Windows Security Environment

Motivation

- Popularity, widespread use of Windows
  - Big surface, big impact
- Protection via user/kernel architecture and CPU modes
- Multiple-users environment, same physical resources
- Easy to install < security > easy to use

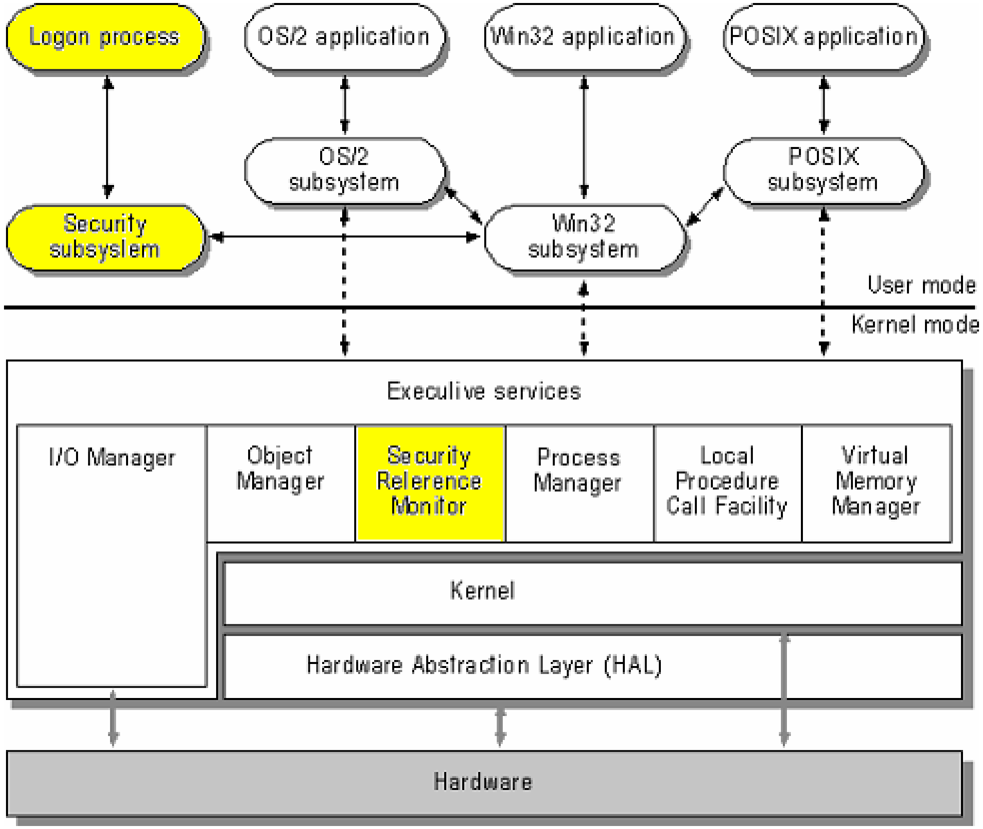
Windows Security Environment

Basic concepts

- Principal must be authenticated
  - Identification – Challenging the user
- Most OS objects are secured
  - Authorization – Enforcing rights on objects
- Owner of an object defines its security
  - Enforcing discretion
- Administrators define the security boundary
  - Management – Enforcing policy
- Administrators audit security-related events
  - Accountability – Tracking actions

