

# Internet Security 2

## General Windows Security 2/2

Markus Kammerstetter

Christian Platzer

[inetsec@iseclab.org](mailto:inetsec@iseclab.org)

Gilbert Wondracek

Edgar Weippl

# News

*Int. Secure Systems Lab  
Technical University Vienna*

---

- Challenge 1

- 55 ppl solved it so far.
- Extended until Saturday

- Challenge 2 starts today

- Remote Exploit
- Memory corruption knowledge will come in handy

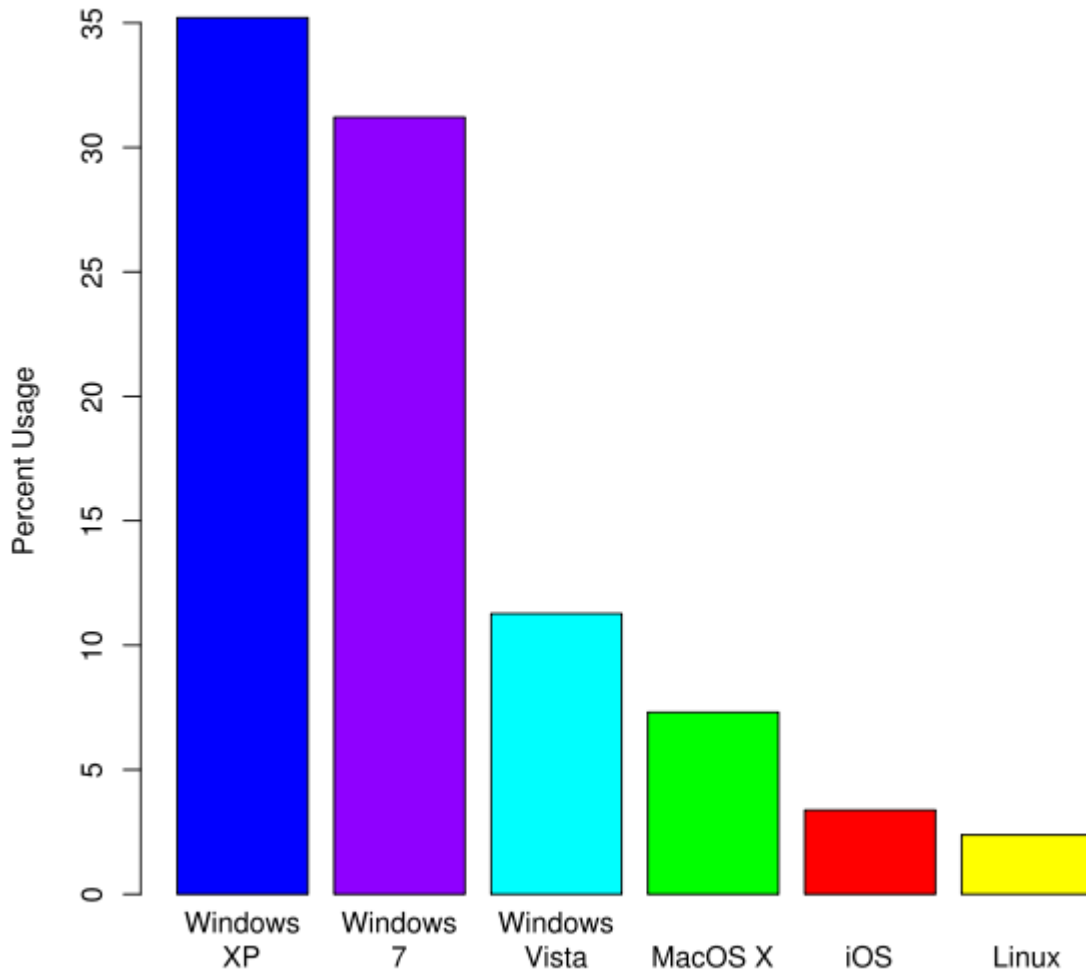
# Windows OS details

# Single User OS (DOS/95/98/ME)

Int. Secure Systems Lab  
Technical University Vienna

- Almost no user security (just like DOS)
  - Anyone can install anything, *locking down* not possible
- Local Security
  - Highly vulnerable to viruses and trojan horses
  - Highly vulnerable to unauthorized local access/console
  - No file encryption (e.g., like in WinXP).
- Remote Security
  - Highly vulnerable to denial-of-service (weak TCP/IP stack)
    - ping of death, winnuke, land attack
  - If file/print sharing is used (port 445)
    - Registry can be accessed
  - Win 95/98 are not supported by Microsoft anymore!
    - There are “zillion” vulnerabilities meanwhile!
  - Usage down to <1% (luckily)

## Usage share of web client operating systems: August 2011



— *Int. Secure Systems Lab* —  
*Technical University Vienna*

(Source: Median values from **Usage share of operating systems** for August 2011. Including Clicky Webalytics, StatOwl, W3C Counter, StatCounter, etc.)

# Windows 95/98/ME

*Int. Secure Systems Lab  
Technical University Vienna*

- Registry
  - used to store system configuration (read/write for all)
- Login Process
  - no authentication – simply press cancel
  - determines only profile, no enforced restrictions
- Profile
  - desktop preferences
  - access to saved passwords (in .pwl files)
    - access shared resources, dial-up network
    - Resource Record – Triple <type, name, passwd>
    - passwd is encrypted with login name

# Windows 95/98/ME

*Int. Secure Systems Lab  
Technical University Vienna*

- Password files
  - login password is not stored encrypted, instead
  - pwl-file is decrypted with login password and a checksum verified (using user name as well)
  - Windows 95 – algorithm very easy to crack
