Système Windows ***Démo***

Classification

- *Operating Systems (OS)*

Classification (critères) :

- *System monotask – multitasks (thread, process)*
- *System for one user – multiusers*
- *File system*
- *Desktop – server (file, mail, web, …)*
- *I/O (stockage, networking, …)*

Principles of Design for OS Security

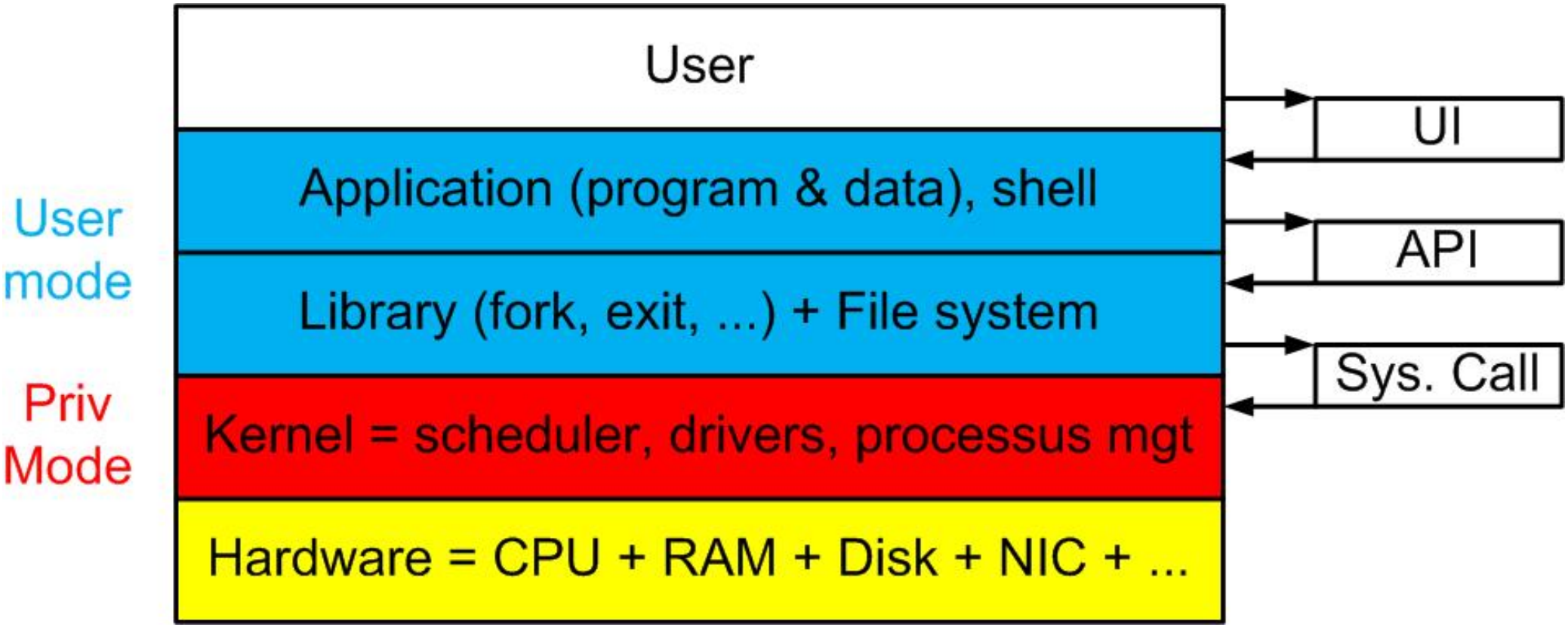
Saltzer & Schroeder 1975

- Economy of mechanism
  Keep the design as simple & small as possible
  → http://en.wikipedia.org/wiki/Source_lines_of_code
- Fail-safe defaults
  Base access decisions on permission rather than exclusion (white/black list)
- Complete mediation
  Every access to object must be checked for authorization
- Open Design (vs security by obscurity)
  Review by experts → Open Source
- Separation of privileges
  Protection mechanisms with 2 keys are better than simpler mechanism with 1 key
- Least privileges
  No more privileges than necessary
- Least common mechanism
  Minimize the amount of mechanism common to more that one user
- Psychological acceptability
  The security facilities must be understandable & **the users apply it**

Modèle en couches de Linux

Un système d'exploitation comme Linux :

- interagit avec le matériel
- fournit un environnement d'exécution aux applications



Modèle en couches de Linux

1. Matériel composé de processeur(s) *(Central Processing Unit)*, de mémoire RAM *(Random Access Memory)*, d'unité(s) de stockage *(disk)*, d'interface réseau *(Network Interface Card)*, d'un clavier, …

2. Noyau Linux (monolithique) qui gère les divers processus dans le temps *(time sharing)*, accède au matériel via des pilotes de périphériques

3. Bibliothèques d'appels système (créer – terminer un processus) et système de fichiers

4. Programmes utilisateurs & serveurs

5. Système (multiutilisateurs) où plusieurs utilisateurs peuvent cohabiter

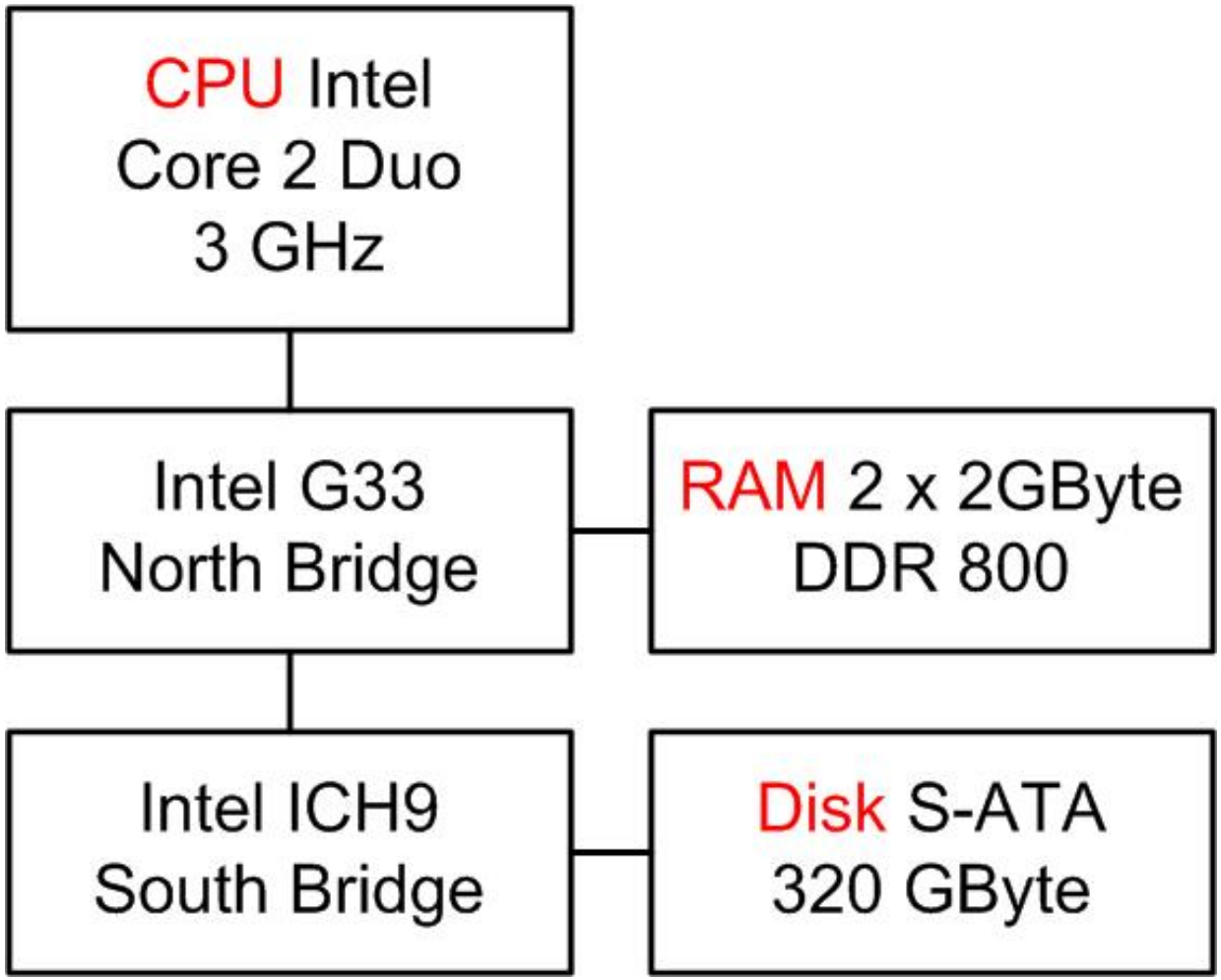
CPU

- Illustration avec processeur Intel x86

- Exécution de code machine (jeu d'instructions assembleur)
  http://siyobik.info/index.php?module=x86

- 4 niveaux de privilèges (Ring 0-3) dont 2 sont utilisés (démo)
  Certaines instructions ne s'exécutent qu'en mode privilégié
  Noyau (et les pilotes) s'exécutent avec le privilège maximum
  Crash du système en cas d'erreur de programmation *(bug)*
  Processeur est essentiellement en mode utilisateur pour exécuter les programmes
  → Le CPU, en mode utilisateur, qui exécute une instruction privilégiée va effectuer une exception (saut à une adresse fixe)

Motherboard



Performances **élevées** avec registres à l'intérieur du CPU

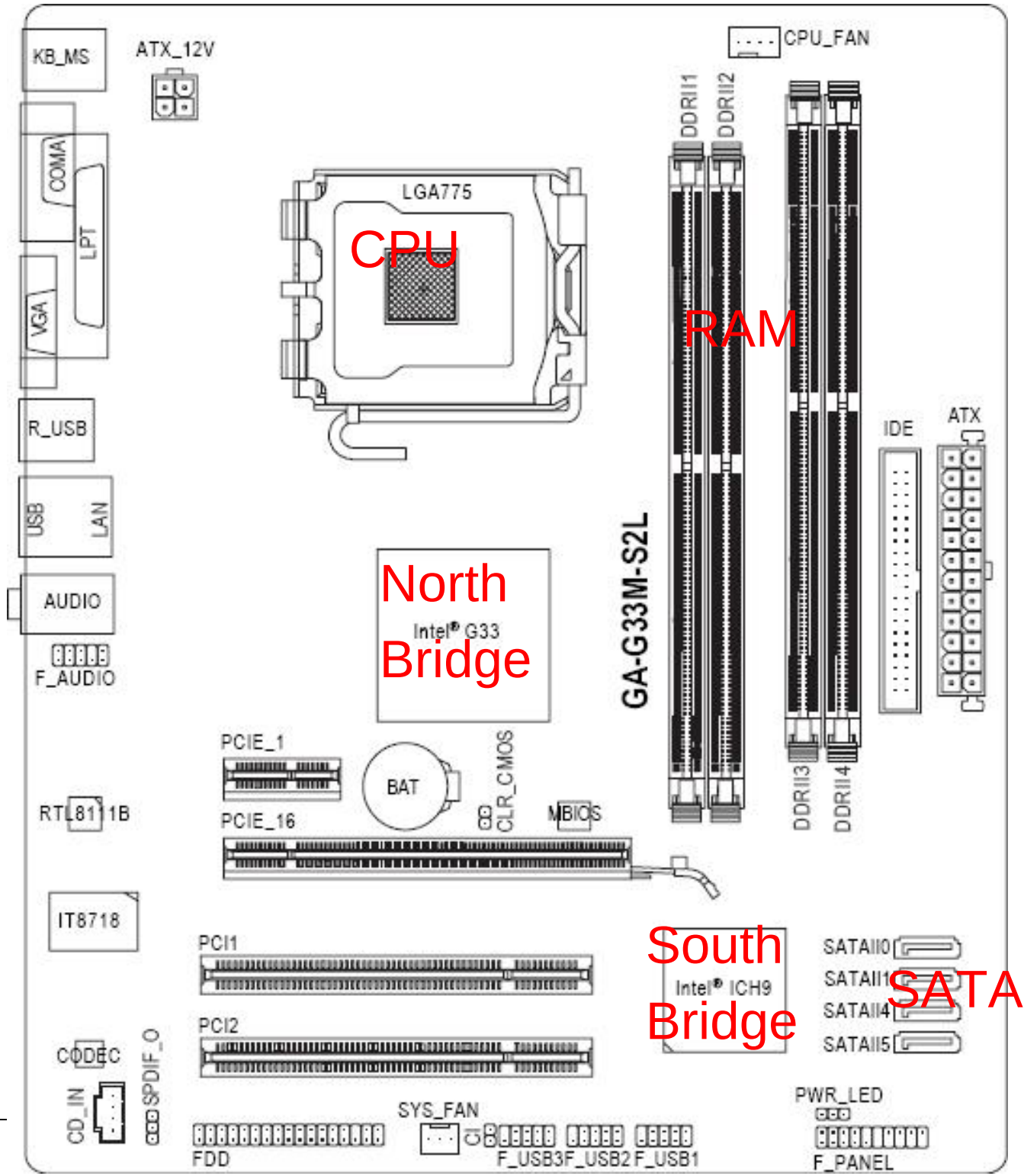
Performances **moyennes** avec mémoire RAM