Windows Security Environment

Security Subsystem



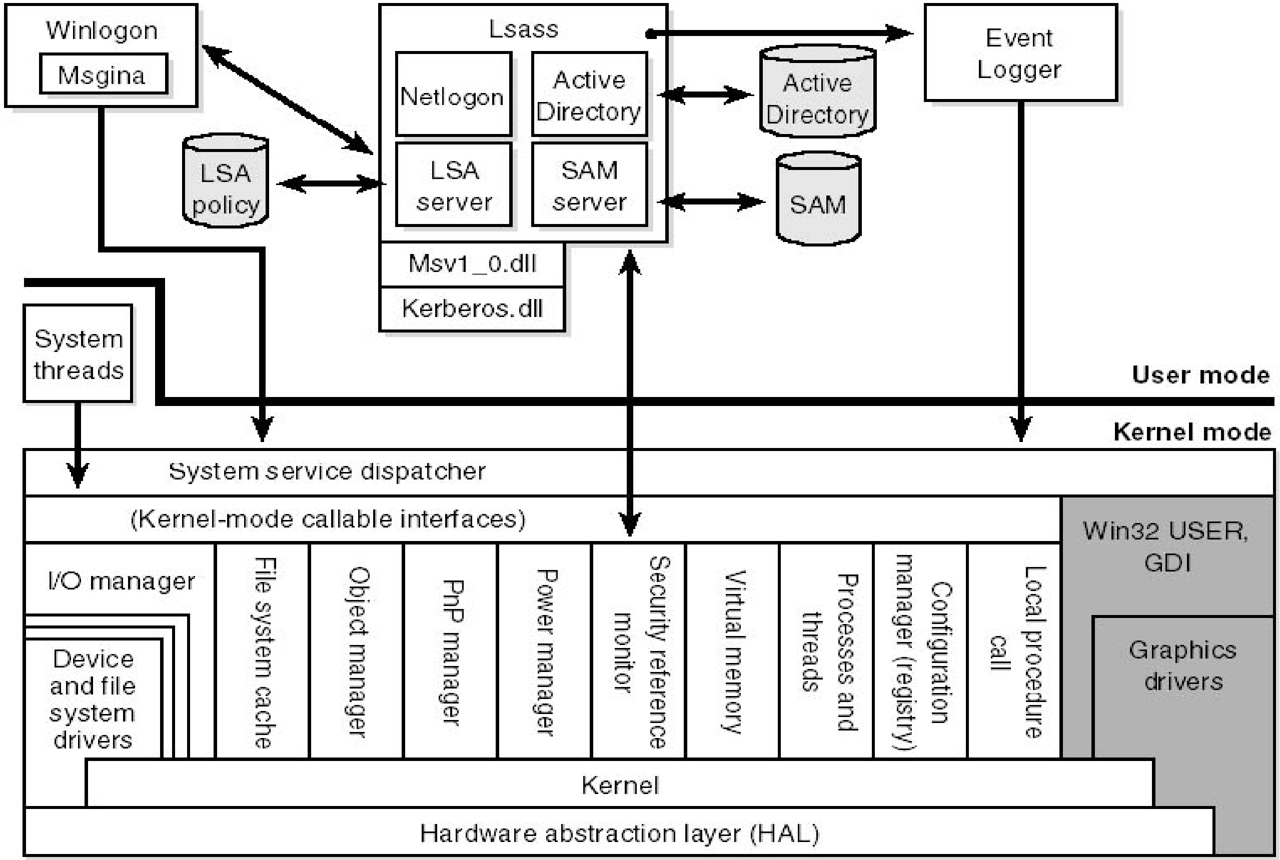
Windows Security Environment

Security System Components

- Security Reference Monitor (SRM)
  - Secured objects accesses validation, Event log audit messages management
- Local Security Authority Subsystem (LSASS)
  - Provide authentication
  - Local system policy, privileges and password management
  - Creation of local accounts
  - Creation of the Shell - User environment initialization
- Security Account Manager (SAM)
  - User names/groups accounts management
- Logon Process (Winlogon)
  - Provide protected interactive logon – SAS
    - Remove any UI, Place GINA, Capture Keyboard
  - Manage GINA Plug-ins
- Graphical Identification and Authentication (GINA)
  - User interface authentication management
- Net Logon service (NetLogon)
  - Domain locater
  - Authentication forwarder

Windows Security Environment

Security System Components



Windows Security Environment

Objects - Protection

- OS is “object oriented”
- Objects are protected by the SRM
- Common, uniform mechanisms for using system resources
- Central location for important tasks on objects
  - Provide human-readable names for system resources
  - Share resources and data among processes
  - Protect resources from unauthorized accesses
- Support of objects use and processes quota
- Uniform rules for object retention