  - Windows 98 – stronger algorithm (RC4)
    - world-readable
    - vulnerable to brute force / dictionary attacks
  - passwords are always converted to uppercase (makes brute force attacks much easier)
  - unreliable caching mechanism (important information maybe cached)

# Windows 95/98/ME Attacks

*Int. Secure Systems Lab  
Technical University Vienna*

- Screen-Saver protection
  - Ctrl-Alt-Del
  - CD-ROM autorun feature to execute programs
    - autorun.inf and entry “open=progname”
  - Password is stored in Registry (i.e. User.dat)
- Malicious Code / Remote exploits
  - Multiple Internet Explorer vulnerabilities (latest Version is IE 6)
  - Zillion spyware programs, publicly available exploits
  - Good idea not to use Win 95/98/ME – but this is not always possible

# Multi User (XP, NT, 2000, 2003)

*Int. Secure Systems Lab  
Technical University Vienna*

- Notion of multiple users
- Authentication
- Access Control
- Privilege Management
- Accounting, Quotas
- Windows NT, XP, 2003
  - object-oriented
  - Systems are based on similar technologies and code-base (i.e., vulnerabilities are usually across multiple platforms)
    - Easy to exploit multiple platforms with one weakness
    - Usually patched by MS on all platforms simultaneously
  - Security Monitor, tightly coupled host and network security

# NT Passwords

*Int. Secure Systems Lab  
Technical University Vienna*

- NT Maintains backward compatibility to Win95/98, NT passwords can be easy to crack
  - A LANMAN password hash is upper cased, padded to 14 characters, divided into two seven character parts, each of which is used as a key to encrypt a constant.
  - After LANMAN passwd hash is cracked, 2 to the nth power (where n is the length of the password) gives the maximum number of case variations that must be tried to get the NT password (about a second ).
  - LANMAN authentication could only be partially disabled. The passwd storage scheme and encryption was still weak against brute force attacks.
- In 2001, a method was provided to disable LANMAN hashes on 2000 and XP, but not NT
- LANMAN 2 was introduced (NTLM v2) with Service Pack 4
  - Stronger encryption
  - Also works on Windows 95/98/ME with Active Directory enabled

