

# An Analysis of Local Security Authority Subsystem

Shailendra Nigam

*Computer Science & Engineering Department  
DIET, Kharar Mohali(Punjab) India.*

Sandeep Kaur

*Computer Science & Engineering Department  
BBSBEC, Fatehgarh Sahib (Punjab) India*

Bhanu Sharma



*Computer Science & Engineering Department  
BBSBEC, Fatehgarh Sahib (Punjab) India*

**Abstract:** - This paper is based on the literature survey. We will analyze the Local Security Authority Subsystem that how it secure our system form illegal users or any other Malware intrusions because the number of illegal work committed based on the Malware intrusions is never ending as the usage of internet is expanding globally. Basically Local Security Authority Subsystem is a protected subsystem that authenticates and logs users onto the local computer and maintains information about all aspects of local security on a computer. Analysis of local security authority subsystem service is invoked at login time. The security subsystem keeps track of the security policies and the accounts that are in effect on the computer system. Local Security Authority Subsystem Service provides an interface for managing local security domain authentication and active directory process. It handles authentication for the client and for the server.

**KEYWORDS** - Security, Malware, Authenticates, Directory, SAM, LSA, LSASS, Syskey, Winlogon, PEK.

## I. INTRODUCTION

Analysis of Local Security Authority Subsystem Service is invoked at login time. It is a verify the user authentication and grants the system access token, which is used to start the initial shell and is inherited by all programs spawned during this login session. It is maintains the user account database required by the LSA. Local Security Authority Subsystem processes create an LPC port and then handle security requests. Local Security Authentication Server verifies the validity of user login to your PC or Server. This topic basically based on the security issue for system security but I will use the client and server architecture then I will used the network model so this topic is based on the security issue but used in network architecture. Local Security Authority Subsystem Service (LSASS) provides an interface for managing local security, domain authentication, and Active Directory processes. It handles authentication for the client and for the server. Local security authority subsystem service process is called upon to store the hashes in memory. If a password is used that consists of 14 or less characters both hashes will be created and stored in the local security account manager file or in active directory. This topic it is also provide the information about password. This tool to provide forensics, criminal investigators, security officers and government authorities with the ability to analysis a variety of passwords stored on a PC.

- Local Security Authority Subsystem Service (LSASS)
  - Invoked at login time, it verifies the user authentication and grants the system access token (SAT), which is used to start the initial shell and is inherited by all programs spawned during this login session
  - Performs audit functions
  - Operates in user mode
- Security Account Manager
  - User mode component
  - Maintains the user account database required by the LSA
  - Therefore the login sequence requires the following intermediation by security-related services:
    - Winlogon  LSA  SAM

- SAM & Authentication

- It is possible to configure a special computer called a *domain controller* to consolidate the SAM database in a single server.
- Secure Attention Sequence: <CTRL> + <ALT> + <DEL> cannot be captured by user-level programs

The system invokes Winlogon, which starts a graphical application (GINA), to handle local and remote connection requests (via the LSA and SAM)

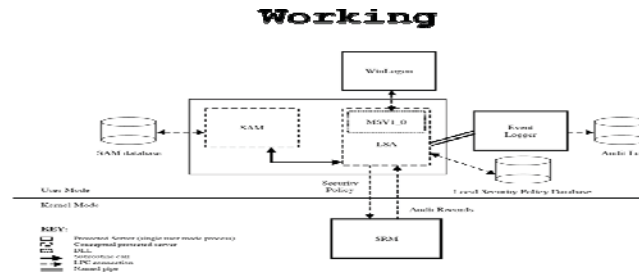


Figure No: - 1 Working of Local Security Authority Subsystem



Figure No: -2 Overview of Security Authority

### Allowing Only Authorized Access

- Three parts to security
- Authentication: Task of authenticating a subject who attempts access
- Authorization: Task of determining if the subject is authorized to have access to a specific secure entity.
- Must also ensure that the secure entity is not copied or accessed while it is in transit (e.g., over the internet).
- Use cryptography to ensure this.
- Provides a “secure container” for information.