Performances **faibles** avec disque

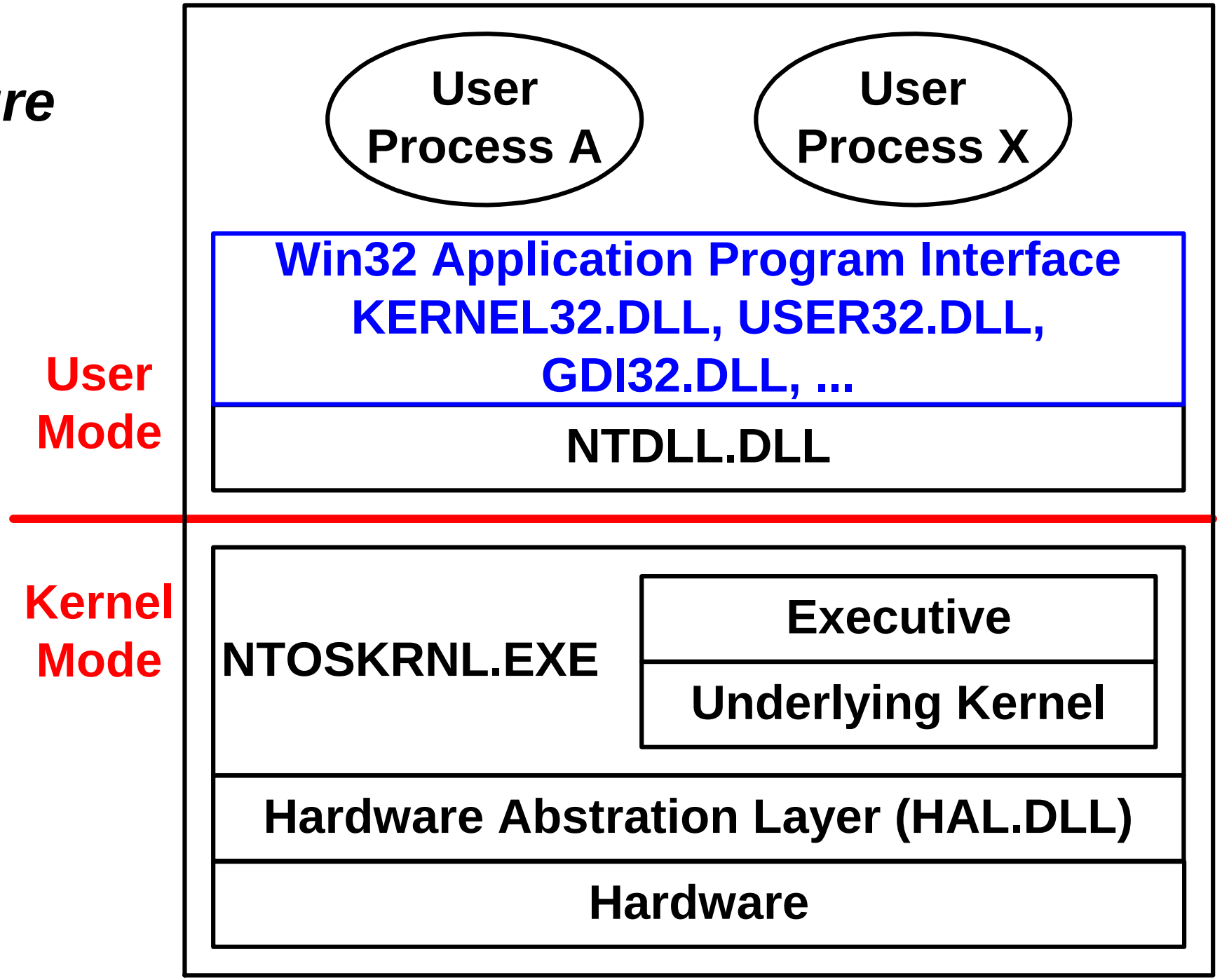
Motherboard

- Illustration de la carte utilisée au labo

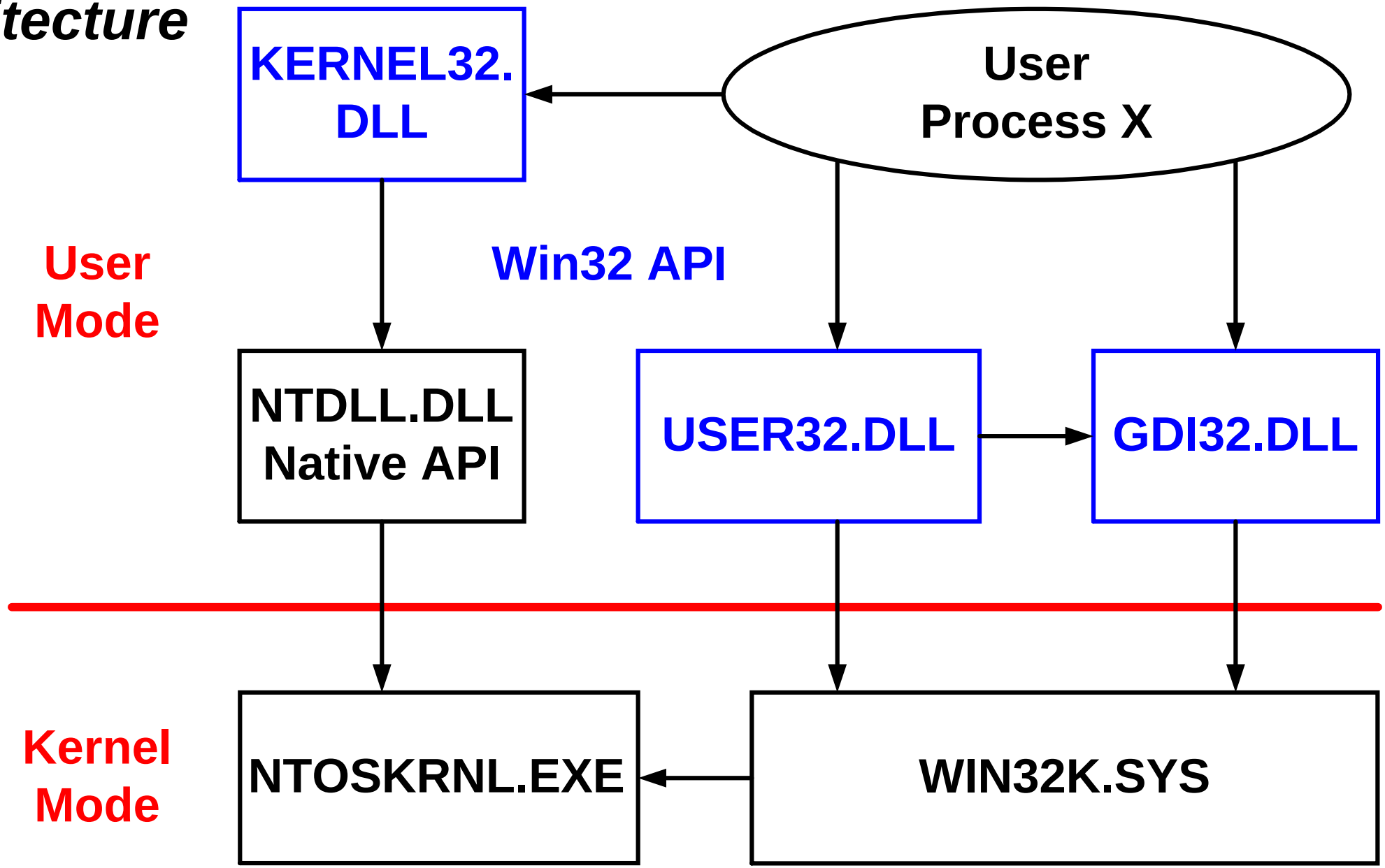
http://www.tdeig.ch/vmware/Montage_PC_Gigabyte.pdf



Windows Architecture



Windows Architecture



Principales DLLs

- KERNEL32.DLL

  Services non GUI *(Graphic User Interface)* tels que *file I/O*, *management (memory*, *object*, *process*, *thread*, …*)*

  Utilise *Native API*

- GDI32.DLL *(Graphic Device Interface)*

  Services graphiques tels que ligne, *bitmap*, …

- USER32.DLL

  Services graphiques (GUI) tels que *window* magagement, menu, boîte de dialogue, …

Process & Thread (Windows)

Un processus Windows comprend

- Un espace d'adressage privé virtuel de 4 Gbyte
- Un programme exécutable

  exemple : image C:\WINDOWS\explorer.exe
- Une liste de *handles* (pointeurs) pour les objets utilisés
- Un contexte de sécurité (slide 23)
- Un *ProcessID* (PID)
- Au moins un *thread*

  Le temps CPU(s) est alloué aux différents *threads*

→ Outils Task Manager, **Process Explorer**, Security Explorer, …, *Command Line Interface*

Task Manager

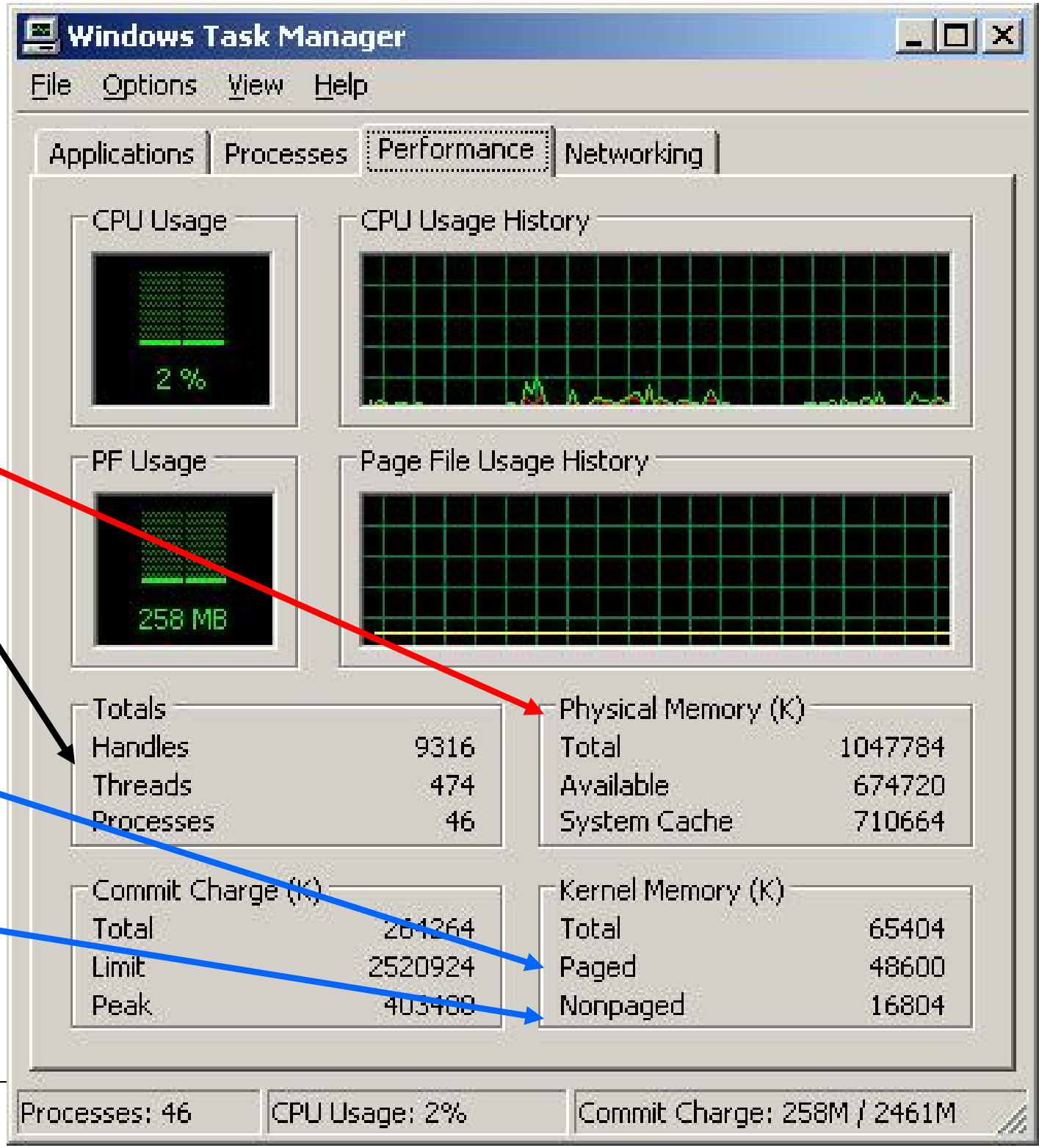
<Ctrl Maj Esc>

Physical Memory

Handles - Threads

Paged Swappable

Nonpaged resident in RAM



Process → Process Explorer (www.sysinternals.com)