# NT and 98 Threat Mitigation Guide

*Int. Secure Systems Lab  
Technical University Vienna*

- Syn flooding protection registry hacks
  - Syn flooding is a common attack. Each connection request requires server to allocate certain amount of memory and kernel structures
  - HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect(RegDword) = 1
  - HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen(RegDword) = 100 (maximum number of connections)
  - Drop in the bucket, only 98 and ME
- Tips and tricks to configure your system (e.g., ICMP redirects, router discovery, RPC stuff)

# NT and 98 Threat Mitigation Guide

*Int. Secure Systems Lab  
Technical University Vienna*

- NSA has developed a set of recommended permissions for NT servers and workstations
  - “Guide to securing MS Windows NT networks”
- Restrict null-session and anonymous accesses (i.e., to the registry)
- Prevention of the storage of LANMAN passwords
- Patching is recommended by MS, but sometimes this is not possible (i.e., on illegal copies... is this a good idea?)
  
- Or directly from Microsoft:

## **The Microsoft Windows NT 4.0 and Windows 98 Threat Mitigation Guide**

# Intermezzo

*Int. Secure Systems Lab  
Technical University Vienna*

- This was Part 1: The “ugly” past of MS Windows OS’.
- Main Problems
  - Legacy support, emerged from DOS
  - Huge customer base
  - Most widely used OS → Target
- Part 2: The not-so-ugly continuance
  - XP, Vista, 7
  - General Guides.

# Windows XP Security Check List

*Int. Secure Systems Lab  
Technical University Vienna*

- Provide physical security for the machine ;-)
  - Obvious, but often forgotten.
- Use NTFS on all your partitions (Linux:, writeable since Ubuntu 7.04)
  - It is faster than FAT32, supports permissions down to the file level, encryption and compression
  - You can watch HD movies that way (supports > 4GB files)
- Disable **Simple File Sharing**.
  - If you are connected to Internet, no firewall, your shares may be readable by practically anyone
  - *Start > My Computer > Folder Options > View > Advanced settings > Simple File Sharing*
  - Does not work on XP Home
  - Make sure your shares are read only and hide them (i.e., using \$ at the end)

# Windows XP Security Check List

*Int. Secure Systems Lab  
Technical University Vienna*

- Use passwords on all accounts
  - Both XP Professional and Home allow user accounts to utilize blank passwords (no more remote logins allowed)
- XP Home Edition **all** user accounts have administrative privileges and no password **by default**.
- Use the Administrator Group with care
- Disable the guest account
  - The guest account has been a huge hacker hole
  - Unfortunately, much easier on Professional than Home. If you disable guest, it is not really “removed”. The only solution is to choose a strong password

# Windows XP Security Check List

*Int. Secure Systems Lab  
Technical University Vienna*

- Be careful with Internet Connection Sharing (ICS)
  - Anyone maybe able to connect and surf over your network. Especially interesting for wireless connections.
- Use the Security Configuration Manager
  - SCM tools allow admins to define security templates. These can contain passwd, lockout, audit policies and event log settings, registry values, service startup modes, user rights, permissions, etc.
  - Not available on XP Home edition
- Password security
  - Force policies: GPEDIT.MSC > *Computer Configuration > Windows Settings > Security Settings > Local Policy > Security Options*

# Windows XP Service Pack 2

*Int. Secure Systems Lab  
Technical University Vienna*

- A set of security “technologies” for improvement of situation
  - Network protection
    - Improved firewall, reduced RPC attack surface (reduced credentials)
  - Memory protection
    - MS version of StackGuard has been deployed (/GS switch, canary)
  - E-mail handling
    - Outlook has been “fixed”, recompiled
  - Web browsing security
    - Privileges / locking down
  - Automatic updates (there were reports of problems at first)