Windows Security Environment

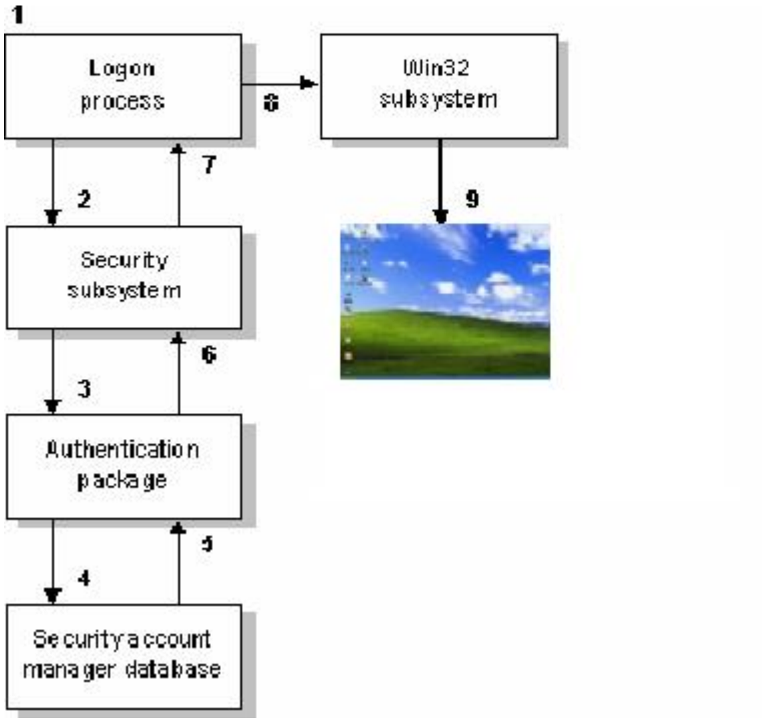
Object - Types

Type	Description
Process	Program invocation, including the address space and resources required to run the program
Thread	Executable entity within a process
Job	Collection of processes manageable as a single entity
Section	Region of shared memory
File	Instance of an opened file or I/O device
Port	Destination for messages passed between process
Access token	Security profile (user SID, user rights,…) of a process or a thread
Event	Object with a persistent state (signaled, not signaled) used for synchronization or notification
Semaphore	Counter that regulates the number of threads that can use a resource
Mutex	Synchronize (serialize) access to a resource
Timer	Notify a thread when a fixed period of time elapses
Symbolic link	Indirectly referencing an object
Key	Index key for referring to records in the configuration database (registry)
Window station	Contains a clipboard, a set of global atoms, and a group of desktop objects
Desktop	Contains windows, menus and hooks
Application object	Application private object