Process	PID	CPU	Description	Session	Integrity Level	User Name
System Idle Process	0	96.97			n/a	NT AUTHORITY\SYSTEM
Interrupts	n/a		Hardware Interrupts	0		
DPCs	n/a		Deferred Procedure Calls	0		
System	4			0	System	NT AUTHORITY\SYSTEM
smss.exe	376		Windows Session Manager	0	System	NT AUTHORITY\SYSTEM
csrss.exe	456		Client Server Runtime Process	0	System	NT AUTHORITY\SYSTEM
wininit.exe	508		Windows Start-Up Application	0	System	NT AUTHORITY\SYSTEM
services.exe	592	1.52	Services and Controller app	0	System	NT AUTHORITY\SYSTEM
lsass.exe	612		Local Security Authority Process	0	System	NT AUTHORITY\SYSTEM
lsm.exe	620		Local Session Manager Service	0	System	NT AUTHORITY\SYSTEM
csrss.exe	516		Client Server Runtime Process	1	System	NT AUTHORITY\SYSTEM
winlogon.exe	564		Windows Logon Application	1	System	NT AUTHORITY\SYSTEM
explorer.exe	1932		Windows Explorer	1	Medium	DELL6000\albert
conime.exe	4060		Console IME	1	Medium	DELL6000\albert
csrss.exe	2164		Client Server Runtime Process	2	System	NT AUTHORITY\SYSTEM
winlogon.exe	2760		Windows Logon Application	2	System	NT AUTHORITY\SYSTEM
explorer.exe	2244		Windows Explorer	2	Medium	DELL6000\ursula

- **Code de couleur**

  `Options - Configure Highlighting`

Boot Process

- Idle — 1 thread / CPU for idle CPU time
- System — kernel-mode threads & drivers

user-mode

- smss — Session Manager → Session 0,1,2,… — account
- csrss — Client-Server Runtime (Win32 API) — SYSTEM
- wininit — lance les services,
  - lsass (Local Security Authority)

pour chaque session utilisateur

- csrss
- winlogon
- explorer

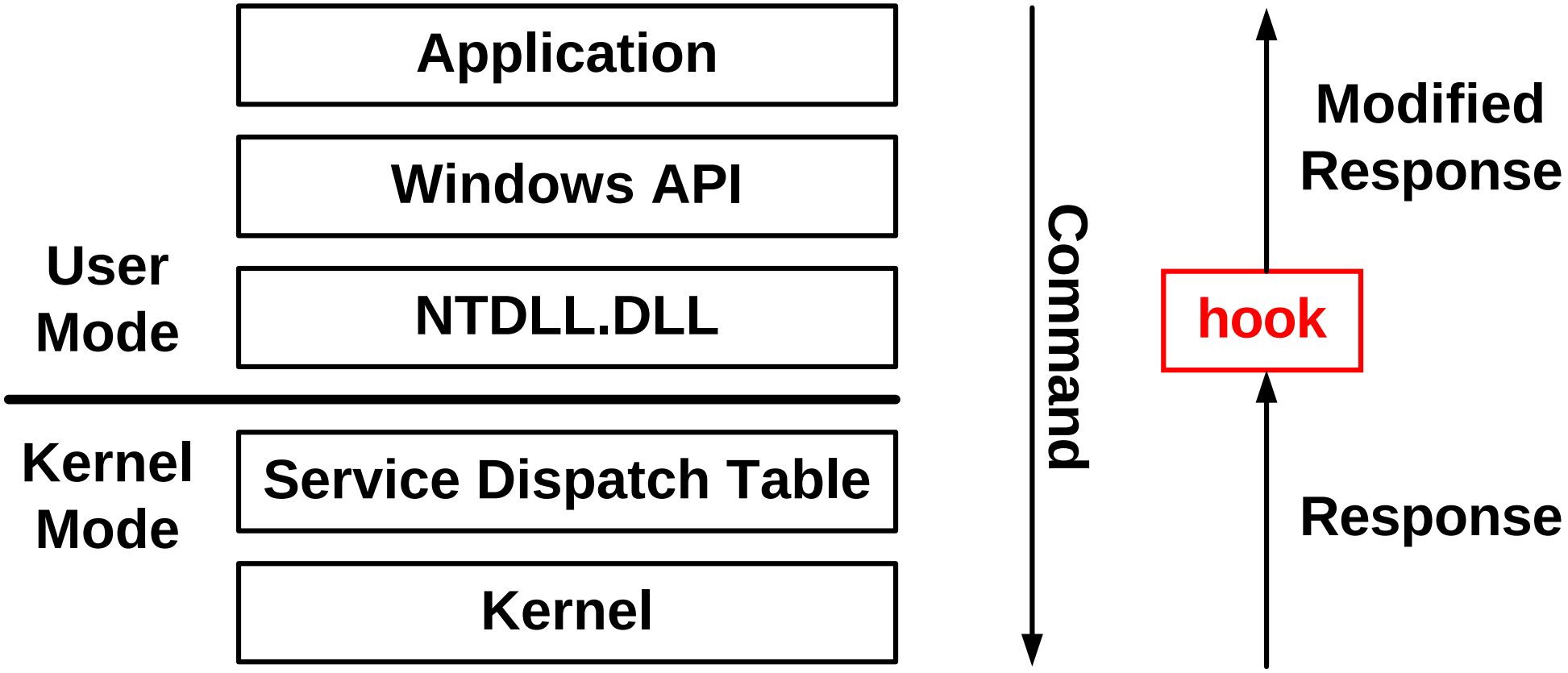
http://homepages.tesco.net/~J.deBoynePollard/FGA/windows-nt-6-boot-process.html

Principaux processus de Windows

- Idle — 1 thread / CPU for idle CPU time
- System — kernel-mode threads = ntoskernel.exe, srv.sys → slide 10
- smss — Session Manager (1er user-mode process) → slide 15
- csrss — Runtime Process = Win32 API → slide 10
- winlogon — Interactive user logon – logoff, Secure Attention Sequence (default = Ctrl+Alt+Delete) → slide 22
- services — Service Control Manager → slide 20
- lsass — Local Security Authentication Server → slide 15+22
  → Access Token = user's security profile
- explorer — User's session → slide 41-43

Rootkit

- L'analyse *live* ne peut plus être considérée comme fiable si le système est infecté par un *rootkit*



- Techniques utilisées → http://www.tdeig.ch/windows/wenger_M.pdf

Rootkit (suite)

- *Rootkits are Trojan horse backdoor tools that modify existing operating system software so that an attacker can keep access to and hide on a machine (Skoudis)*

- La victime *(user / admin)* utilise à son insu du code modifié par l'attaquant qui lui permet de cacher ses actions

- La victime exécute la commande (dir, show process, …)

  Le système d'exploitation répond

  Cette réponse est interceptée puis filtrée avant d'être affichée

  → DLL Injection, API Hooking, …

Isolation par session (cloisonnement)

- Session 0 réservée pour les processus système et les services
  Cette session n'est pas interactive (isolation)
- Session 1, 2, … réservées aux utilisateurs
- Chaque session protège l'utilisateur des autres contextes
  0 → système, 1 → Albert *(Admin)*, 2 → Ursula *(User)*
- Chaque exécutable lancé dans une session hérite des droits du processus appelant
- Au sein de la même session, pas de protection entre les applications → *DLL injection* (du code malveillant est copié en RAM dans un processus légitime) → http://www.tdeig.ch/windows/wenger_M.pdf
  Exemple de faille conceptuelle ! Démo Wenger

Services

Les services sont une cible potentielle d'attaques car :

- ils s'exécutent par défaut lors du *boot*
- ils restent actifs jusqu'à la mise hors service du poste
- certains ont accès au réseau
- ils possèdent souvent plus de droits qu'un simple utilisateur

- Chaque version de Windows ajoute des services supplémentaires (45 pour XP-SP2, 56 pour Vista Enterprise, 102 sur mon Win7, …)
  Win7 default services → http://social.technet.microsoft.com/wiki/contents/articles/4484.windows-7-default-services.aspx

- Outils GUI → Task Manager – Services *(new)*
  Admin Tools – Services
  Procexp *(Sysinternal)*
  

  CLI → sc query

Désactiver les services (méthodologie)

- Trouver le bon document

  VMware View Horizon Optimization Guide p17-22

- Identifier un risque potentiel (ou une fonction inutile)

  Pas besoin de la fonction Discover UPnP devices

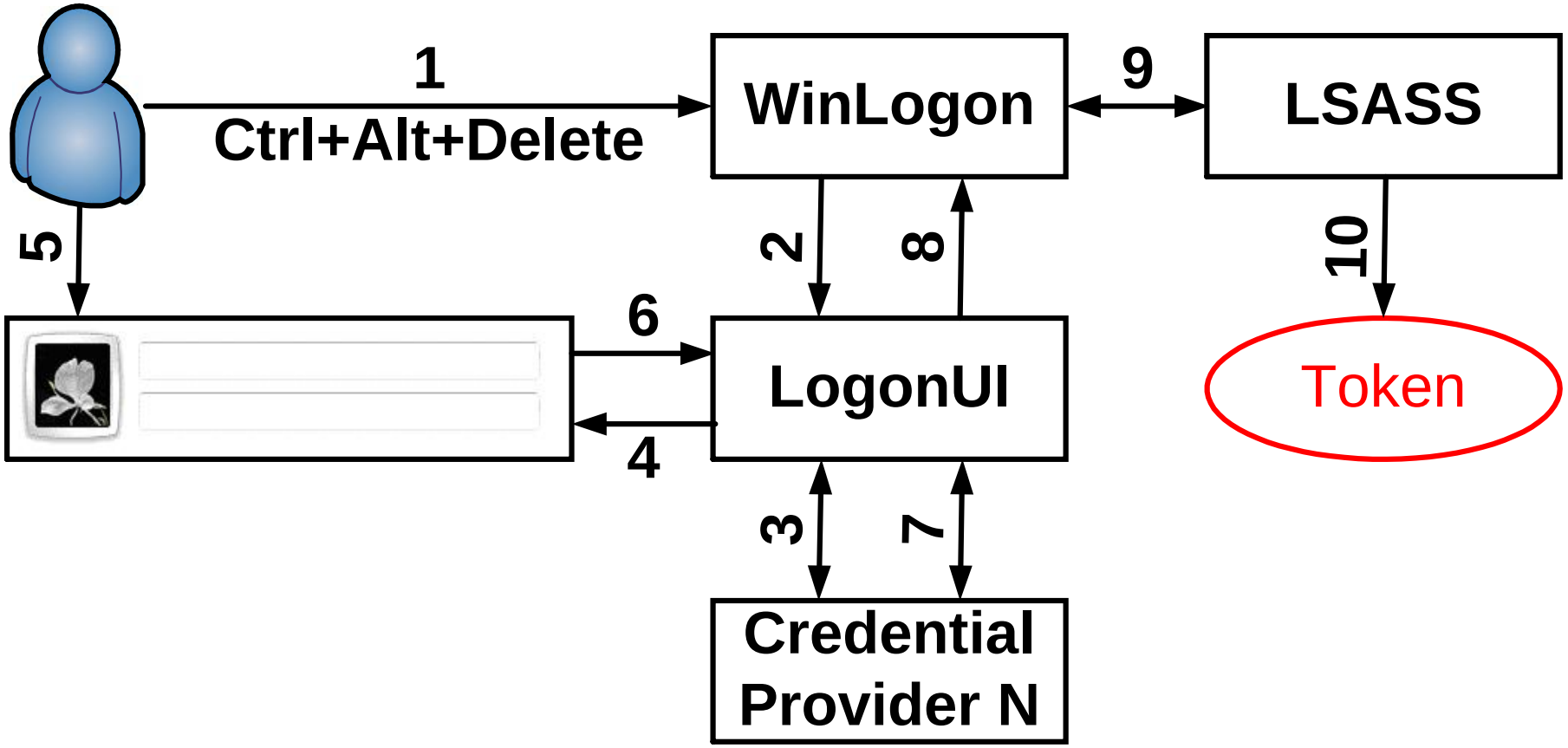
- Désactiver par script

```
Powershell Set-Service ‘ssdpsrv’ -startuptype “disabled”
```

- Tester – tester – tester !!!

