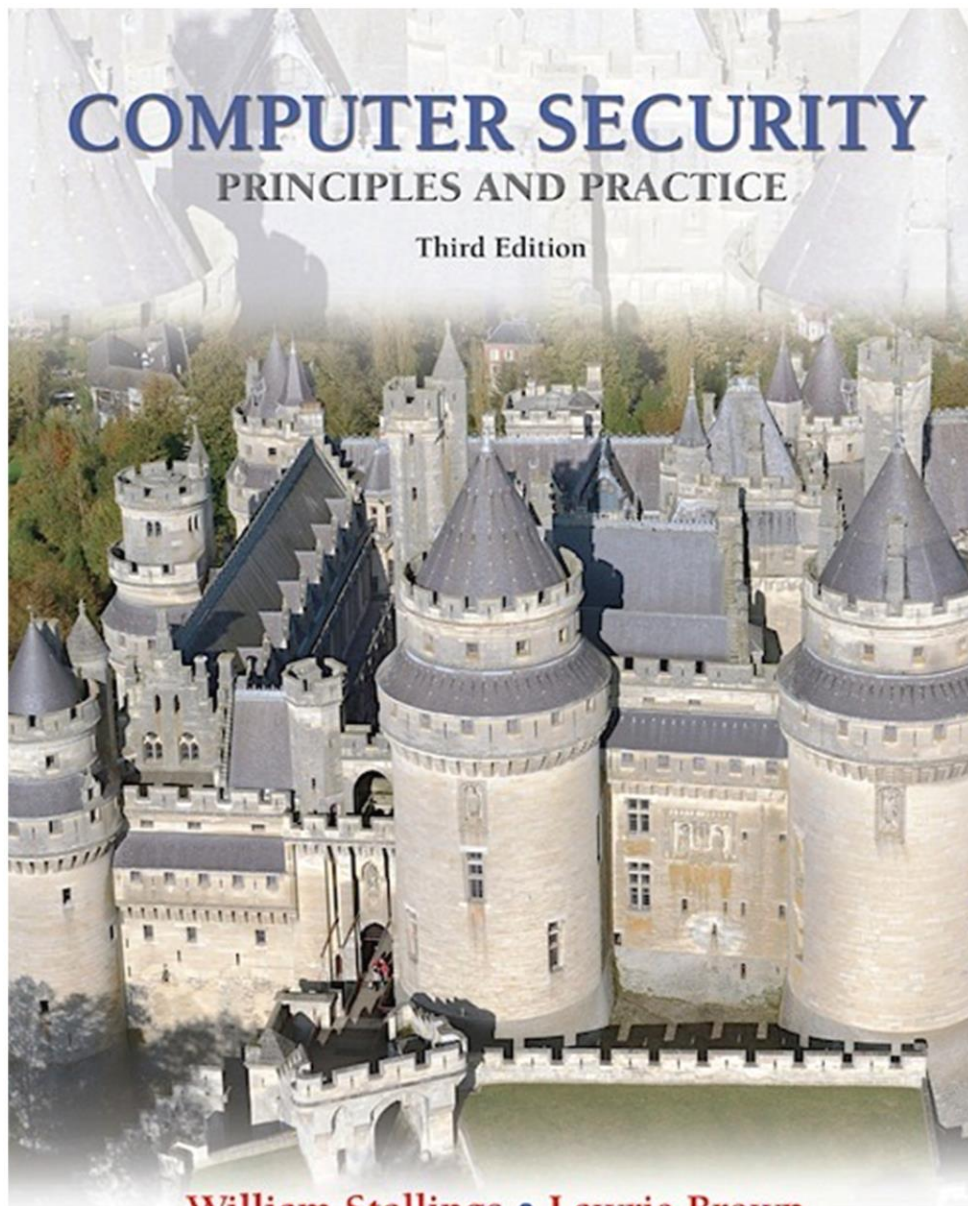


COMPUTER SECURITY

PRINCIPLES AND PRACTICE

Third Edition



William Stallings • Lawrie Brown



Chapter 26

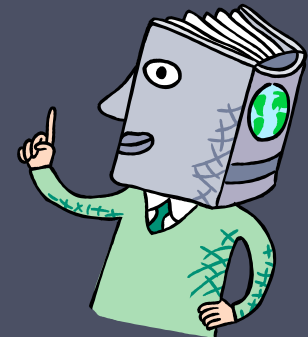
Windows Security

Contributed by:
Michael Howard
Senior Security Program Manager
Microsoft Corporation

