Chapter 24 – Windows and Windows Vista Security

First Edition
by William Stallings and Lawrie Brown

Lecture slides by Lawrie Brown
Windows and Windows Vista Security

- Windows is the world’s most popular O/S
- Advantage is that security enhancements can protect millions of nontechnical users
- Challenge is that vulnerabilities in Windows can also affect millions of users
- Will review overall security architecture of Windows 2000 and later (but not Win9X)
- Then security defenses built into Windows
Windows Security Architecture

- **Security Reference Monitor (SRM)**
  - a kernel-mode component that performs access checks, generates audit log entries, and manipulates user rights (privileges)

- **Local Security Authority (LSA)**
  - responsible for enforcing local security policy

- **Security Account Manager (SAM)**
  - a database that stores user accounts and local users and groups security information
  - local logins perform lookup against SAM DB
  - passwords are stored using MD4
Windows Security Architecture

- Active Directory (AD)
  - Microsoft’s LDAP directory
  - all Windows clients can use AD to perform security operations including account logon
  - authenticate using AD when the user logs on using a domain rather than local account
  - user’s credential information is sent securely across the network to be verified by AD

- WinLogon (local) and NetLogon (net) handle login requests
Local vs Domain Accounts

- a networked Windows computer can be:
  - domain joined
    - can login with either domain or local accounts
    - if local may not access domain resources
    - centrally managed and much more secure
  - in a workgroup
    - a collection of computers connected together
    - only local accounts in SAM can be used
    - no infrastructure to support AD domain
Windows Login Example

- domain admin adds user’s account info (name, account, password, groups, privileges)
- account is represented by a Security ID (SID)
  - unique to each account within a domain
  - of form: S-1–5–21-AAA-BBB-CCC-RRR
- username in one of two forms:
  - SAM format: DOMAIN\Username
  - User Principal Name (UPN): username@domain.company.com
- login using username & password or smartcard
- issued with token (SID, groups, privileges)
  - assigned to every process run by user
Windows Privileges

- are systemwide permissions assigned to user accounts
  - e.g. backup computer, or change system time
- some are deemed “dangerous” such as:
  - act as part of operating system privilege
  - debug programs privilege
  - backup files and directories privilege
- others are deemed “benign” such as
  - bypass traverse checking privilege
Access Control Lists

- two forms of access control list (ACL):
  - Discretionary ACL (DACL)
    - grants or denies access to protected resources such as files, shared memory, named pipes etc
  - System ACL (ACL)
    - used for auditing and in Windows Vista to enforce mandatory integrity policy
Access Control Lists

- Objects needing protection are assigned a DACL (and possible SACL) that includes:
  - SID of the object owner
  - List of access control entries (ACEs)

- Each ACE includes a SID & access mask

- Access mask could include ability to:
  - Read, write, create, delete, modify, etc

- Access masks are object-type specific
  - E.g. Service abilities are create, enumerate
Security Descriptor (SD)

- data structure with object owner, DACL, & SAACL
  - e.g.
    - Owner: CORP\Blake
    - ACE[0]: Allow CORP\Paige Full Control
    - ACE[1]: Allow Administrators Full Control
    - ACE[2]: Allow CORP\Cheryl Read, Write and Delete

- have no implied access, if there is no ACE for requesting user, then access is denied

- applications must request correct type of access
  - if just request “all access” when need less (e.g. read) some user’s who should have access will be denied
More SD’s & Access Checks

- each ACE in the DACL determines access
- an ACE can be an allow or a deny ACE
- Windows evaluates each ACE in the ACL until access is granted or explicitly denied
- so deny ACEs come before allow ACEs
  - default if set using GUI
  - explicitly order if create programmatically
- when user attempts to access a protected object, the O/S performs an access check
  - comparing user/group info with ACE’s in ACL
Impersonation

- process can have multiple threads
  - common for both clients and servers
- impersonation allows a server to serve a user, using their access privileges
  - e.g. ImpersonateNamedPipeClient function sets user’s token on the current thread
  - then access checks for that thread are performed against this token not server’s
  - with user’s access rights
Mandatory Access Control

- have Integrity Control in Windows Vista
- that limits operations changing an object’s state
- objects and principals are labeled (using SID) as:
  - Low integrity (S-1-16-4096)
  - Medium integrity (S-1-16-8192)
  - High integrity (S-1-16-12288)
  - System integrity (S-1-16-16384)
- when write operation occurs first check subject’s integrity level dominates object’s integrity level
- much of O/S marked medium or higher integrity
Vista User Account
Windows Vulnerabilities