- Répéter pour la centaine de services

Authentification



Eléments du jeton selon whoami

```
C:\>whoami /all
User Name      SID
dell6000\jean S-1-5-21-344556351-533155725-1776856995-1001

Group Name                                 Type                 SID
Everyone                                   Well-known group     S-1-1-0
BUILTIN\Users                              Alias                S-1-5-32-545
NT AUTHORITY\INTERACTIVE                   Well-known group     S-1-5-4
NT AUTHORITY\Authenticated Users           Well-known group     S-1-5-11

Privilege Name                Description                          State
SeShutdownPriv.               Shut down the system                 Disabled
SeChangeNotifyPriv            Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from                 Disabled
                              docking station
SeTimeZonePrivilege           Change the time zone                 Disabled
```

Token

- Un jeton *(Access Token)* est généré par Vista (processus lsass) lors d'une authentification réussie

- Il contient notamment les *Security ID* (SID) de l'utilisateur et des groupes *(Users, INTERACTIVE, …)* auxquels il appartient, la liste des privilèges (droits), le niveau d'intégrité, …

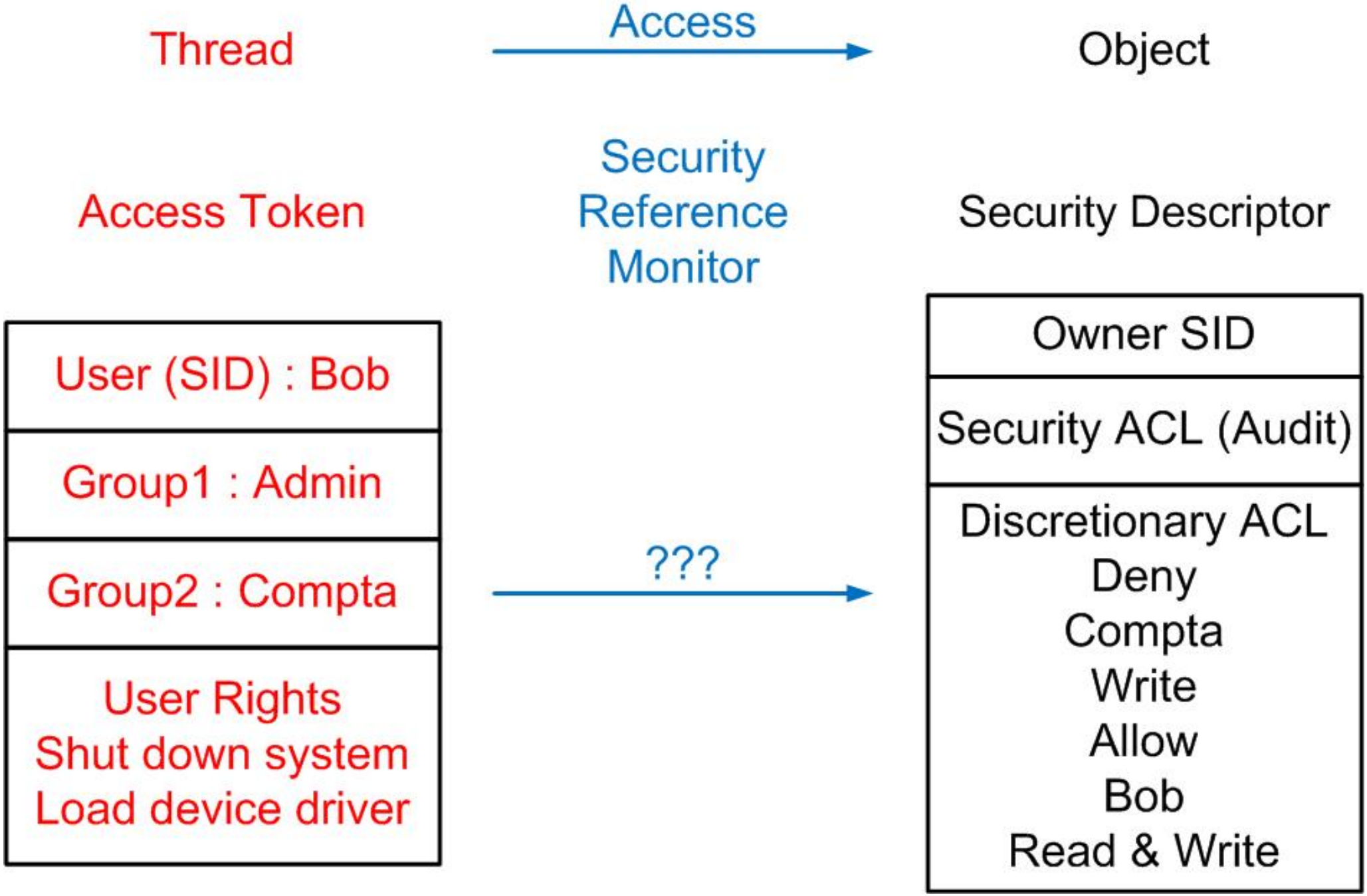
- Illustration avec les privilèges spécifiques

  Jeton complet possède 23 privilèges

  Jeton restreint possède 5 privilèges

  Le compte SYSTEM possède 30 privilèges

- Pour plus de détail, consulter l'excellent mémoire de Master http://www.tdeig.ch/windows/chiarello_M.pdf annexe B p77


Thread
Access
Object
Security
Reference
Monitor
Access Token
Security Descriptor
User (SID) : Bob
Group1 : Admin
Group2 : Compta
User Rights
Shut down system
Load device driver
???
Owner SID
Security ACL (Audit)
Discretionary ACL
Deny
Compta
Write
Allow
Bob
Read & Write

Groupes *système, applicatifs et internes*

- Lors de sa création, un compte possédera des droits spécifiques en fonction de son appartenance aux groupes système *Administrators* : albert, *Users* : ursula, *Backup*, *Debugger*,… Démo

- Il est possible d'ajouter des groupes applicatifs tels que Secrétaires, Comptables, pour faciliter la gestion des utilisateurs

- De plus, Windows gère dynamiquement des groupes internes (21) :

Authenticated Users	contient tous les utilisateurs authentifiés
Interactive	contient les utilisateurs qui accèdent physiquement à l'ordinateur (clavier - écran)
Network	contient les utilisateurs qui accèdent à distance
Everyone	sans intérêt

Security ID (SID)

- SID pour identifier machine, utilisateur, groupe

- SID unique lors de l'installation

S-1-5-21-344556351-533155725-1776856995	Ce PC
S-1-5-21-344556351-533155725-1776856995-500	admin
S-1-5-21-344556351-533155725-1776856995-501	guest
S-1-5-21-344556351-533155725-1776856995-1000	1er
S-1-5-21-344556351-533155725-1776856995-1001	2ème

- Si je supprime le compte jean puis j'en créé un nouveau
  le système supprime jean-1000 puis créé jean-1002

Security ID (SID) : S-1-5

- *Well known SIDs*

  4=*Interactive*, 11=*AuthenticatedUsers*, …

- Ce PC (machine → HKLM = slide 29)

  21-344556351-533155725-1776856995

  ← Numéro unique →

- Utilisateur → *Relative ID (RID)*

  21-344556351-533155725-1776856995-500 built-in admin

  21-344556351-533155725-1776856995-1000 1er créé

- Outil CLI : psgetsid *(Sysinternals)*, whoami

User Rights → granularité utilisateurs & groupes

Quelques droits (privilèges) → slide 23 — Groupe

- Shut down the system — Admin User
- Change the system time — Admin
- Change the time zone — Labo §4 — Admin User
- Force shutdown from a remote system — Admin
- Load and unload device drivers — Admin
- Allow log on locally (interactively) — Admin User
- Access this computer from the network — Admin User
- Take ownership of files or other objects — Admin

- Outil = Local Security Policy – Local Policies – User Rights Assignment (démo : onglet Explain) Démo = secpol.msc (slide 61)

Security Options → granularité machine Démo

Quelques options de sécurité :

- Accounts: Rename administrator account
- Audit: Shutdown system immediately if unable to log security audits
- Devices: Allowed to format and eject removable media
- Devices: Prevent users from installing printer drivers
- Devices: Restrict CD-ROM access to locally logged-on user only
- Devices: Unsigned driver installation behavior
- Interactive logon: Do not display last user name
- Interactive logon: Do not require CTRL+ALT+DEL
- Interactive logon: Message text for users attempting to log on
- Interactice logon: Smart card removal behavior
- Net security: Do not store LMhash value on next password change
- User Account Control → slide 36

Base de registre Démo

- Contient en RAM tous les éléments accessibles depuis *User Rights*, *Security Options*, …

- 2 clés racines sont importantes

  HKEY_LOCAL_MACHINE HKLM → paramètres globaux

  HKEY_USERS HKU → paramètres utilisateur

- Illustration avec outil regedit.exe

  La version Windows 2000 ne possédait pas l'élément *Do not store LM hash value on next password change* → slide 30

  Solution proposée selon http://support.microsoft.com/kb/299656 : ajouter NoLMHash

  dans HKLM\SYSTEM\CurrentControlSet\Control\Lsa démo

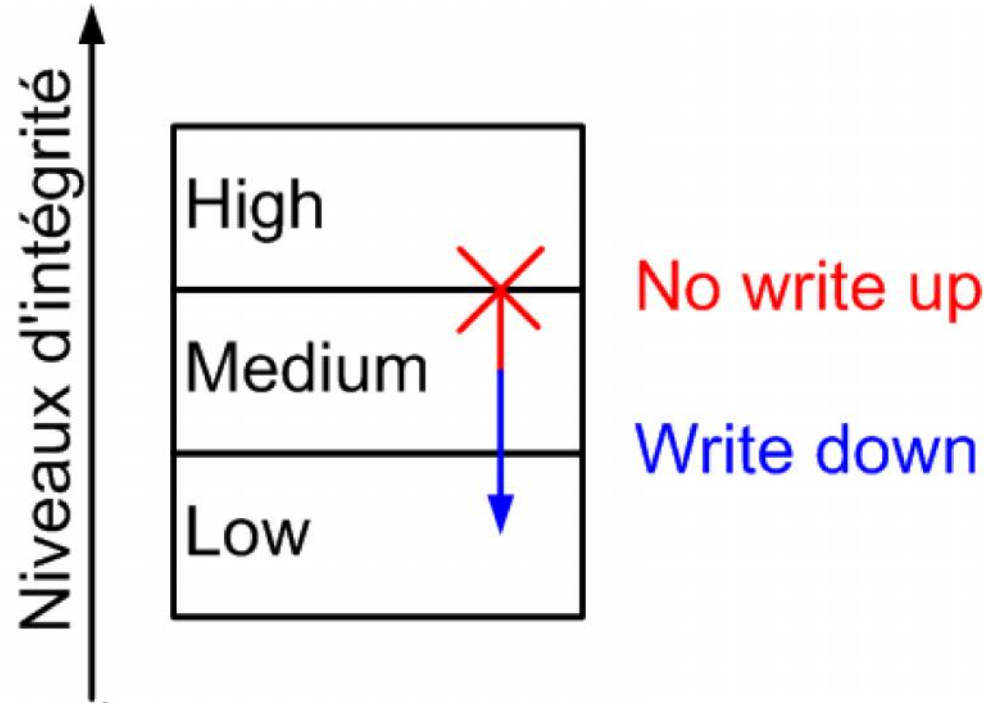
Risques sur la base de registre

- Outil regedit → *no undo function !* → *file export & import*
- L'administrateur possède le contrôle total *(full access)*
- L'utilisateur ne peut que lire
- Labo §6 : autoriser l'exécution que pour le groupe *Administrators*
- Outil Autoruns (www.sysinternals.com) affiche la liste des programmes lancés au démarrage Démo
- Outil ARM *(GUI – no install)*
  Comparaison de 2 sources (file.reg / *scan*)
  file.reg produit avec reg.exe, *scan* de la base de registre
  http://www.protect-me.com/arm/download.html