© 2016 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Fundamental Windows Security Architecture

- Anyone who wants to understand Windows security must have knowledge of the basic fundamental security blocks in the operating system
- Some of the components in Windows that make up the fundamental security infrastructure are:
 - The Security Reference Monitor (SRM)
 - The Local Security Authority (LSA)
 - The Security Account Manager (SAM)
 - Active Directory (AD)
 - Authentication Packages
 - WinLogon and NetLogon



Fundamental Windows Security Architecture

The Security Reference Monitor (SRM)

- This kernel-mode component performs access checks, generates audit log entries, and manipulates user rights (also called privileges)
- Ultimately every permission check is performed by the SRM
- Most modern operating systems include SRM type functionality that performs privileged permission checks
- SRMs tend to be small in size so their correctness can be verified

The Local Security Authority (LSA)

- Resides in a user-mode process named lsass.exe and is responsible for enforcing local security policy in Windows
- It also issues security tokens to accounts so they log on to the system
- Security policy includes:
 - Password policy (such as complexity rules and expiration times)
 - Auditing policy (which operations on what objects to audit)
 - Privilege settings (which accounts can perform privileged operations)

Fundamental Windows Security Architecture

The Security Account Manager (SAM)

- Is a database that stores accounts data and relevant security information about local principals and local groups
- When a user logs on to a computer using a local account the SAM process takes the logon information and performs a lookup against the SAM database
- If the credentials match the user can log on to the system
- The SAM file is binary rather than text, and passwords are stored using the MD4 hash algorithm
- On Windows Vista and later, the SAM stores password information using a password-based key derivation function (PBKCS) which is substantially more robust against password guessing attacks than MD4

Active Directory (AD)

- Microsoft's LDAP directory included with Windows Server 2000 and later
- All currently supported client versions of Windows, including Windows XP and Windows 7, can communicate with AD to perform security operations including account logon
- A Windows client will authenticate using AD when the user logs on to the computer using a domain account rather than a local account

Fundamental Windows Security Architecture

Local versus Domain Accounts

- A networked Windows computer can be in one of two configuration: either domain joined or in a workgroup
- When a computer is domain joined users can gain access to that computer using domain accounts, which are centrally managed in AD
- They can also log on using local accounts but local accounts may not have access to domain resources such as networked printers, Web servers, e-mail servers, etc.
- When a computer is in a workgroup only local accounts can be used, held in the SAM
- A domain has the major advantage of being centrally managed and as such is more secure, users' accounts can be disabled centrally rather than on all individual computers, and security policies are also centrally managed when using AD
- The only advantage of using local accounts is that a computer does not need the infrastructure required to support a domain using AD
- In a workgroup (collection of computers connected to one another using a network) the machines use only local accounts
- The difference between a workgroup and a domain is simply where accounts are authenticated
- A workgroup has no domain controllers, authentication is performed on each computer, and a domain authenticates accounts at domain controllers running AD

Using PowerShell for Security Administration

Windows 7 and Windows Server 2008 and later include an incredibly flexible scripting language named PowerShell

Core things to know about PowerShell:

- PowerShell is based on .NET. If you can do it in C# or VB.NET you can do it in a PowerShell environment
- Commands in PowerShell are called cmdlets and have a consistent verb-noun syntax
- Like all scripting environments PowerShell supports piping output from one command to another. Unlike other scripting environments, PowerShell pipes objects not text. This allows for very rich data processing, filtering and analysis

Windows Security Basics – End-to-End Domain Example

Before a user can log on to a Windows network a domain administrator must add the user's account information to the system (includes the user's name, account name, and password)

After the administrator has entered this information Windows creates an account for the user in the domain controller running Active Directory

Each user account is uniquely represented by a Security ID (SID)

SIDs are unique within a domain and every account gets a different SID

Security ID (SID)

A user account's SID is of the following form:

S -1 -5 -21 – AAA –BBB – CCC – RRR

S simple means SID

1 is the SID version number

5 is the identifier authority (in this example, 5 is SECURITY_NT_AUTHORITY)

21 means “not unique,” which just means there is no guarantee of uniqueness, however, a SID is unique within a domain

AAA-BBB-CCC is a unique number representing the domain

RRR is called a relative ID (RID) – it's a number that increments by 1 as each new account is created. RIDs are never repeated, thus making each SID unique

Username

In Windows a username can be in one of two formats:

- The SAM format ---- is supported by all versions of Windows and is of the form DOMAIN\Username
- User Principal Name (UPN) and looks more like an RFC822 e-mail address (username@domain.company.com)