## II. SYSTEM DESIGN

We have discussed various Research Paper, they provided architecture for Local Security Authority, Windows includes a set of security components that make up the Windows security model. These components ensure that applications cannot gain access to resources without authentication and authorization. Components of the security subsystem run in the context of the Lsass.exe process, and include the following:

- Local Security Authority
- Net Logon service
- Security Accounts Manager service
- LSA Server service
- Secure Sockets Layer
- Kerberos v5 authentication protocol and NTLM authentication protocol

The security subsystem keeps track of the security policies and the accounts that are in effect on the computer system. In the case of a domain controller, which is a computer that has Active Directory installed, these policies

and accounts are the ones that are in effect for the domain in which the domain controller is located. They are stored in Active Directory.

The Local Security Authority (LSA) is a protected subsystem that maintains the information about all aspects of local security on a system (collectively known as the local security policy and provides various services for translation between names and identifiers.

In general, the LSA performs the following functions:

- Manages local security policy.
- Provides interactive user authentication services.
- Generates tokens, which contain user and group information as well as information about the security privileges for that user. After the initial logon process is complete, all users are identified by their security identifier (SID) and the associated access tokens.
- Manages the Audit policy and settings. When an audit alert is generated by the Security Reference Monitor, the LSA is charged with writing that alert to the appropriate system log.

The local security policy identifies the following:

- The domains that are trusted to authenticate logon attempts.
- Who can have access to the system and in what way (for example, interactively, over the network, or as a service).
- Who is assigned privileges.
- What security auditing is to be performed?
- Default memory quotas (paged and non paged memory pool usage).

Figure 3 shows a local perspective of Active Directory within the LSA security subsystem (Lsass.exe). The LSA security subsystem provides services to both the kernel mode and the user mode for validating access to objects, checking user privileges, and generating audit messages.

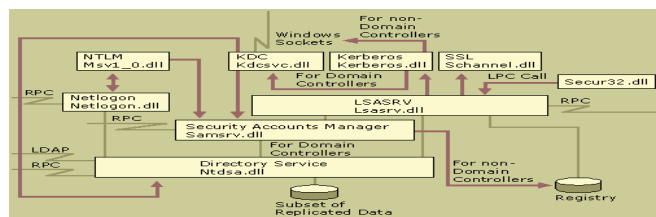


Figure No: - 3 Local perspective of Active Directory within the LSA security subsystem

### III. EXPERIMENTAL STUDY

We have examined that there are lots of process through which our local security can be cracked and the system might be on risk. Anybody can easily crack your security via some commands like they can use the net user command to create and modify user accounts on computers. When you use this command without command-line switches, the user accounts for the computer are listed. The user account information is stored in the user accounts database. This command works only on servers.

You can use the following parameters with the net user command:

- username  
Is the name of the user account you want to add, delete, modify, or view. The name of the user account can have as many as 20 characters.
- password  
Assigns or changes a password for the user's account. A password must satisfy the minimum length set with the /minpwlen option of the net accounts command. It can contain as many as 14 characters.
- \*  
Produces a prompt for the password. The password is not displayed when you type it at a password prompt.

- /domain  
Performs the operation on the primary domain controller (PDC) of the current domain. This parameter applies only to computers running Windows NT Workstation that are members of a Windows NT Server domain. By default, Windows NT Server-based computers perform operations on the PDC.
- /add  
Adds a user account to the user accounts database.
- /delete  
Removes a user account from the user accounts database.