Mandatory Integrity Control (MIC)

- Inspiré du modèle Biba (1977) qui contient 3 axiomes = *No write up (intégrité)*, *No read-down (confidentialité)* et *No Execute Up*

- Un sujet ne peut pas modifier les niveaux d'intégrité supérieurs



MIC : mise en oeuvre

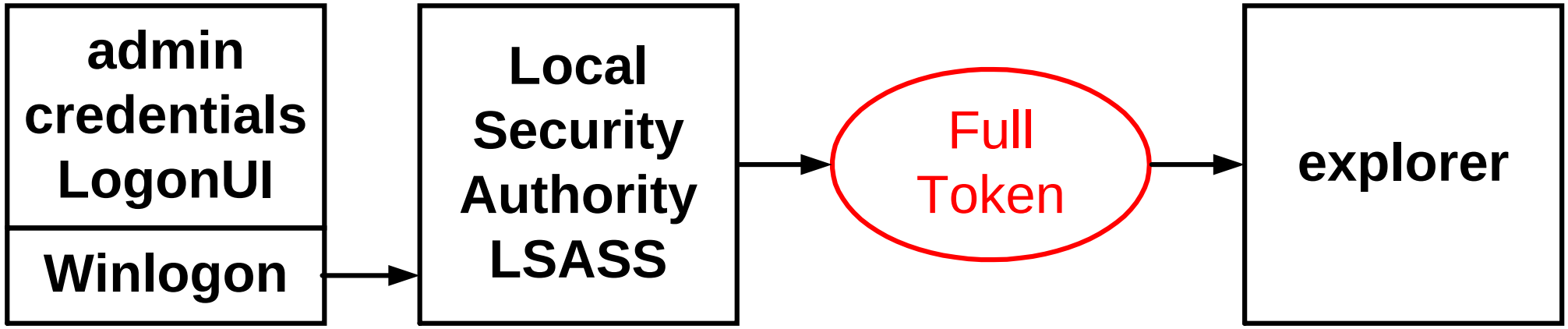
- 5 niveaux d'intégrité (de confiance) démo OSK

Account	*Integrity Level*	*Object*
System	System	Service
Admin	High	Registry
User	Medium	File
?	Low	objet IE
	Untrusted	Chrome

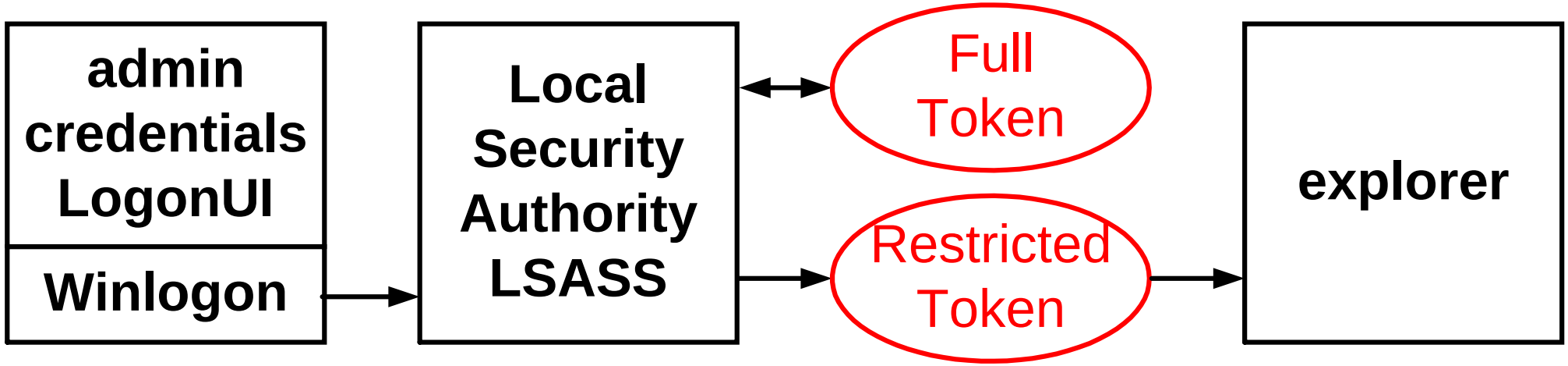
- Jeton *(token)* possède un niveau par héritage
- Objet possède un niveau dans Security ACL (slide 23)

Comparaison XP / Vista pour un administrateur

- **XP : explorer hérite des droits admin**



- **Vista : explorer hérite des droits utilisateur** **démo cmd**



UAC (User Account Control) : Fonctionnement

Lors de l'authentification :

- Membre du groupe *Users* reçoit 1 jeton restreint
- Membre du groupe Admin reçoit 1 jeton restreint + 1 jeton complet

→ Mode par défaut utilise le jeton restreint (moindre privilège)

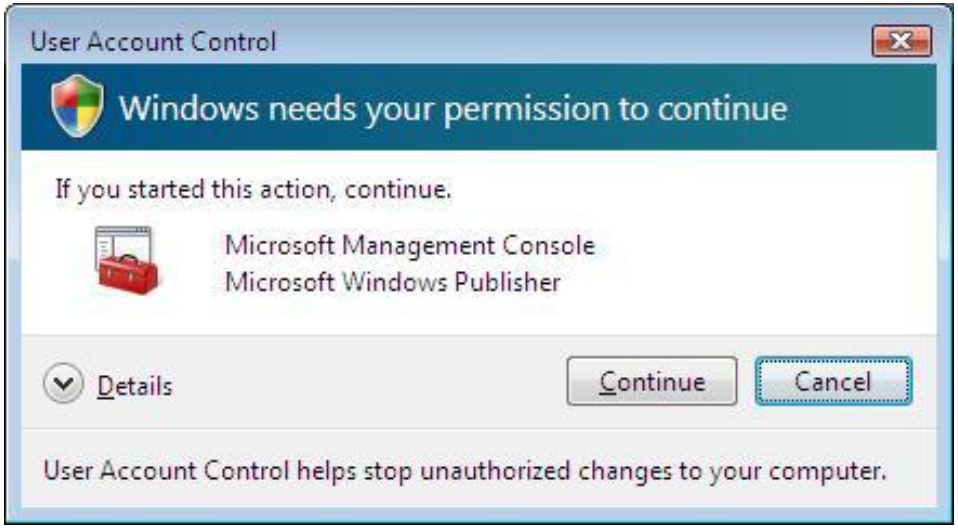
Application qui exige des droits admin

- doit l'indiquer dans son *manifest* → *requireAdministrator*
- est signalée par le bouclier

- Elévation de privilège (automatique, consentement, authentification)

UAC : affichages

Session admin avec demande de consentement pour exécuter mmc



Idem mais avec saisie du mot de passe *(credential)*

UAC : élévation de privilège des applic. GUI

Admin veut exécuter une applic. GUI qui exige les droits admin

- Demande de consentement *consent (default)*
- Authentification *credential*
- Automatique *auto*

Behavior of the elevation prompt for administrators in Admin Approval Mode

User veut exécuter une applic qui exige les droits admin

- Pas possible *no prompt (default enterprise)*
- Authentification *prompt (home edition)*

Behavior of the elevation prompt for standard users

L'élévation de privilège est protégée par un bureau spécifique appelé *Secure desktop*

UAC : code de couleur

- Programme ou fonction Vista *(Operating System)*

   *Windows needs your permission to continue*

- Application signée (Visual Studio, …)

   *A program needs your permission to continue*

- Application tierce non signée

   *An unidentified program wants access to your computer*

- Application bloquée *(publisher*, *Group Policy)*

   *This program has been blocked*

Par défaut

- Compte *Built-in Administrator* est désactivé
  possède des droits supérieurs aux membres du groupe admin

- Compte *Guest* est désactivé

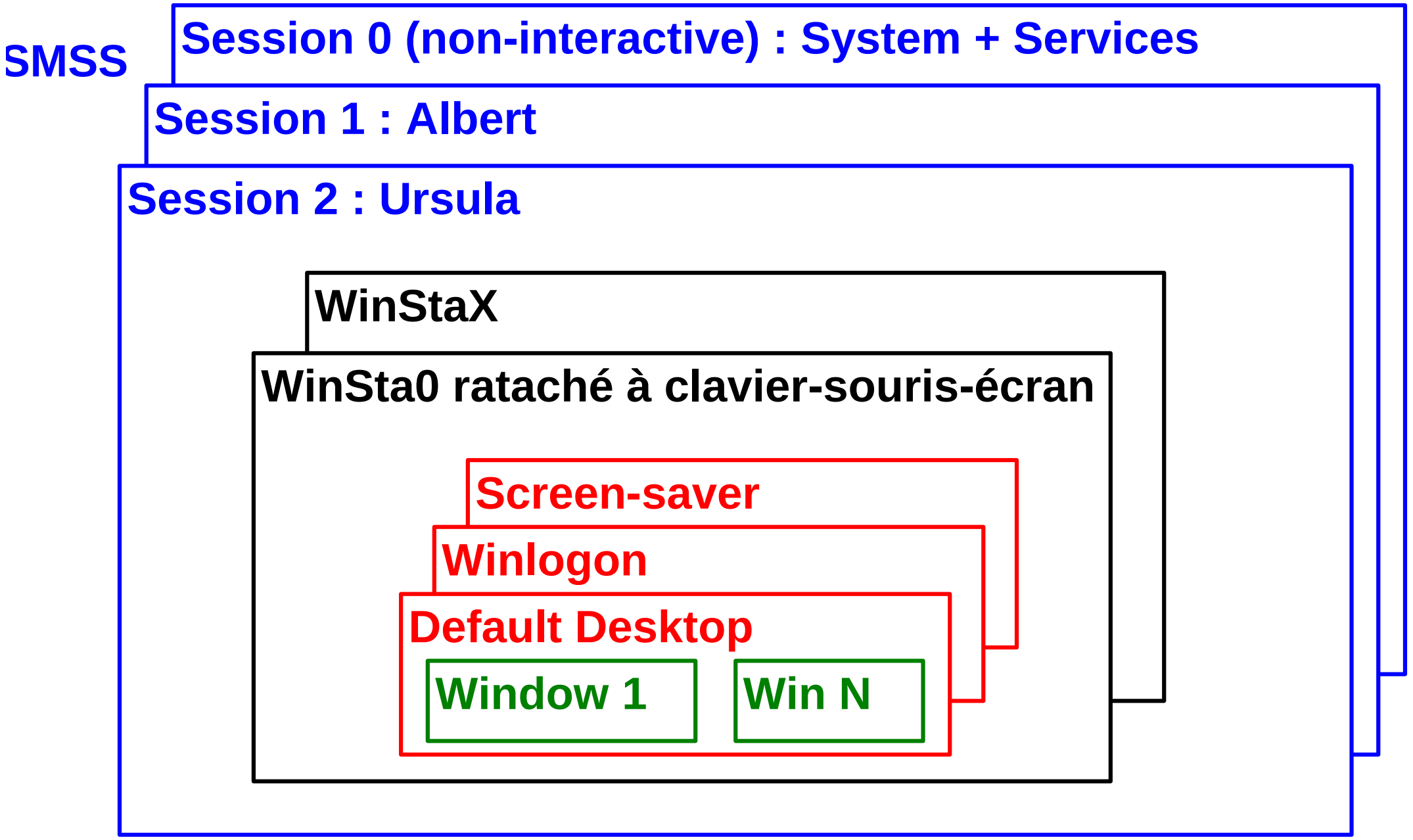
- 1er compte créé fait partie du groupe *Administrators*

- les autres comptes créés sont membres du groupe *Users*

- UAC est activé

- Firewall activé

Sessions, *Windows Stations*, *Desktops*, *Windows*



What's a windows station ?

- A windows station is a secure container that contains a clipboard, some global information, and a set of one or more desktops. A Windows 2000 session will have several windows stations, one assigned to the logon session of the interactive user, and others assigned to the Winlogon process, the secure screen saver process, and any service that runs in a security context other than that of the interactive user.
- The interactive window station assigned to the logon session of the interactive user also contains the keyboard, mouse, and display device. The interactive window station is visible to the user and can receive input from the user. All other window stations are noninteractive, which means that they cannot be made visible to the user, and cannot receive user input.
- http://www.microsoft.com/technet/security/bulletin/fq00-020.mspx

What's a desktop ?