The SAM name should be considered a legacy format

Assuming the user logs on correctly, a token is generated by the operating system and assigned to the user

If the user enters just a username then the domain in which the machine resides is pre-pended to the user name

A token contains the user's SID, group membership information, and privileges

The user's token is assigned to every process run by the user

Privileges in Windows

- Privileges are essentially system-wide permissions assigned to user accounts
- Some privileges are deemed “dangerous”, which means a malicious account that is granted such a privilege can cause damage
- Examples of dangerous privileges include:
 - Act as part of operating system privilege
 - This is the most dangerous privilege in Windows and is granted only the Local System account; even administrators are not granted this privilege
 - Debug programs privilege
 - This privilege basically means a user can run any code he or she wants in any running process
 - Backup files and directories privilege
 - Any process running with this privilege will bypass all access control list checks

Access Control List (ACL)

Windows has two forms of ACL:

- Discretionary ACL (DACL)
 - Usually what most people mean when they say ACL
 - Grants or denies access to protected resources in Windows such as files, shared memory, named pipes, etc.
- System ACL (SACL)
 - Used for auditing
 - In Windows Vista used to enforce mandatory integrity policy

Two important things to keep in mind about access control in Windows:

- There is no implied access
- When a Windows application accesses an object, it must request the type of access the application requires

Objects that require protection are assigned a DACL (and possibly a SACL) which includes the SID of the object owner (usually the object creator) as well as a list of ACEs

ACEs

- Access control entries
- Each ACE in the DACL determines access; and an ACE can be an allow ACE or a deny ACE
- Includes a SID and an access mask (an access mask could include the ability to read, write, create, delete, modify)

Access Controls

- When a user account attempts to access a protected object the operating system performs an access check
- It compares the user account and group information in user's token and the ACEs in the object's ACL
- If all requested operations are granted, then access is granted, otherwise the user gets an access denied error status

Impersonation



Windows is a multithreaded operating system, which means a single process can have more than one thread of execution at a time

This is very common for both server and client applications

Impersonation means setting the user's token on the current thread

When a thread is impersonating a user, the user's token is assigned to the thread, and the access check for that thread is performed against the token on the thread, not the process token

When the connection is done, the thread "reverts" (the token is dropped from the thread)