Windows Security Environment

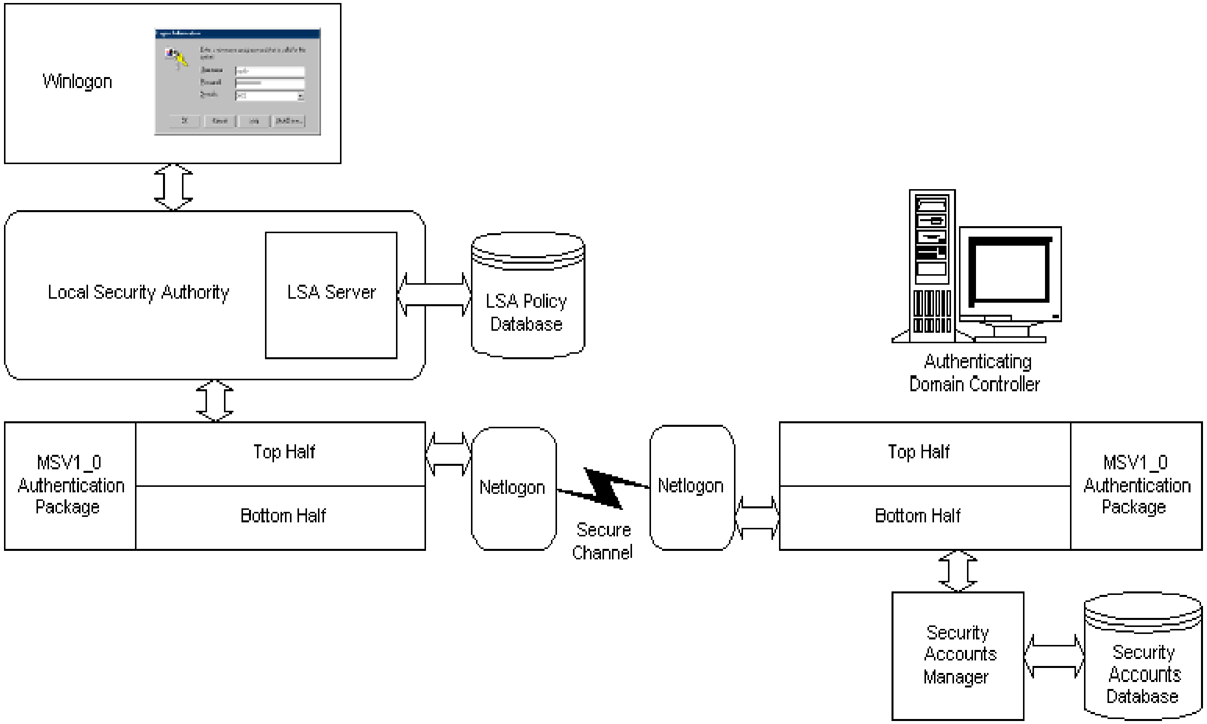
Local Authentication Request

- Steps that are taking place during a local logon



Remote Authentication Request

- Steps that are taking place during a remote logon


Winlogon
Local Security Authority
LSA Server
LSA Policy Database
MSV1_0 Authentication Package
Top Half
Bottom Half
Netlogon
Secure Channel
Netlogon
Authenticating Domain Controller
Top Half
Bottom Half
MSV1_0 Authentication Package
Security Accounts Manager
Security Accounts Database

Windows Security Environment

Security Information Storages

- Local Users, Groups and passwords (encrypted)
- Trusted domains names and passwords (encrypted)

Hive Name	Description	Files
HKLM\SAM	Security Access Manager data	SAM, SAM.LOG, SAM.SAV
HKLM\SECURITY	Accounts and Passwords data	SECURITY, SECURITY.LOG, SECURITY.SAV

Hive Name	Sub-key
HKLM\SECURITY\Policy\LSA\Secrets	$MACHINE.ACC

- GINA plugin

Key	Value
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDll	MyGina.dll

Logon Sessions

- Motivations
  - Access to a machine needs authentication
  - Access to secured resource needs new authentication
  - Access to remote secured resource needs new authentication
- Definitions
  - Documents a successful principal authentication (badge)
  - Represents principal appearance
  - Allows a principal to use secured resources
  - Contains principal credentials
  - Determines lifetime of a process
- Benefits
  - Comfort
  - Performance