- A desktop is a secure container object that is contained within a window station. There may be many desktops contained within a windows station.

- A desktop has a logical display surface and contains windows, menus, and hooks. Only the desktops of the interactive window station can be visible and receive user input. On the interactive window station, only one desktop at a time is active. This active desktop, also known as the input desktop, is the one that is currently visible to the user and that receives user input.

- http://www.microsoft.com/technet/security/bulletin/fq00-020.mspx

- Parler du dipl. Solleder http://www.tdeig.ch/windows/solleder_M.pdf

Shatter attack

- Utilisateur qui manipule son clavier ou sa souris communique avec son applications à l'aide de messages Windows

- Malheureusement à l'intérieur d'un bureau *(desktop)*, chaque application peut envoyer un message à une fenêtre car aucun mécanisme d'authentification n'existe

- Technique *(Exploiting design flaws in the Win32 API for privilege escalation)*

  A partir du compte Guest

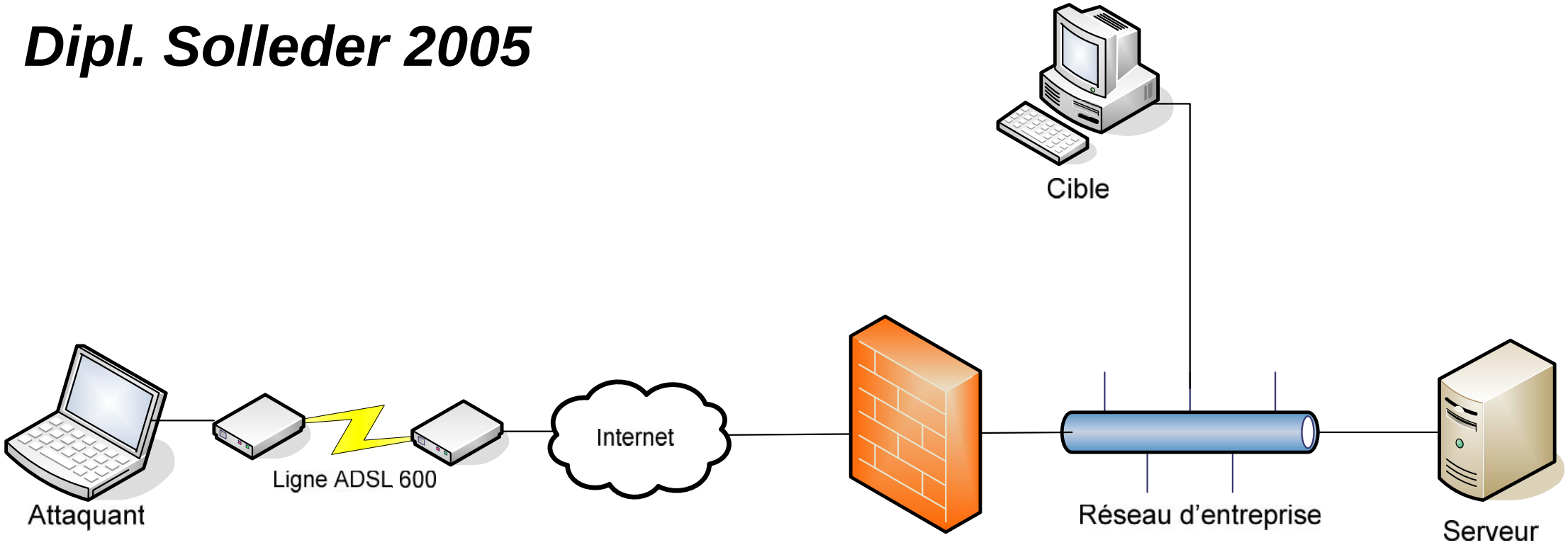
  Utiliser une fenêtre du bureau (NA VirusScan) qui s'exécute avec le compte LocalSystem

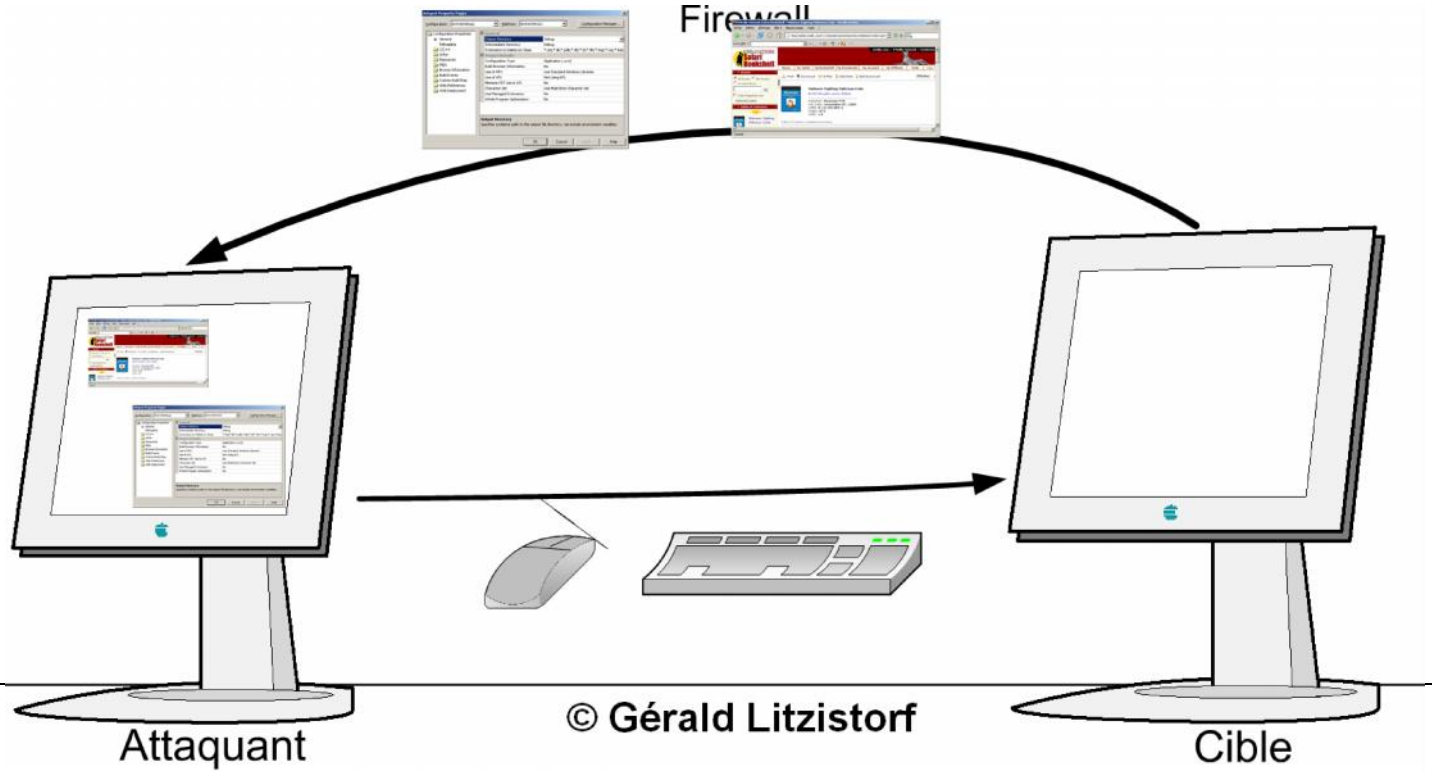
  Injecter puis exécuter l'exploit pour élever les privilèges

- Solution dans Vista : plus de services dans Session 0 + UIPI

- http://en.wikipedia.org/wiki/Shatter_attack

Dipl. Solleder 2005





Cahier des charges

- Furtivité

Ressources CPU	négligeable (~1%)
Taille mémoire	12 kByte
Taille buffer	taille de la fenêtre originale
	1024 x 768 x 32 / 8 = 3,1 Mbyte

Charge réseau : compression (8 bpp + *run length* + codage différent.)

	1ère	suivante
cmd.exe	10%	0 – 10%
calc.exe	20%	< 1%

- Exécution en mode utilisateur
- Mémoire de diplôme → http://www.tdeig.ch/windows/solleder_M.pdf

Volume NTFS (New Technologies File System)

- Volume = partition logique du disque (physique)

  C:\ pour le système (exécutables) séparation

  D:\ pour les données recommandée

- *Sector* = unité de stockage physique en Byte
- *Cluster* = unité de stockage en Byte vue par NTFS

  groupe de secteurs

```
C:\>fsutil fsinfo ntfsinfo c:
...
Bytes Per Sector  :                512        Sector
Bytes Per Cluster :                4096       Cluster
Bytes Per FileRecord Segment    : 1024        MFT record
```

Autorisations NTFS

- Une **partition** au format NTFS donne accès à des mécanismes d'autorisation du type **ACL *(Access Control List)***

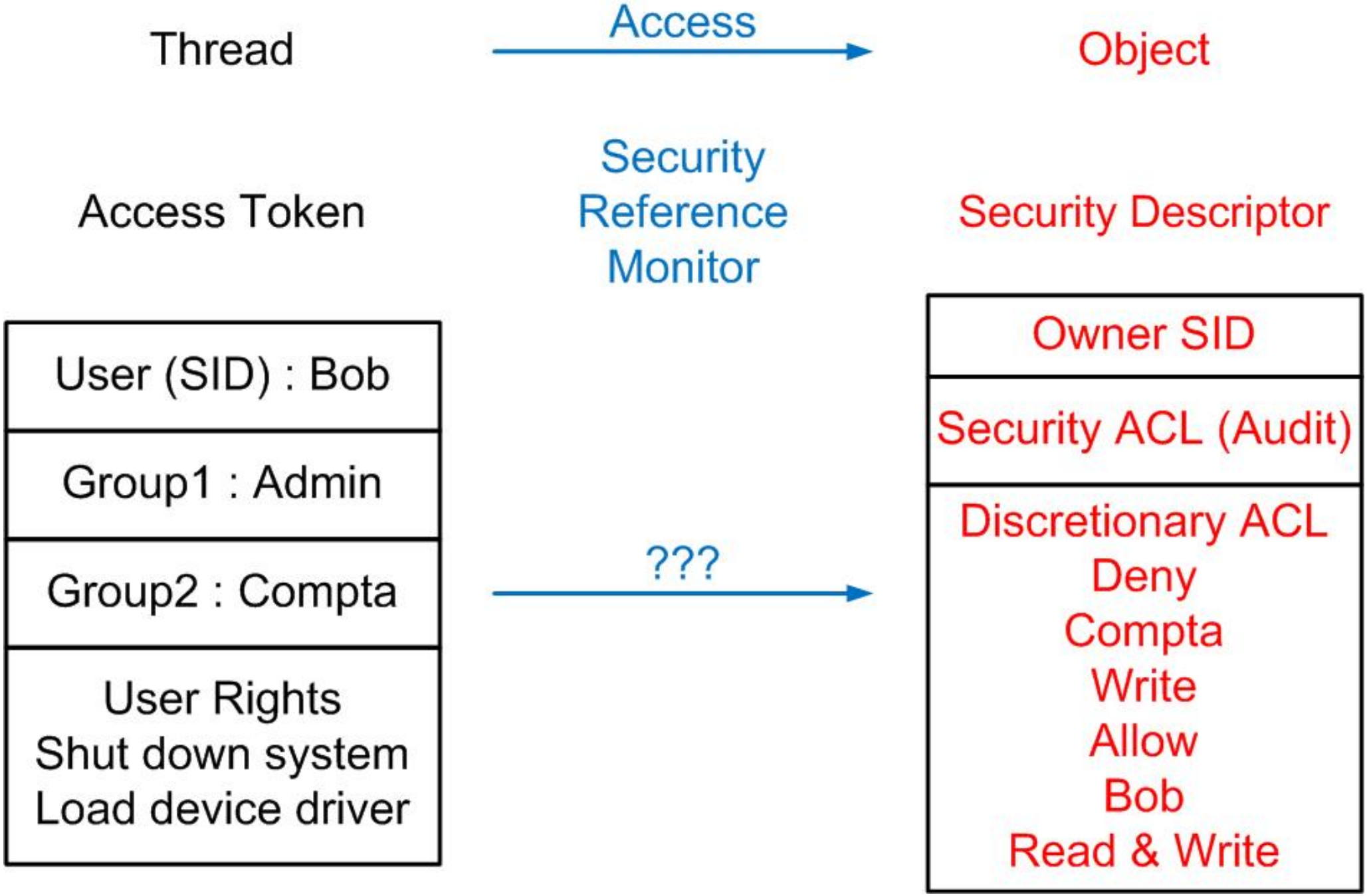
- **Exemples**

  Autoriser l'utilisateur Jean à accéder au dossier D:\privé

  Autoriser Pierre à lire le fichier salaire.doc

  Autoriser les membres du groupe Admin à exécuter regedit.exe

- Il s'agit d'un mécanisme de type ***white-list*** (ou *black-list*) appelé aussi *Discretionary ACL (DACL)* → **voir slide 47 = 23**