With impersonation it is possible to restrict who can do what to the db.tx file

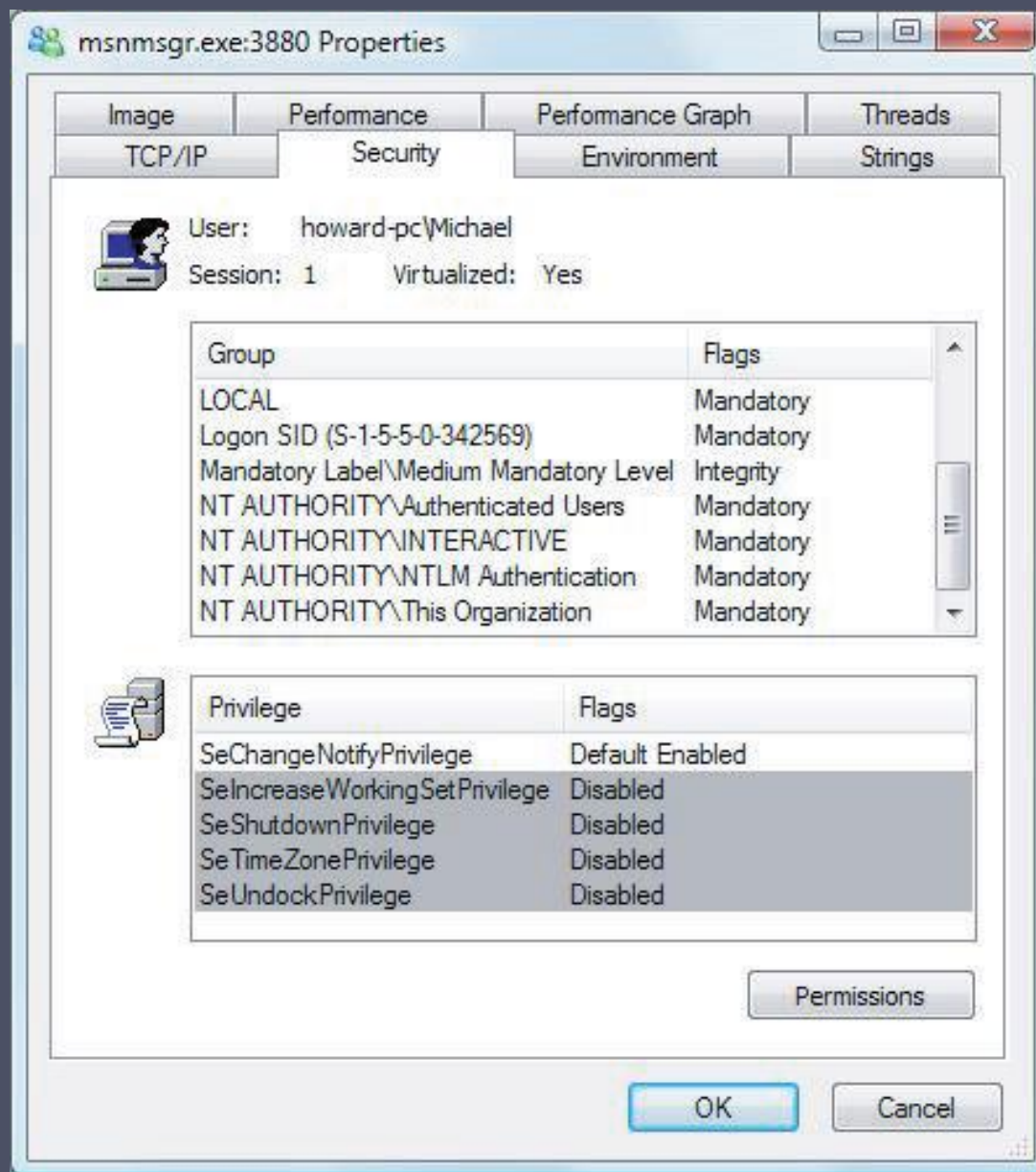


Figure 26.1 Screen Shot of User Account in Windows Vista

Windows Vulnerabilities

- After 2001 Microsoft decided to change its software development process to better accommodate secure design, coding, testing, and maintenance requirements with the goal of reducing the number of vulnerabilities in all Microsoft products
- Security Development Lifecycle core requirements
 - Mandatory security education
 - Secure design requirements
 - Threat modeling
 - Attack surface analysis and reduction
 - Secure coding requirements and tools
 - Secure testing requirements and tools
 - Security push
 - Final security review
 - Security response

Windows Security Defenses

The defenses with Windows can be grouped into four broad categories

Account defenses

Network defenses

Memory corruption defenses

Browser defenses

Windows System Hardening Overview

The process of hardening is the process of shoring up defenses, reducing the amount of functionality exposed to untrusted users, and disabling less-used features

This process is called Attack Surface Reduction

80/20 rule – if the feature is not used by 80% of the population then the feature should be disabled by default


One of the simplest and effective ways to reduce attack surface is to replace anonymous networking protocols with authenticated networking protocols

Windows Server 2003 is a server and not a client platform, the Web browser Internet Explorer was stripped of all mobile code support by default

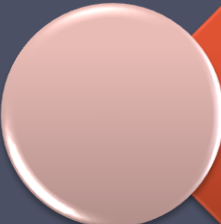
Account Defenses



Principle of least privilege dictates that users should operate with just enough privilege to get the tasks done, and no more



Windows XP and Windows Server 2003 add a feature named “Secondary Logon” which allows a user account to right click an application, select “run as....”, and then enter another user account and password to run the application



Restricted token is a thread token with privileges removed and/or SIDs marked as deny-only SIDs



User Account Control (UAC)

- When a user wants to perform a privileged operation, the user is prompted to enter an administrator’s account name and password
- If the user is an administrator, the user is prompted to consent to the operation
- Often referred to as “over the shoulder logon”

Low Privilege Service Accounts

- The Local Service account and the Network service account allow a service local or network access, but processes running with these accounts operate at a much lower privilege level
 - Neither of these accounts are members of the local administrator's group
- RPCSS
 - Ran as the System account (the most privileged account in Windows) in versions of Windows prior to Windows XP SP2
 - In XP SP2 RPCSS was split in two and a new service called the DCOM Server Process launcher was created ---- RPCSS runs as the lower-privilege Network service account and DCOM runs as SYSTEM
 - Apache, OpenSSH, and Internet Information Services (IIS)6 and later also use this model
 - A small amount of code runs with elevated identity and related components run with lower identity

Stripping Privileges

Another useful defense is to strip privileges from an account when the application starts and should be performed very early in the application startup code (*AdjustTokenPrivileges*)