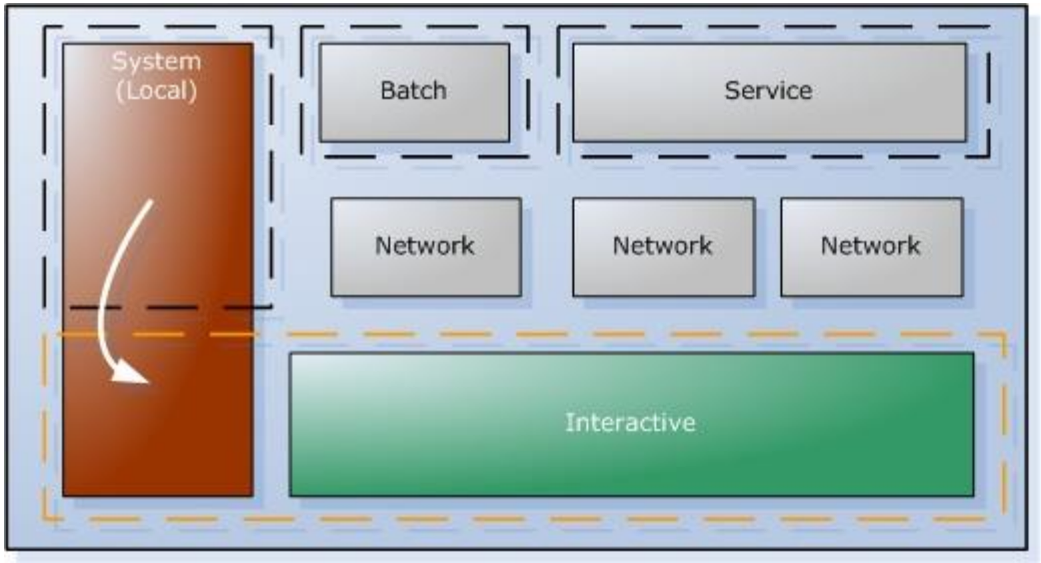
Logon Sessions Types

- System
  - House of the TCB’s (privileged) processes and boundary
  - First created (compulsory) and unique (boot)
  - Only one that can create other logon sessions
  - Last removed
- Network
  - Once per authenticated connection
  - Does not cache user identification (credentials misuse)
  - Cannot initiate a network authentication exchange (single hop)
- Batch and Services
  - Created by the SCM
  - House of the NT Services and DCOM objects
- Interactive
  - Created (on demand) when user successfully logs-on
  - Unique
  - House of all user’s processes
  - Only one that can interact with the user (desktop/keyboard/mouse events)
  - Caches user credentials to transparently respond to network authentication requests
  - Resource expensive
  - Removed when no more needed (user logs off)