Thread
Access
Object
Access Token
Security Reference Monitor
Security Descriptor
User (SID) : Bob
Group1 : Admin
Group2 : Compta
User Rights
Shut down system
Load device driver
???
Owner SID
Security ACL (Audit)
Discretionary ACL
Deny
Compta
Write
Allow
Bob
Read & Write

NTFS : Autorisation standards DEMO

	Fichier	Dossier
• Full Control	X	X
• Modify	X	X
• Read & Execute	X	X
• List Folder Content		X
• Read	X	X
• Write	X	X

NTFS : Autorisations étendues sur un dossier

	R	LF	R&E	W	M	FC
• Traverse Folder		X	X		X	X
• List Folder	X	X	X		X	X
• Read Attributes	X	X	X		X	X
• Creates Files				X	X	X
• Create Folders				X	X	X
• Write Attributes				X	X	X
• Delete					X	X
• Read Permissions	X	X	X	X	X	X
• Change Permissions						X
• Take Ownership						X

NTFS : Autorisations étendues sur un dossier

• Traverse Folder	Accéder au sous-dossier
• List Folder	Voir les fichiers et dossiers
• Read Attributes	Lire les attributs (hidden, system, …)
• *Read Extended Attributes*	obsolète
• Creates Files	Créer un nouveau fichier
• Create Folders	Créer un sous-dossier
• Write Attributes	Modifier les attributs
• *Write Extended Attributes*	obsolète
• *Deletes Subfolders and Files*	POSIX
• Delete	Supprimmer fichier, dossier et attributs
• Read Permissions	Lire security tab
• Change Permissions	Modifier le descripteur de sécurité
• Take Ownership	Devenir propriétaire du dossier

NTFS : Autorisations étendues sur un fichier

	R	R&E	W	M	FC
• Execute File		X		X	X
• Read Data	X	X		X	X
• Read Attributes	X	X		X	X
• Write Data			X	X	X
• Append Data			X	X	X
• Write Attributes			X	X	X
• Delete				X	X
• Read Permissions	X	X	X	X	X
• Change Permissions					X
• Take Ownership					X

NTFS : Autorisations étendues sur un fichier

• Execute File	Exécuter un fichier (exe, bat, …)
• Read Data	Ouvrir, lire et copier un fichier
• Read Attributes	Lire les attributs (hidden, system, …)
• Write Data	Modifier un fichier
• Append Data	Ajouter des données à un fichier existant
• Write Attributes	Modifier les attributs
• Delete	Suppression de fichier et des attributs
• Read Permissions	Lecture de *security tab*
• Change Permissions	Modification de *security tab*
• Take Ownership	Devenir propriétaire du fichier

NTFS : autorisations de C:\ par défaut

Name	Permission	Inherited ...	Apply To
Administrators (INS...	Full control	<not inhe...	This folder, subfolders and files
SYSTEM	Full control	<not inhe...	This folder, subfolders and files
Users (INSPIRON6...	Read & execute	<not inhe...	This folder, subfolders and files
Authenticated Users	Special	<not inhe...	Subfolders and files only
Authenticated Users	Create folders / ...	<not inhe...	This folder only

- Le système (Vista) possède des autorisations **par défaut**
- Les autorisations sont données aux **groupes** *Administrators*, …
- Les objets (dossier, fichier) créés **héritent** des autorisations
- Ne pas oublier de prendre en compte le champ ***Apply To = This folder, subfolders & files !*** *This folder only / This folder and subfolders / This folder and files / Subfolders and files only / Subfolders only / Files only*

NTFS : labo §5

- **Cumul des autorisations des groupes**

- ***Effective Permissions***

- **Donner à Ursula les autorisations NTFS minimales sur le dossier et les fichiers suivants :**

D:\Test	pour parcourir ce dossier
D:\Test\Read.txt	pour lire ce fichier
D:\Test\calc.exe	pour exécuter calc.exe copié depuis C:\Windows\System32\calc.exe
D:\Test\ReadWrite.txt	pour lire & écrire dans ce fichier

- **Supprimer le mécanisme d'héritage**

NTFS : propriétaire & labo §6

- Chaque fichier et dossier possède un **propriétaire unique**
- Utiliser l'onglet ***Owner***

- Propriétaire est celui qui **crée** le fichier – dossier
- Le compte ayant l'autorisation ***Take Ownership*** peut devenir propriétaire du fichier – dossier
- L'admin. peut toujours devenir propriétaire d'un fichier – dossier
- **Labo §6 :** Empêcher qu'un membre des utilisateurs ne puisse exécuter **`C:\Windows\regedit.exe`**

Audit Policy

- Il peut être utile de **conserver des traces *(logs)* d'actions** telles qu'authentification réussie (et pas réussie), accès à un fichier sensible comme celui des salaires, …

- Audit account management (success / failure) → labo §7c

  Action (créer, changer, supprimer compte – mot de passe)

- Audit logon events (success / failure) → labo §7c

  Authentification locale et réseau

- Audit system events (success / failure) → labo §7a

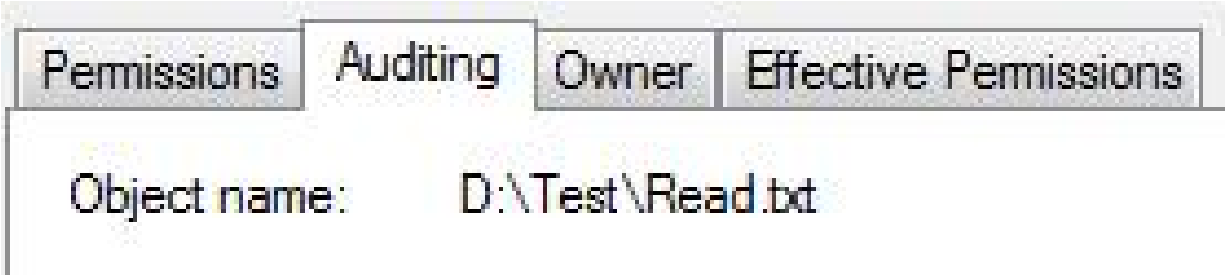
  System startup, shutdown, changes to auditing system

- **Résultats** dans *Event Viewer* démo

Audit Policy & Security ACL (slide 49)

- Les accès aux objets Windows tels que fichiers, dossiers, clé de registre, … peuvent être consignés dans un fichier de logs avec l'option Audit object access (success / failure)

- Grâce aux *Security* ACL, chaque objet dispose de la granularité NTFS pour chaque compte et chaque groupe



→ Labo §7e

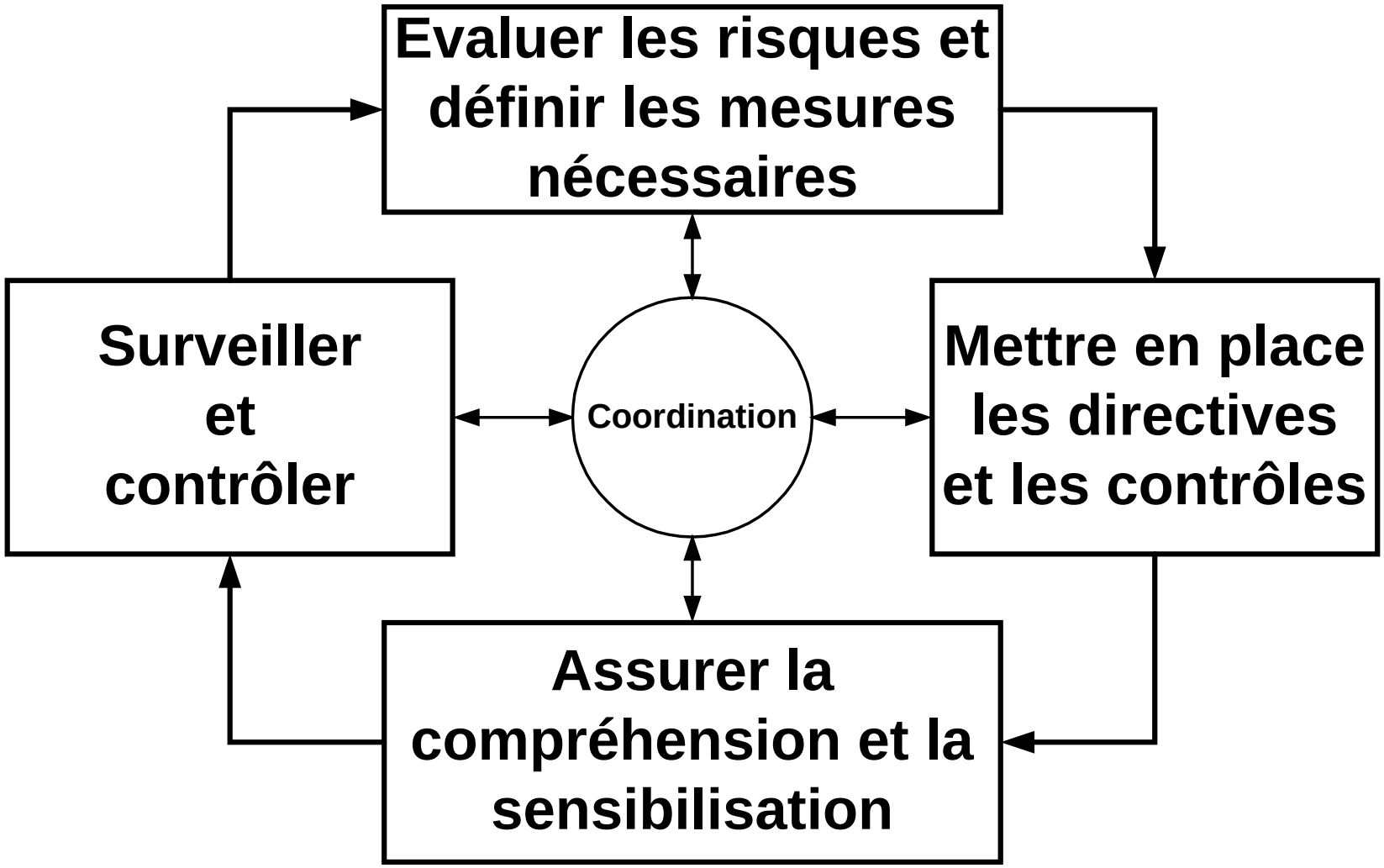
Labo Windows *(90 min)*

§1	User Account Control (UAC)	10’
§2	Task Manager & Resource Monitor	10’
§3	procexp	15’
§4	MIC	10’
§5	User Rights Assignment	5’
§6	Autorisation NTFS	20’
§7	Supprimer le droit d’exécuter	10’
§8	Audit	10’