Windows Vista and later also add a function to define the set of privileges required by a service to run correctly (*ChangeServiceConfig2*)

Network Defenses – IPSec and IPv6

- The reason distributed denial-of-service (DDoS) attacks occur is because IPv4 is an unauthenticated protocol
- UDP is one of the worst offenders because it's a connectionless protocol
- Even with TCP the initial SYN packet is unauthenticated and a set of attack servers could easily incapacitate a vulnerable server on the Internet by sending millions of bogus TCP SYN packets
- IPSec and IPv6 both support authenticated network packets

Network Defenses – Firewall

- All versions of Windows since XP have included a built-in software firewall
- The version included with XP was limited in that:
 - It was not enabled by default
 - Its configuration was limited to blocking only inbound connections on specific ports
- Changes in XP SP2
 - Option to open a port to the Internet --- but only on the local subnet --- in order for users with multiple computers in the home to share files and print documents
 - The firewall is enabled by default
- Changes in Vista and later
 - The firewall is a fully integrated component of the rewritten TCP/IP networking stack
 - The firewall supports optionally blocking outbound connections

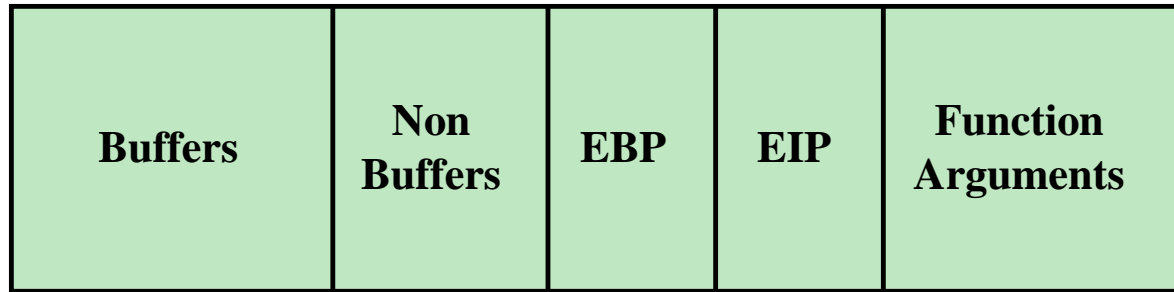
Memory Corruption Defenses

Most operating systems and software used today is written in the C and C++ programming languages

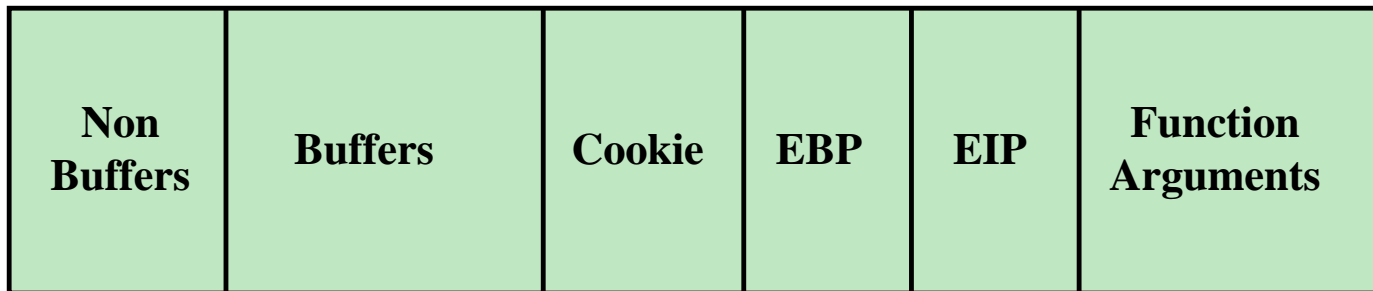
C was designed as a high-level assembly language, and because of that, gives the developer direct access to memory through pointers and with this functionality comes the risk of having the ability to corrupt memory

Converting C and C++ to another language would be a monumental task and does not solve the real problem of software developers having too much trust in the data they receive

You have memory corruption vulnerabilities when the application does not constrain write operations to the correct memory locations



(a) Without /GS option



(b) With /GS option

Figure 26.2 Stack Layout in Windows Vista

No EXecute

Named NX by Advanced Micro Devices (AMD), Data Execution Prevention (DEP) by Microsoft, and eXecution Disable (XD) by Intel, this technology requires CPU support that helps prevent code from executing in data segments

Most modern Intel CPUs support the capability today, and all current AMD CPUs support NX