Windows Security Environment

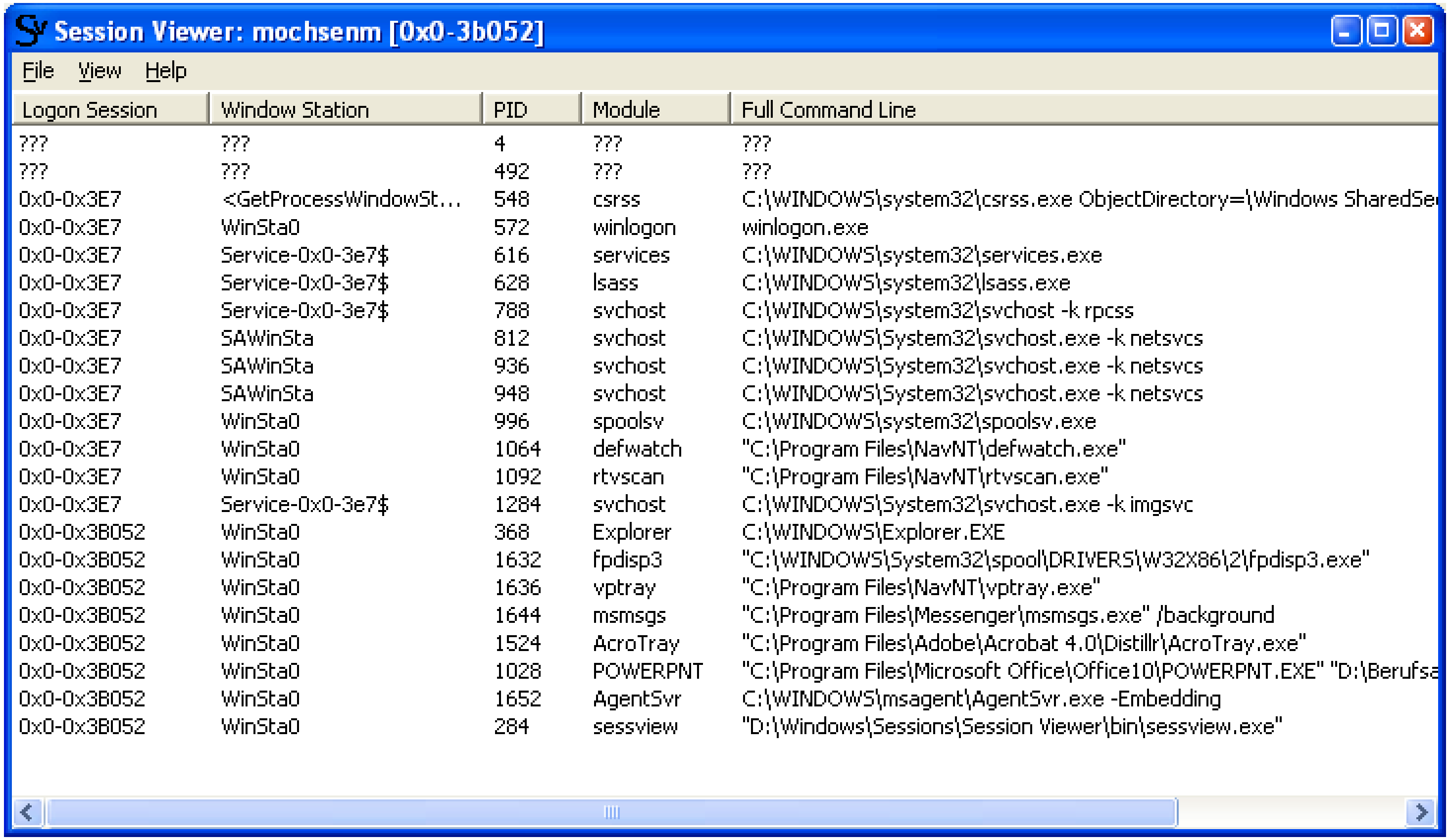
Logon Sessions Types

- Windows is fully functional without an interactive user
- Creation
  - Always
  - Most of the time
  - On demand
- Processes protection
- Processes boundaries



Windows Security Environment

Viewing the Logon sessions



Logon Session	Window Station	PID	Module	Full Command Line
???	???	4	???	???
???	???	492	???	???
0x0-0x3E7	<GetProcessWindowSt...	548	csrss	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSe
0x0-0x3E7	WinSta0	572	winlogon	winlogon.exe
0x0-0x3E7	Service-0x0-3e7$	616	services	C:\WINDOWS\system32\services.exe
0x0-0x3E7	Service-0x0-3e7$	628	lsass	C:\WINDOWS\system32\lsass.exe
0x0-0x3E7	Service-0x0-3e7$	788	svchost	C:\WINDOWS\system32\svchost -k rpcss
0x0-0x3E7	SAWinSta	812	svchost	C:\WINDOWS\System32\svchost.exe -k netsvcs
0x0-0x3E7	SAWinSta	936	svchost	C:\WINDOWS\System32\svchost.exe -k netsvcs
0x0-0x3E7	SAWinSta	948	svchost	C:\WINDOWS\System32\svchost.exe -k netsvcs
0x0-0x3E7	WinSta0	996	spoolsv	C:\WINDOWS\system32\spoolsv.exe
0x0-0x3E7	WinSta0	1064	defwatch	"C:\Program Files\NavNT\defwatch.exe"
0x0-0x3E7	WinSta0	1092	rtvscan	"C:\Program Files\NavNT\rtvscan.exe"
0x0-0x3E7	Service-0x0-3e7$	1284	svchost	C:\WINDOWS\System32\svchost.exe -k imgsvc
0x0-0x3B052	WinSta0	368	Explorer	C:\WINDOWS\Explorer.EXE
0x0-0x3B052	WinSta0	1632	fpdisp3	"C:\WINDOWS\System32\spool\DRIVERS\W32X86\2\fpdisp3.exe"
0x0-0x3B052	WinSta0	1636	vptray	"C:\Program Files\NavNT\vptray.exe"
0x0-0x3B052	WinSta0	1644	msmsgs	"C:\Program Files\Messenger\msmsgs.exe" /background
0x0-0x3B052	WinSta0	1524	AcroTray	"C:\Program Files\Adobe\Acrobat 4.0\Distillr\AcroTray.exe"
0x0-0x3B052	WinSta0	1028	POWERPNT	"C:\Program Files\Microsoft Office\Office10\POWERPNT.EXE" "D:\Berufsa
0x0-0x3B052	WinSta0	1652	AgentSvr	C:\WINDOWS\msagent\AgentSvr.exe -Embedding
0x0-0x3B052	WinSta0	284	sessview	"D:\Windows\Sessions\Session Viewer\bin\sessview.exe"