# Windows XP Service Pack 2

*Int. Secure Systems Lab  
Technical University Vienna*

- Hardware enforced NX Page flag
  - Allows to flag a (virtual) page in memory as **not executable**
    - 1 Bit in Page table entry (PTE)
    - Standard-heap protection, Stack protection
  - Only available for “newer” CPU’s
    - Intel: XD (Execute disabled)
    - AMD: NX (No Execute)
- Software enforced (DEP)
  - Also available when CPU does not support NX
  - Not as powerful as NX
- For system binaries enabled by default
  - Possible opt-in by modified PE header
  - Possible system-wide opt-out setting (boot.ini)

# Windows XP Service Pack 2

Int. Secure Systems Lab  
Technical University Vienna

- Possible problems when using DEP for all executables
  - Old software may crash
  - Self-modifying code
  - JIT compilers (like Spidermonkey) cease to function
  - It's not a solution for all problems
- Enjoy XP SP2 firewall with care: Only *inbound* connections are checked
  - It is possible for code to modify setting and firewall.

# Windows Vista Security

*Int. Secure Systems Lab  
Technical University Vienna*

- The “wow!” effect ;-)
  - Polished UI
  - very shiny
  - Hidden advanced functionality
- Now, most applications run in non-admin mode
  - User account control: If privilege is required, Secure Desktop mode is activated
- Bitlocker Drive encryption, Encryption FS
  - Full volume encryption, key can be stored on USB
- Totally flopped

# Windows Vista Security

*Int. Secure Systems Lab  
Technical University Vienna*

- Windows Firewall
  - Has been improved (e.g., outbound connections, port ranges, IP ranges, etc.)
- Windows Defender
  - Microsoft's anti-spyware utility is included
- Windows Parental Controls
  - Web content blocking, time limitations on account, restrictions on programs executed, etc.
- Exploit prevention
  - Address Space Layout Randomization (ASLR)
  - Encryption of function pointers
  - Stack overflow detection (canary mechanism)

# Windows Vista Security

*Int. Secure Systems Lab  
Technical University Vienna*

- Data Execution Prevention (DEP)
  - Vista fully supports NX features of processor
    - Beginning with Athlon64 / Pentium 4 (~2003)
- Application isolation
  - Mandatory Integrity Control
  - Application in a lower integrity level cannot access resources in higher integrity level
- Network Access Protection (NAP)
  - Computers should conform to preset “system health” level, otherwise, network access limited or denied (e.g., updates need to be installed)

# Windows Vista Security

*Int. Secure Systems Lab  
Technical University Vienna*

- Process Isolation
  - Previous versions of Windows, all services ran under same session
  - Not so anymore: Isolation Session 0
  - Normal process can not show popups or dialogs anymore
  - If it does, it will be invisible and will sit in the background
  - To interact, processes need to use Windows calls (so there is stricter control)

# Windows Vista Security

*Int. Secure Systems Lab  
Technical University Vienna*

- File and registry virtualization
  - Windows programmers generally assumed that they are admin
  - Thousands of programs exist out there so backwards compatibility is important
  - However, all-access registry operations have been disabled
  - Microsoft has introduced a file and registry virtualization for backwards-compatibility
  - Application writes to a “per user/ per app” location, does not realize it, it is transparent

# Windows 7 Security

*Int. Secure Systems Lab  
Technical University Vienna*

- User Account Control
  - Mimics Linux' and MAC OSX' sudo
  - Introduced in Windows Vista
  - Displays a warning dialogue, when a critical action is performed
    - Write to c:\
    - Open System Console
    - Install Driver/Software
  - Turned off by most users, because they were annoyed
    - Resulted in 3 dialogs to access certain settings
  - Restructured in Windows 7 with four different thresholds
    - Can also be done in Vista, but only through gpedit.msc
  - Patched in Vista SP1

# Windows 7 Security

*Int. Secure Systems Lab  
Technical University Vienna*

- Direct Access
  - Transparent VPN connection
  - Direct Access Server required
  - Enforces Network Access Protection (NAP)
    - System Admin defines a access policy
    - Client must be policy-conform to use the VPN
  - External Traffic (e.g. normal Browsing) not tunneled
    - Can also be altered by admin
  - Client  $\leftrightarrow$  Server already is IPv6/IPSec
    - Must be tunneled via 6to4, ISATAP etc..
    - But one day.....