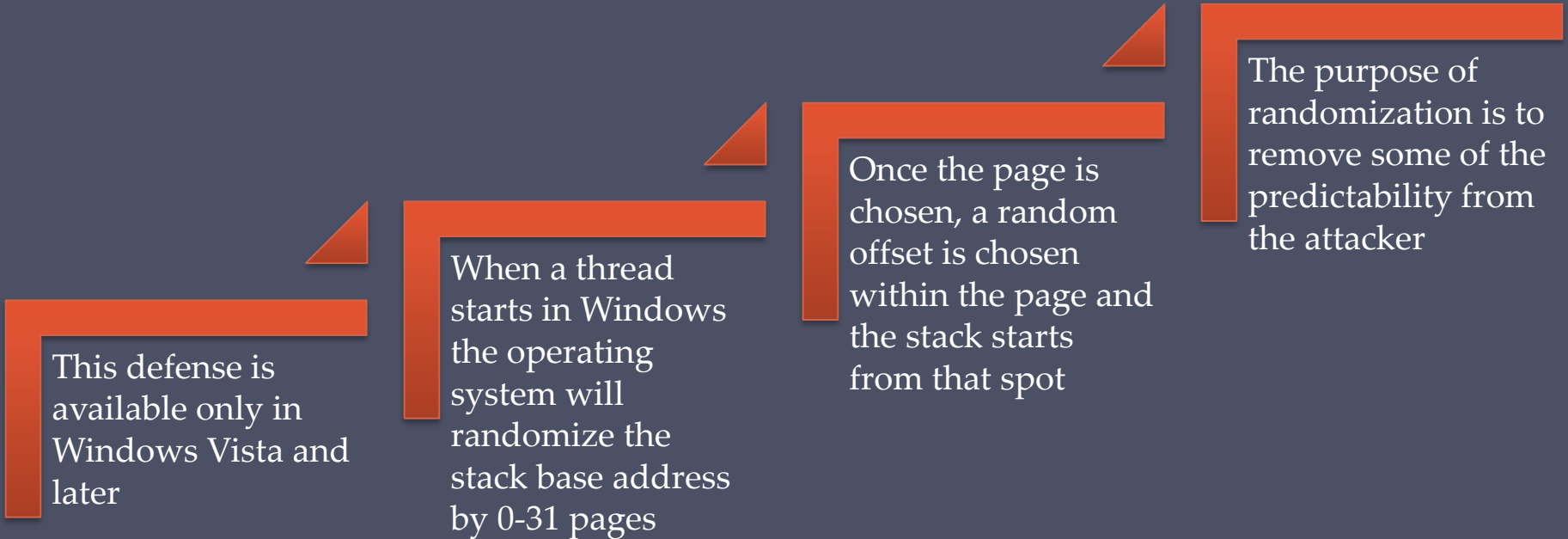
ARM-based CPUs also support NX

DEP support was first introduced in Windows XP SP2 and is critically important defense in Windows

The goal of NX is to prevent data executing

By default, most system components in Windows and applications can use NX by linking with the /NXCOMPAT linker option

Stack Randomization



This defense is available only in Windows Vista and later

When a thread starts in Windows the operating system will randomize the stack base address by 0-31 pages

Once the page is chosen, a random offset is chosen within the page and the stack starts from that spot

The purpose of randomization is to remove some of the predictability from the attacker

Heap-Based Buffer Overrun Detection

- Heap-based buffer overruns are exploitable and can lead to code execution
- The first heap defense, added to XP SP2, is to add a random value to each heap block and detect that this cookie has not been tampered with
 - If the cookie has changed the heap has been corrupted and the application could be forced to crash
 - Note: the application crash is not due to instability in the application caused by data corruption, rather the heap manager detects the corruption and fails the application
 - The process of shutting down an application in this manner is often called “failstop”
- The second defense is heap integrity checking
 - When heap blocks are freed, metadata in the heap data structures are checked for validity, and if the data are compromised, either the heap block is leaked or the application crashes

Heap randomization

Designed to take some of the predictability away from the attacker

When a heap is created the start of the heap is offset by 0-4 MB

This feature is new to Windows Vista

Image randomization

When the operating system boots, it starts up in one of 256 configurations (in other words, the entire operating system is shifted up or down in memory when it is booted)

This makes the operating system less predictable for attackers and makes it less likely that an exploit will succeed

Service restart policy

In Vista, Microsoft set some of the critical services to restart only twice, after which the service will not restart unless the administrator manually restarts the service