- Windows, like all O/S’s, has security bugs
  - and bugs have been exploited by attackers to compromise customer operating systems
- Microsoft now uses process improvement called the Security Development Lifecycle
  - net effect approx 50% reduction in bugs
- Windows Vista used SDL start to finish
- IIS v6 (in Windows Server 2003) had only 3 vulnerabilities in 4 years, none critical
Windows Security Defenses

- Attackers are now criminals rather than young, anarchic miscreants, and are highly motivated by money.
- Have categories of security defenses:
  - Account defenses
  - Network defenses
  - Buffer overrun defenses
  - Browser defenses
Windows System Hardening

- process of shoring up defenses, reducing exposed functionality, disabling features
  - known as attack surface reduction
  - use 80/20 rule on features
  - not always achievable
  - e.g. requiring RPC authentication in XP SP2
  - e.g. strip mobile code support on servers

- servers easier to harden:
  1. are used for very specific and controlled purposes
  2. perceive server users are administrators with better computer configuration skills than typical users
Account Defenses

- User accounts can have privileged SIDs.
- Least privilege dictates that users operate with just enough privilege for tasks.
- Windows XP users in local Administrators:
  - For application compatibility reasons.
  - Can use “Secondary Logon” to run apps.
  - Also restricted tokens reduce per-thread privilege.
- Windows Vista reverses default with UAC:
  - Users prompted to perform a privileged operation.
  - Unless admin on Server.
Low Privilege Service Accounts

- Windows services are long-lived processes started after booting
  - many ran with elevated privileges
  - but many do not need elevated requirements
- Windows XP added Local Service and Network service accounts
  - allow a service local or network access
  - otherwise operate at much lower privilege level
- Windows XP SP2 split RPC service (RPCSS) in two (RPCSS and DCOM Server Process)
  - example of least privilege in action, see also IIS6
Stripping Privileges

- another defense is to strip privileges from an account soon after an application starts
  - e.g. Index server process runs as system to access all disk volumes
  - but then sheds any unneeded privileges as soon as possible
  - using AdjustTokenPrivileges

- Windows Vista can define privileges required by a service
  - using ChangeServiceConfig2
Network Defenses

- need more than user defenses
- vulnerable to attack via network service
- have IPSec and IPv6 with authenticated network packets enabled by default in Windows Vista
  - IPv4 also enabled by default, expect less use
- have built-in software firewall
  - block inbound connections on specific ports
    - Vista can allow local net access only
  - optionally block outbound connections (Vista)
  - default was off (XP) but now default on (Vista)
Buffer Overrun Defenses

- many compromises exploit buffer overruns
- Windows Vista has “Stack-Based Buffer Overrun Detection (/GS)” default enabled
  - source code compiled with special /GS option
  - does not affect every function; only those with at least 4-bytes of contiguous stack data and that takes a pointer or buffer as an argument
- defends against “classic stack smash”
Windows Stack and /GS flag

(a) Without /GS option

(b) With /GS option
Buffer Overrun Defenses

- No eXecuteNamed (NX) / Data Execution Prevention (DEP) / eXecution Disable (XD)
  - prevent code executing in data segments
  - as commonly used by buffer overrun exploits
  - applications linked with /NXCOMPAT option
- Stack Randomization (Vista only)
  - randomizes thread stack base addresses
- Heap-based buffer overrun defenses:
  - add and check random value on each heap block
  - heap integrity checking
  - heap randomization (Vista only)
Other Defenses

- **Image Randomization**
  - O/S boots in one of 256 configurations
  - makes O/S less predictable for attackers

- **Service Restart Policy**
  - services can be configured to restart if fail
  - great for reliability but lousy for security
  - Vista sets some critical services so can only restart twice, then manual restart needed
  - gives attacker only two attempts
Browser Defenses

- Web browser is a key point of attack
  - via script code, graphics, helper objects
- Microsoft added many defenses to IE7
  - ActiveX opt-in
    - unloads ActiveX controls by default
    - when any then first run prompts user to confirm
  - protected mode
    - IE runs at low integrity level (see earlier)
    - so more difficult for malware to manipulate O/S
Cryptographic Services

- low-level crypto for encryption, hashing, signing
- Encrypting File System (EFS)
  - allows files / directories to be encrypted / decrypted transparently for authorized users
  - generates random key, protected by DPAPI
- Data Protection API (DPAPI)
  - manages encryption key maintenance protection
  - keys derived in part from user’s password
- BitLocker Drive Encryption
  - encrypts an entire volume with AES
  - key either on USB or TPM chip
Summary

- Windows security architecture
- Vulnerabilities
- Security defenses
  - account, network, buffer, browser
- Crypto services