#### Protecting the SAM with Syskey

If you want to secure your Local security authority subsystem then you should protect your SAM File with the use of Syskey. You should use Syskey to protect the SAM for four reasons:

- If you use appropriate security practices and limit administrative accounts and require the use of strong passwords, you will mitigate the threat of pwdump2 and Lophtrcrack 3.0 being used interactively on your systems. Indeed, if an administrative account has been compromised, there may be little need for cracking passwords in the SAM at all because the administrative account can be used to access any resources protected by DACLs.
- You have no way of knowing what the attacker is able to deal with, nor what weapons he has in his arsenal. Just because there are armor-piercing bullets should not prevent me from wearing armor if I may be shot at. The bullets fired at me may be of the regular kind, and I will survive the attack.
- It is always a good idea to layer security on your system. Each problem that you throw in an attacker's way decreases your risk of compromise. If you make attacking your network difficult, many attackers will move on to "lower hanging fruit."
- For a nonadministrative user to use these tools against your SAM, he must somehow obtain a copy of the SAM and use the tools offline. Good security practices can reduce the possibilities of an attacker obtaining a copy of the SAM. Servers, especially domain controllers, should be physically secured. Emergency Repair Disks and backups of the Registry need to be physically secured. The C:\WINNT\Repair directory (which holds a copy of the Registry when the RDISK program is run to create an ERD) needs to be protected, and Registry files can be removed from this location.

#### IV. IMPLEMENTATION

The key used to encrypt the passwords is randomly generated by the Syskey utility. This Password Encryption Key (PEK) is itself encrypted with a randomly generated "System" key (Syskey) and stored in the Registry. Encrypting the PEK prevents compromise of the encrypted passwords. If the PEK were stored unencrypted in the Registry, it might be obtained and used to decrypt the passwords. The Syskey must be present for the system to boot. However, now there is a problem: how to protect the Syskey. This protection may be implemented in one of three ways:

- The Syskey is obfuscated and stored in the Registry. System can boot without administrative action.
- The Syskey is obfuscated and placed on a floppy disk that must be present when the system reboots. The Syskey is not stored anywhere on the system. The key is stored in a file call STARTKEY.KEY. Do not store the key on an ERD. To do so would be to provide two items needed to attack your system in one location. Do make copies of the disk. Without it you cannot boot your Windows NT system.
- A passphrase is entered and then used to create encrypt the Syskey. An MD5 cryptographic hash (digest) of the Syskey is stored in the Registry. The password must be entered during system boot to make the system usable.

In either the floppy disk choice or the password choice, the Syskey is not stored anywhere on the system. Therefore, these choices are more secure. If the floppy disk is lost or becomes corrupt, however, or if the password is forgotten, the system cannot be booted. To apply the additional security provided by using Syskey, follow the procedure listed in Step by Step 1.

#### STEP BY STEP 1 Applying Syskey Protection to the SAM

- Create a backup copy of the Registry prior to completing the additional steps. Be sure to label the backup as pre-Syskey, and store it forever. The only way to recover a Syskey-protected SAM if the Syskey is lost or corrupted is to restore from this pre-Syskey backup of the SAM.
- Check the service pack level. Apply the most current service pack. (Service Pack 3 was the first service pack to incorporate Syskey.) Applying the most current service pack adds the code necessary to use Syskey.
- If you applied a service pack in step 2, you might want to make another backup of the Registry. Label this one as post-SP and pre-Syskey.
- From a command prompt, enter the Syskey.exe command.
- In the pop-up window, check the radio button to enable strong encryption.
- Select the choice of Syskey operations by selecting the radio button that matches your choice on the windows .
- If you have selected to enter a passphrase, do so now.
- If prompted, provide a floppy disk.
- Click OK.
- A pop-up window will indicate success.
- Reboot the system.
- Make a new backup of the Registry and label it post-Syskey.
- Repeat the process for each domain controller (the Syskey is not replicated) or Windows NT 4.0 workstation that is to be protected.

#### V. RESULTS AND DISCUSSIONS

This Screen Shots are showing the experimental Result and Discussion about project.