This gives the attacker only two attempts to get the attack to work

Browser Defenses

- A malicious Web page could take advantage of many possible attack vectors
 - Code and data makes for a rich and productive end-user environment but it is hard to secure
 - Web browsers can also render various multimedia objects; many file formats are rendered by helper objects called MIME handlers
- ActiveX opt-in
 - New feature added by Internet Explorer
 - Essentially unloads ActiveX controls by default, and when a control is used for the first time, the user is prompted to allow the control to run
- Protected mode
 - When this default configuration is used Internet Explorer runs at low integrity level, making it more difficult for malware to manipulate the operating system, which operates at a medium or higher integrity level
- ASLR and DEP
 - Current versions of Internet Explorer also enable these by default

Browser Defenses

- It is important to point out that Protected Mode, DEP and ASLR only help mitigate against memory corruption vulnerabilities, they do not help protect against Phishing attacks or common web-specific vulnerabilities such as cross-site scripting (XSS)
- Microsoft added defenses to Internet Explorer to help address these issues
 - First, a cross-site scripting detection logic to help detect and prevent some classes of XSS
 - The second defense is a phishing filter --- when a user visits a web site, the site's URL is sent to a service that determines if the site is a known phishing or malware distribution site and the user is warned if the site is suspicious
 - A final defense to help prevent users being tracked is a privacy-enhancing mode named InPrivate mode, which does not persist cookies or site history

Cryptographic Services – Encrypting File System (EFS)



EFS allows files and directories to be encrypted and decrypted transparently for authorized users

All versions of Windows since Windows 2000 support EFS


A user or administrator marks a directory to use EFS and from that point on any file created in that directory is encrypted

At a very high level, EFS works by generating a random file encryption key (FEK) and storing that key, encrypted using the user's encryption key

This key is protected using the Data Protection API (DPAPI) in Windows and the key is derived from the user's password

EFS also supports the concept of a file recovery agent if for some reason the users lose their EFS keys

Cryptographic Services – Data Protection API (DPAPI)




The DPAPI allows users to encrypt and decrypt data transparently --- the tasks of maintaining and protecting encryption keys is removed from the user and administered by the operating system

When DPAPI is used to encrypt user data, the encryption keys are derived in part from the user's password

Developers need only call one of two functions, *CryptProtectData* to encrypt and *CryptUnprotectData* to decrypt

These functions also add a message authentication code to the encrypted data to help detect tampering

Cryptographic Services – BitLocker



Windows adds a much needed defense to the operating system, BitLocker Drive Encryption
The core threat this technology helps mitigate is data disclosure on stolen laptops
BitLocker encrypts the entire volume with using AES and the encryption key is stored either on a USB drive or within a Trusted Platform Module (TPM) chip on the computer motherboard
When booting a system that requires the USB device, the device must be present so the keys can be read by the computer, after which BitLocker decrypts the hard drive (the downside is if the device is lost)
Perhaps the most important aspect of BitLocker is that BitLocker policy can be set as a policy for a single computer and that policy “pushed” to computers that use Active Directory

Windows adds a much needed defense to the operating system, BitLocker Drive Encryption


The core threat this technology helps mitigate is data disclosure on stolen laptops

BitLocker encrypts the entire volume with using AES and the encryption key is stored either on a USB drive or within a Trusted Platform Module (TPM) chip on the computer motherboard

When booting a system that requires the USB device, the device must be present so the keys can be read by the computer, after which BitLocker decrypts the hard drive (the downside is if the device is lost)

Perhaps the most important aspect of BitLocker is that BitLocker policy can be set as a policy for a single computer and that policy “pushed” to computers that use Active Directory

Cryptographic Services – Trusted Platform Module (TPM)