Windows Security Environment

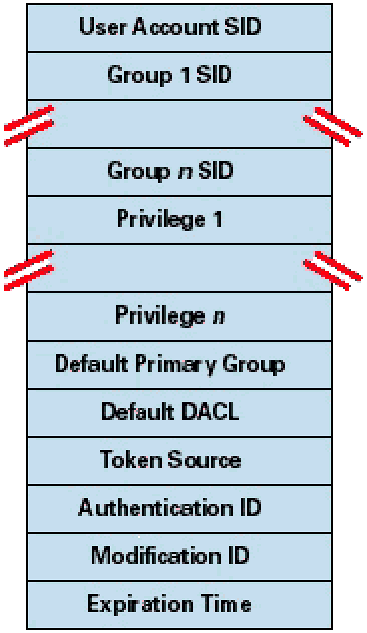
Access Token

- Motivation
  - Single security settings container for all processes (badge)
  - Allow process security customization without affecting other processes
  - Allow processes autonomy - every program inherits a copy of the initial token winlogon created
- Definition
  - Document privileges, accounts and groups associated with a process/thread
  - Visible area of a Logon session
  - Always associated with a single Logon session
- Benefits
  - Use protected resource without caring about security
  - Consistent security settings policy by keeping default settings centralized - CreateFile(...LPSECURITY_ATTRIBUTES...)

Windows Security Environment

Anatomy of a Token

- User Account SID
  - Principal behind the process/thread
- Group(s) SID(s)
  - List of groups User’s account is member of
- Privileges
  - List of (collection) rights associated with the token
- Default DACL
  - List of “who can do what” applied when a
  - process/thread does not explicitly provide it
- Expiration Time
  - Period of time before expiring
  - Unused since NT3.1
- No SACL!
  - SACL are given at administrator’s discretion



User Account SID

Group 1 SID

Group *n* SID

Privilege 1

Privilege *n*

Default Primary Group

Default DACL

Token Source

Authentication ID

Modification ID

Expiration Time

Windows Security Environment

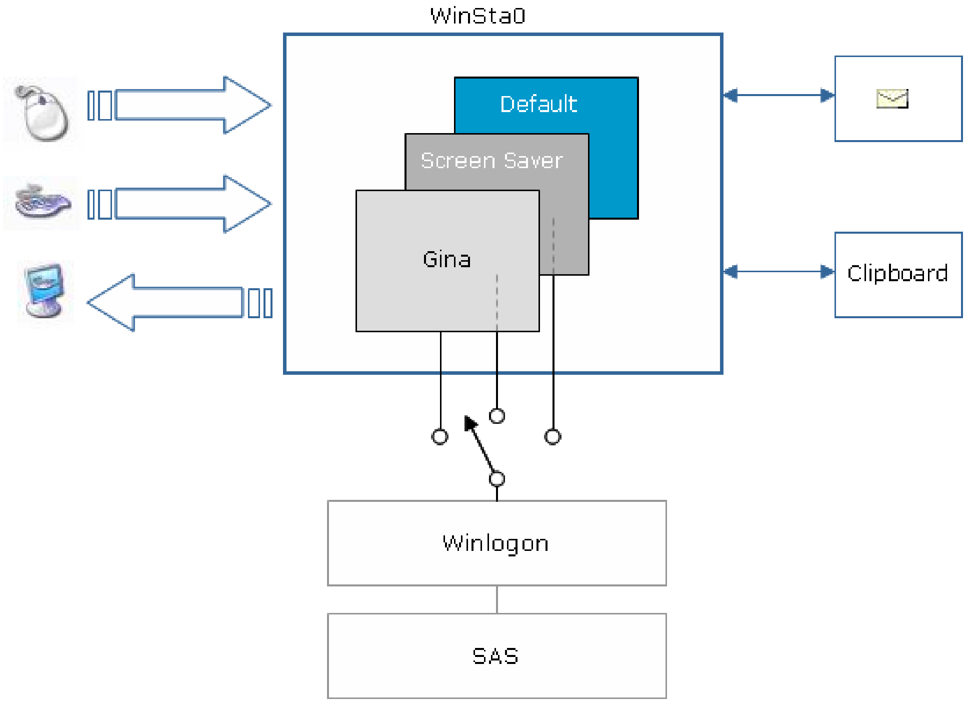
Window stations

- Motivation
  - Windows message-based attack from another process
  - Just as pointers are process relative, handles are window station relative
  - Create sandbox Windows objects are living in
- Advantage
  - Increases the programming comfort.
    - Windows are objects and yet CreateWindowEx(…) API does not need a reference to a Security Descriptor. .
    - CreateWindowStation(..) API references a Security Descriptor!