# Windows 7 Security

*Int. Secure Systems Lab  
Technical University Vienna*

- BitLocker (Vista + 7)
  - Drive Encryption
  - 128Bit or 256Bit Advanced Encryption Standard (AES)
  - Supports TPM (trusted platform module)
  - Also available for Vista (Ultimate/Enterprise)
- BitLocker 2 go (7 only)
  - Same technique but also for FAT, extFAT and FAT32
  - Designed for removable drives (can be READ under Vista/XP)
- EFS (Encrypted File System)
  - File System encryption
  - For bad Passwords → brute forcing is possible

# Windows 7 Security

Int. Secure Systems Lab  
Technical University Vienna

- Buffer overflow protection (Ring 0):
  - **Safe unlinking**
  - Checks for pointer integrity, if an entry should be removed
  - Pool (kernel mode heap) consists of single-linked or double-linked lists (depending on the allocated size)
  - *Safe unlinking* adds a simple link-check before actually unlinking blocks.
  - No perfect solution, pool overruns still possible, but hardened.

# .NET Framework Security

*Int. Secure Systems Lab  
Technical University Vienna*

- Managed execution and type safety
  - Exception manager
  - Buffer overflows not possible
  - Security Engine
    - Code Access Security
  - But wait... there is “unmanaged” mode...
- CLR Integrated Security
  - Code access security
  - Role-based security
- .NET Framework Libraries
  - Cryptography
  - Web Services and Applications

# .NET Framework Security

*Int. Secure Systems Lab  
Technical University Vienna*

- Remote code:
  - With the growth of the Internet, applications are increasingly downloaded from remote sources
  - Users are susceptible to executing malicious code
- The proposed solution by Microsoft:
  - Introduced the .NET framework, where machine-independent byte-code is executed on a virtual machine
  - .NET is an implementation of the Common Language Infrastructure (CLI)
  - Consists of Common Type System (CTS)
  - .NET is type-safe and memory-safe

# .NET Framework Security

Int. Secure Systems Lab  
Technical University Vienna

- An important feature of .NET
  - It allows access to native libraries (i.e., legacy code support)
  - .NET applications are called *managed* and native code is referred to as *unmanaged* code
  - The runtime environment can enforce security restrictions by relying on type and memory-safety
    - Security model is called Code Access Security (CAS)
    - CAS uses *evidence* provided by the program and security policies to generate permissions (e.g., file access)
- Unfortunately, the execution of unmanaged native code is not restricted by the security model
  - Hence, an attacker can completely circumvent the .NET security mechanisms

# Invoking Unmanaged Code in .NET

Int. Secure Systems Lab  
Technical University Vienna

- To support interoperability with languages such as C, C++
  - CLI uses a mechanism called *Platform Invoke Service* (P/Invoke)
  - Because native code can modify the security state of user's environment, .NET permissions are *full trust*
  - The native code is run within the same process as CLI, an attacker could modify .NET runtime itself
  - Microsoft suggests P/Invoke to be used for highly-trusted code
    - This, however, cannot always be feasible

# Lockdown rules – The most important

---

*Int. Secure Systems Lab  
Technical University Vienna*

## User Education

# The Sinful 7

(source: Sophos)

---

*Int. Secure Systems Lab  
Technical University Vienna*

1. Downloading music and movies and appz
2. Opening email attachments or clicking on links in unsolicited emails (spam)
3. Surfing pornographic or other dubious websites
  - Although our research suggests otherwise
4. Running "joke" programs sent by friends and colleagues
5. Installing unauthorized software and web browser plug-ins
  - Danger of getting a BHO-like program
6. Giving information to unknown parties via phone or email
7. Using the same password on different websites

# Conclusion

---

*Int. Secure Systems Lab  
Technical University Vienna*

- The last two lectures investigated Windows security
- Next week, we'll look at Race Conditions
  - Lecture held by Edgar Weippl