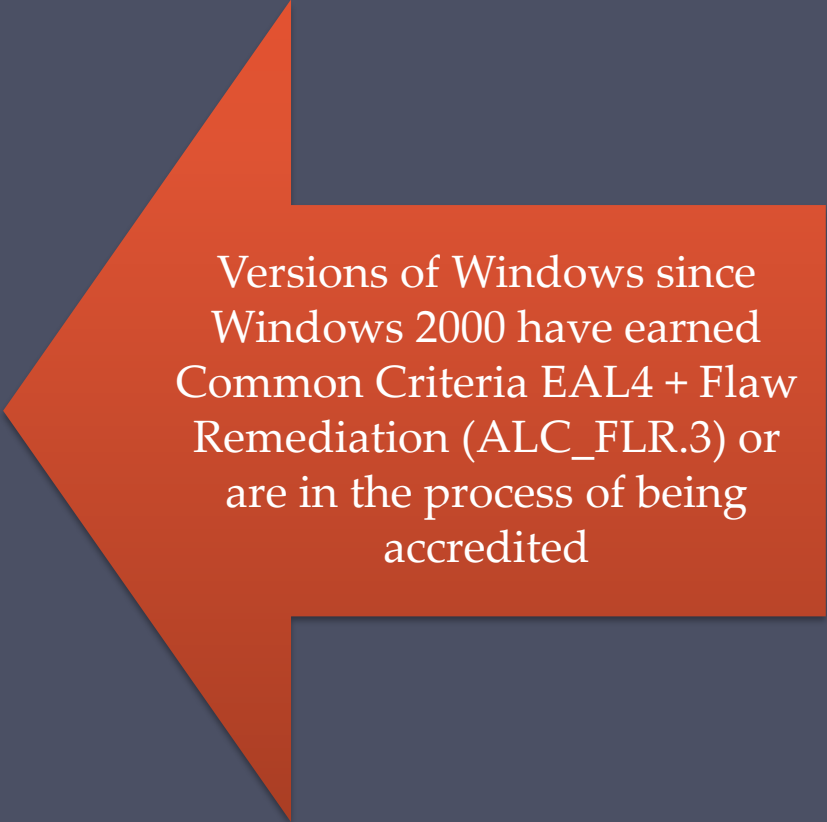
The TPM is the product of a specification from the Trusted Computing Group, designed to enhance system security by moving many sensitive cryptographic operations into hardware (many software-based attacks do not affect a hardware solution)

Windows Vista supports TPM version 1.2

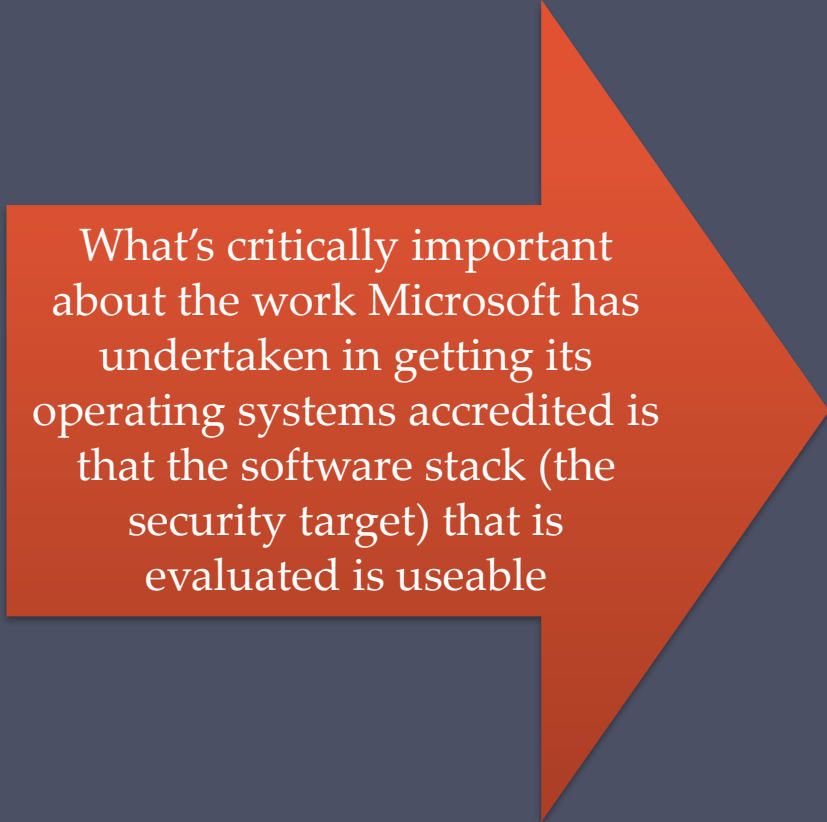
When a TPM is present and the system is configured appropriately, Windows will use the TPM to validate that the operating system has not been tampered with (this is known as trusted boot or secure startup)

Most laptops shipping today include a TPM on the motherboard

Common Criteria



Versions of Windows since Windows 2000 have earned Common Criteria EAL4 + Flaw Remediation (ALC_FLR.3) or are in the process of being accredited



What's critically important about the work Microsoft has undertaken in getting its operating systems accredited is that the software stack (the security target) that is evaluated is useable

Summary

- Fundamental Windows security architecture
- Windows vulnerabilities
- Windows security defenses



- Browser defences
- Cryptographic services
- Common criteria