Windows Security Environment

Desktops

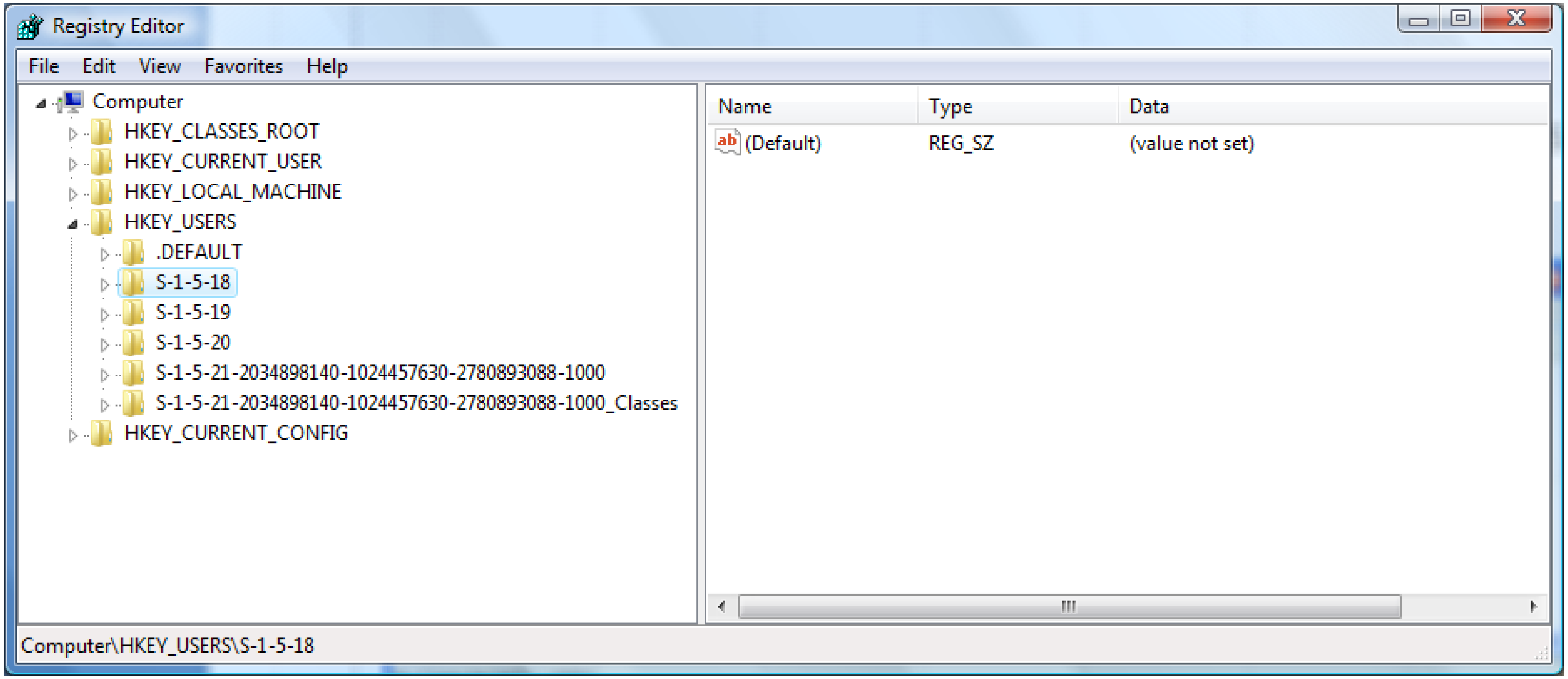
- A desktop contains all screens of a specific session.



Windows Security Environment

Profiles

- Principals using system resources are associated with a profile



Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_USERS\S-1-5-18

Windows Security Environment

Links

- Programming NT Security (Addison-Wesley, Keith Brown)
- Windows NT Security (R&D Books Miller Freeman, N.Okuntseff)
- Windows NT Security Guide (Addison Wesley, Stephen A. Sutton)
- Windows Internals (Microsoft Press, Russinovich)
- Secure Networking with Windows 2000 and Trust Services (Addison Wesley, Jalal Feghhi and Jalil Feghhi)
- Modern Operating Systems – Second Edition (Prentice Hall, Tanenbaum)