, the original clear-text password. Microsoft says the particular OWF is considered to be non-invertible, i.e., given the hash it is infeasible to find a password to match. Each of the passwords uses a different OWF – see below. The second encryption is used for obfuscation purposes; it is an encryption of the user's relative ID (RID). This is only protective against someone who has access to the double-encrypted password, the user's RID, and the algorithm. The user's RID is a 32bit value that makes up part of the user's Security ID (SID). Well known accounts such as the administrator and guest accounts always have the same RID. RIDs start at 1000 and are incremented by 1.

The LAN Manager OWF version of the encrypted password is computed by uppercasing and truncating/padding the user supplied password to 14 characters. From this a pair of 56-bit DES keys are derived to (ECB) encrypt a fixed 8-byte quantity. The first 7 bytes of the clear-text password are used to compute the first 8 bytes of the encrypted password. The second 7 bytes of the clear-text password are used to compute the second 8 bytes of the encrypted password. The two chunks are then concatenated to form the 16 byte encrypted password. The ECB-encrypted value is known to be `0xAAD3B435B51404EE` decrypted with a key of all zeros. Therefore, this encrypted password is vulnerable to brute force attack.



* LAN Manager is a precursor to Microsoft's present networking strategy. It dates from when there was a close working relationship between Microsoft and IBM.

The NT password is expressed in the Unicode character set; it is case sensitive and can be up to 128 characters long. The OWF version is computed using the MD-4 algorithm – a 16-byte digest (hash) of the (unpadded) variable length clear-text password. This may not be as secure as it first seems as it appears that all existing user interfaces truncate the password to 14 characters, making dictionary attacks feasible where they should not have been on examination of the algorithm alone. Also, transforming an ASCII password into Unicode introduces an alternating pattern of zeros and characters in the input to MD4. It is suspected that this makes the MD4 hash easier to reverse although there is currently no known way to exploit this.



It turns out that there are cases when a user may be missing either the LAN Manager or NT password. For example, only the LAN Manager password will exist if the password was changed from a LAN Manager or Windows for Workgroups client. Conversely, only the NT password will exist if the password was set from an NT client and the password has no LAN Manager representation such as when it is longer than 14 characters or the characters cannot be represented in the OEM character set.

During all NT logins, if both the Windows NT and LAN Manager OWF versions of the Password are available they will both be used. This can be controlled with the `LmCompatabilityLevel` Registry key. Quoting from Microsoft Knowledge Base Article Q147706:

```
HKLM\SystemCurrentControlSet\Control\LSA
  LMCompatibilityLevel
  REG_DWORD
  Value: 0-5 (Default 0)
    0 = Both NT and LM, Never NTLMv2
    1 = NTLMv2, NTLM, or LM response
    2 = NTLM response only
    3 = NTLMv2 response only
    4 = DC Refuses LM responses
    5 = DC Refuses NTLM and LM responses
```

IMPORTANT: If level 1 or greater, if the last password change came from a downlevel client (i.e. WFW or LAN Manager), the NTLM and NTLMv2 data will not be available on the Domain Controller

Level 0 (the default) allows case sensitivity to be enforced when authenticating between NT machines, but it also allows backwards compatibility. Of course it is possible that a user can login from an NT client to a server but will not be able to login to that same server from a LAN Manager or Windows for Work Groups client.

User Authentication Process

Now we are finally ready to examine the Interactive logon to the machines. We will start by looking at using the local SAM.

The process starts from `Winlogon.exe`. This in turn calls the `Msgina.dll` (dynamically linked library). The default GINA library may be replaced by a third party library to provide additional or supplementary authentication services. The Microsoft default GINA library will invoke the sub-authentication process `Lsass.exe` which is Microsoft's implementation of the Local Security Authority. The LSA provides access to the `LsaLogonUser` API.

All NT user authentication initially uses the `LsaLogonUser` API. The LSA initiates login processing by calling an authentication package; the default NT authentication package is `Msv1_0` which is implemented in `Msv1_0.dll` (installed in `C:\WINNT\system32`). Third party vendors can offer replacements for `MSV1_0` which may offer custom services.

The MSV is conceptually split into two halves. The first half executes on the machine being logged into. The second half executes on the machine that contains the user account. When performing authentication against the local SAM database, both halves execute on the same machine.

MSV "Top"

`LsaLogonUser` supports different types of logins; again, the most common are Interactive, Network, and Service. The local User name, the requested NT Domain, and the clear-text Password are passed into `LsaLogonUser` and the first half of the MSV authentication package.

During a local login the first half of the MSV doesn't have to do much; it checks to see if the requested NT domain matches the local machine name. If so, it simply converts the clear-text password into both a LAN Manager OWF password and an NT OWF password, as described above, then it passes these onto the second half of the MSV.

MSV “Bottom”

The second half of the MSV uses the local SAM to validate the user. It passes the User name and both of the OWF passwords for the User name to the SAM.

If the User name does not exist in the local SAM or the Passwords are not correct for the given User name, this is communicated to the MSV and from there to the LSA which then displays the message,

> "The system could not log you on. Make sure your username and domain are correct, then type your password again."

If the account and encrypted passwords match the entries found in the local SAM database then the SAM returns a structure which contains the user's Security Identifier (SID) and group memberships associated with the User name. The second half of the MSV then returns this information to the first half of the MSV which returns it to the LSA.