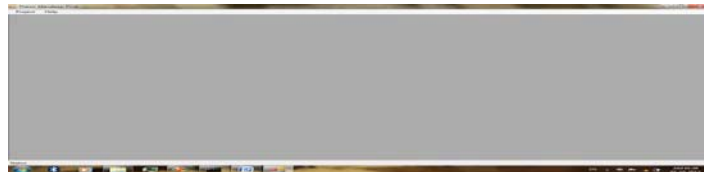


Figure No: - 6.1 Home Screen

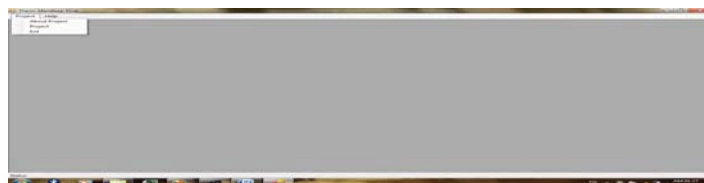


Figure No: - 6.2 Show Menu Items



Figure No: - 6.3 Show About Project

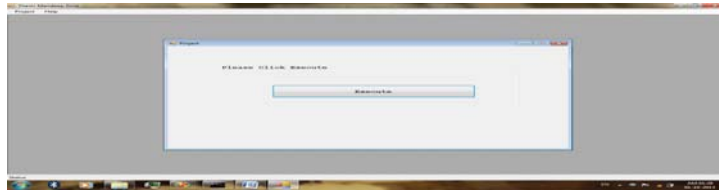


Figure No: - 6.4 Show How to Run Project

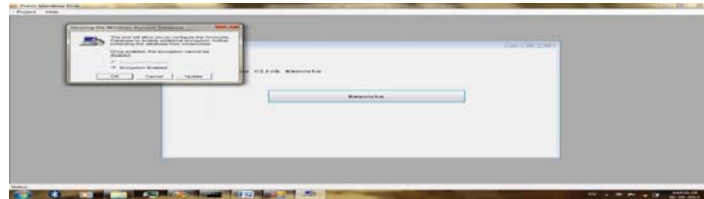


Figure No: - 6.5 Show the Steps

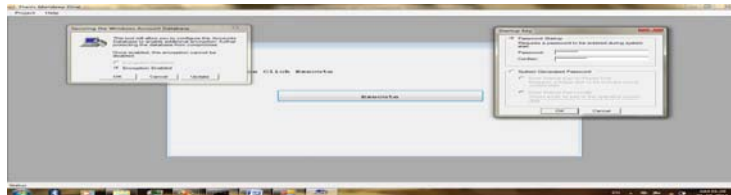


Figure No: - 6.6 Shows Set the Password

## VI. CONCLUSION

There is advantage and disadvantage in every Security Concepts. The fundamental concept is based on local security design strategy. Comparison of the two-concept of security design strategy is done on the basis of syskey concept and lsas.exe concept. After the study of all various design strategy we find that different concept and different requirement and have advantages and disadvantages depending on the different parameters and different technique. So I will provide best solution of LSA.

## VII. FUTURE SCOPE

Further research can be done to choose the best concept out of all design strategies for a particular problem considering all the parameters. In all the problems it is seen that many design strategies are tested and design are made using various techniques. If some guidelines are available regarding the suitability of a particular technique to a problem, then a lot of time can be named and designed may be developed only in that technique method.

## REFERENCES

- [1] Siti Rahayu S., Robiah Y., Shahrin S., Mohd Zaki M., Faizal M.A., and Zaheera Z.A., "Advanced Trace Pattern For Computer Intrusion Discovery", Journal of Computing, Volume 2, Issue 6, June 2010, Issn 2151-9617.
- [2] Michael Muckin, Lockheed Martin, "Window security Internal", Corporate Information Security Engineering, 2009.
- [3] EEEY: Windows Local Security Authority Service Remote Buffer Overflow, April 13, 2004.
- [4] US-CERT Technical Cyber Security Alert TA04-104A Multiple Vulnerabilities in Microsoft Products, US-CERT April 14, 2004.
- [5] Microsoft Security Bulletin MS04-011: Security Update for Microsoft Windows (835732), Microsoft Corporation April 13, 2004.
- [6] CAN-2003-0533, Common Vulnerabilities and Exposures (CVE).
- [7] Ryan Spangler, "Analysis of the Microsoft Windows LSASS Exploit" Packetwatch Research 2004.