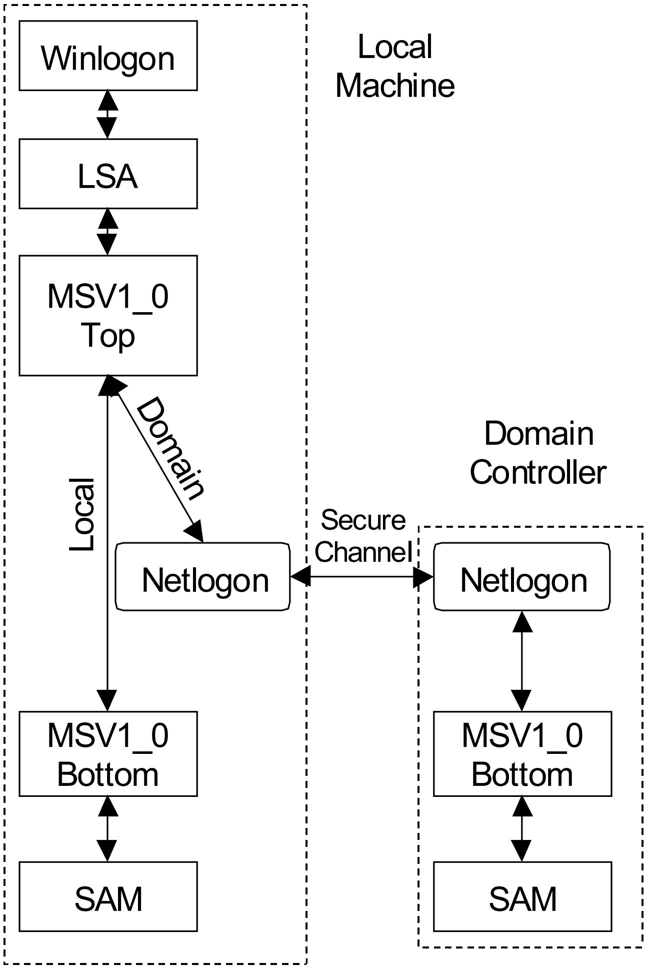
The LSA then uses the SIDs to create an access token that contains the user's rights and group memberships via the `AddAccessAllowedAce` “API” and related functions. The token is then passed back to `Winlogon`. At this point `Winlogon` creates a new process (the user's shell, usually `explorer.exe`), and attaches the token to it. If the user's rights or group memberships are changed, the SID will reflect those changes the next time the user logs on. Whenever the user accesses an NT service or opens a resource, the access token attached to the user's process will be presented to the service or resource manager so that the SID in the token can be compared to the SIDs in the service or resource access control list. At this point, you are logged in and ready to get down to productive work.

Using a Domain Account

The process for using an NT domain account is VERY similar to the local SAM process. The only difference is the mechanism by which the “bottom” half of `Msv1_0` gets the information from the “top” half.

This transfer of information is done via the `Netlogon` service, utilizing the "Secure Channel" (the specification for this service is not published by Microsoft – so no further information is available). The top half of `Msv1_0` will determine the need to utilize the `Netlogon` service by looking at the value of the domain in the logon request. If it is the local machine name, then the process we described happens. If not, then the `Netlogon` service is used to pass the information to the appropriate Domain Controller. The information (User name, Password, and Domain) are sent via the Secure Channel to one of the Domain Controllers for the domain. The Domain Controller will then authenticate the account in the exact same way with its `Msv1_0` “bottom”.

A Graphic



SystemEXPERTS
LEADERSHIP IN SECURITY

About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at technical conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and NT/Windows 2000 security at Usenix, SANs, Networld-Interop, CSI, and InternetWorld are among the most popular and highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio and we wrote the authoritative reference work on Windows® 2000, the Windows® 2000 Security Handbook (Osborne McGraw-Hill).

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention.

Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients.

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. In addition, using our signature workshop-style methodology, our consultants will work with your team to review the security of applications or systems in their full environmental context. During these comprehensive reviews, we will thoroughly explore the business as well as technical issues and we will balance the cost, schedule, and operational constraints of each technical alternative. Many of our clients include these reviews as the jumping off point for planning and prioritizing their security initiatives each year.

Security Blanket & Emergency Response

It is not a question of *if* your organization will be the target of a hacker, it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked and web sites or critical business resources are compromised, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment.

Intrusion Detection and Event Management

In security it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in NT/Windows 2000, Unix, and heterogeneous environments. In addition we frequently perform code reviews of critical applications and web sites.

Security Policy & Best Practices

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice.

Security Stolen/Lost Laptop Analysis

Many organizations expend considerable effort and resources to secure their internal networks, key computing resources, and connections to the Internet. Few recognize that a significant amount of their most proprietary information is traveling around the country on the largely unsecured laptop computers of road warriors and senior executives. SystemExperts' laptop analysis will help you to understand the potential risk of a lost or stolen laptop and what measures you can take to mitigate those exposures.

VPN and Wireless

Certain technologies like VPN and Wireless are becoming ubiquitous and yet most organizations don't know how to properly secure them. We do - and we can help you.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 . 888 . 749 . 9800.

Boston Los Angeles New York San Francisco Tampa Washington DC Sacramento

www.SystemExperts.com info@SystemExperts.com