Pour trouver rapidement l'outil

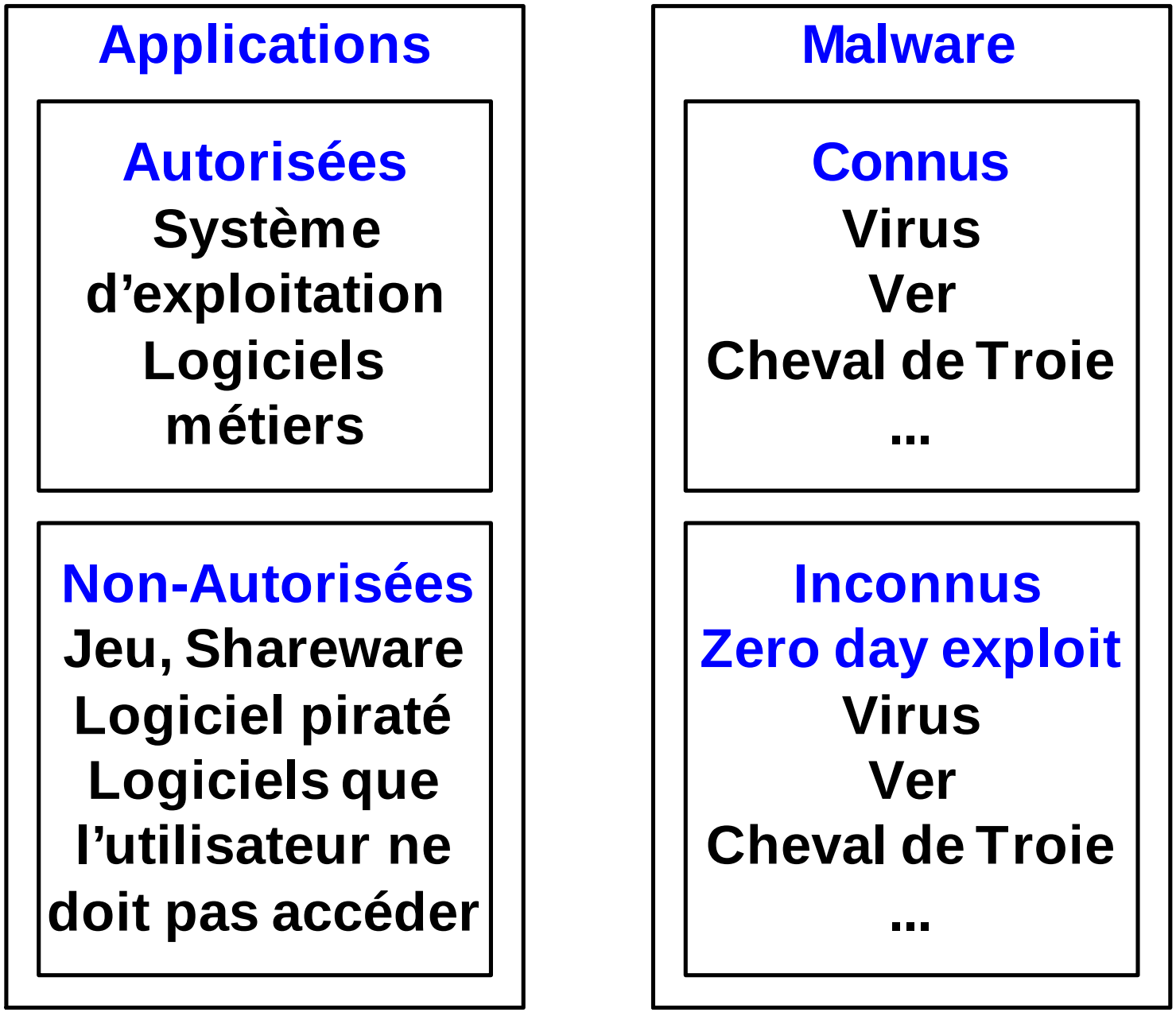
compmgmt.msc	*Computer Management*
eventvwr.msc	*Event Viewer*
lusrmgr.msc	*Local Users & Groups*
perfmon.msc	*Reliability & Performance Monitor*
devmgmt.msc	*Device Manager*
diskmgmt.msc	*Disk Management*
services.msc	*Services*
secpol.msc	*Local Security Policy*
gpedit.msc	*Group Policy Object Editor*
wf.msc	*Windows Firewall with Advanced Security*
certmgr.msc	*Certificates – Utilisateur actuel*

Principe 1 : Cycle de gestion des risques

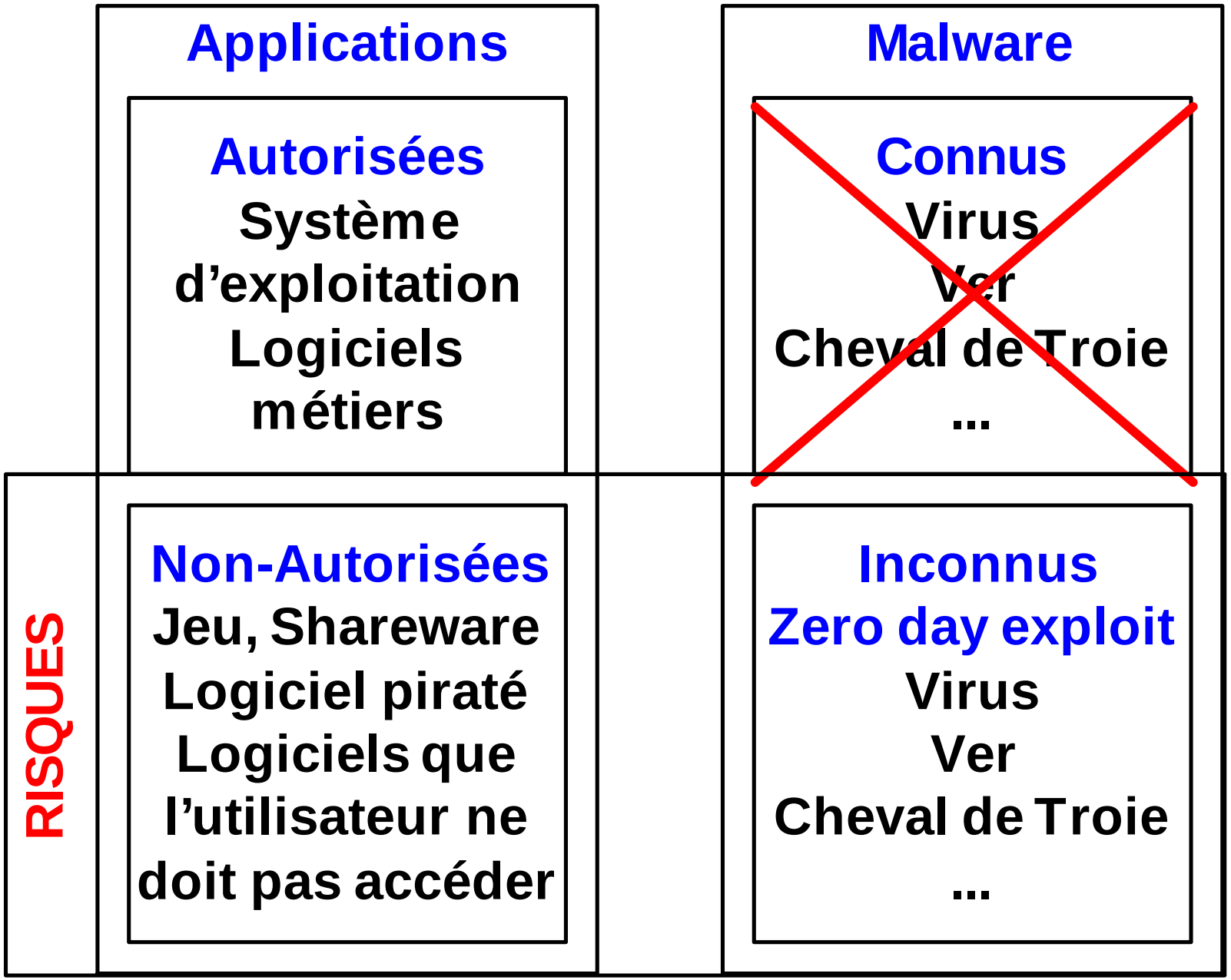


- Illustration → http://www.tdeig.ch/publication/BP_VoIP_Security.pdf
- Compromis entre mesures organisationnelles et sécurité logique

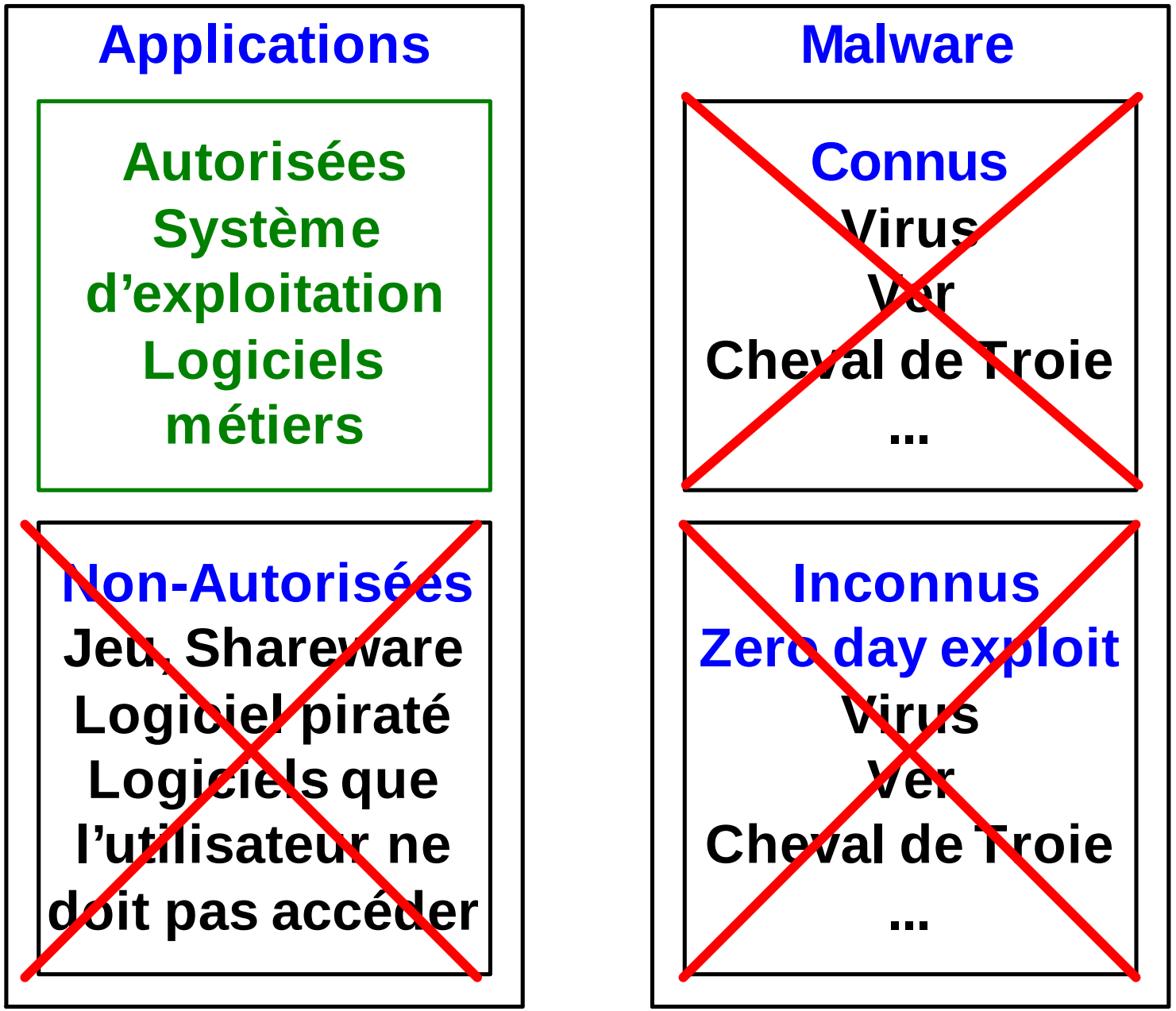
Principaux risques (SecureWave)



Protection de type black list



Protection de type white list



Principes de sécurité

2 Eduquer & sensibiliser les utilisateurs

- Tout système informatique (pas seulement les systèmes MS) présente des risques de failles (erreurs de programmation, erreurs conceptuelles)

3 Moindre privilège

- Utilisateur dispose des droits minimum (mode par défaut de Vista)
- Administrateur élève ses droits si nécessaire (installation de logiciel)
- Des applications telles que IE sont exécutées avec un niveau d'intégrité minimum (inférieur à une session utilisateur)

Principes de sécurité

4 CPU ne doit exécuter que du code légitime

- Exécution possible seulement depuis dossiers système **`c:\windows\system32, c:\Program Files\, ...`**
- Activer *Software Restriction Policies* disponibles depuis XP modèle *white-list* (ou *black-list*)
- TPM *(Trusted Platform Module)* chaîne de confiance : *loader*, *operating system*, applications

5 Protéger dossiers & fichiers système

- Partitions séparées Cpour le système (C:\) & les données (D:\)
- Autorisations NTFS de C:\ pour l'utilisateur (Read, eXecute), pour l'administrateur (Full) et de D:\ (no eXecute)

Limites de NTFS (failles conceptuelles)

Si NTFS est réputé pour ses autorisations (ACL), il l'est moins pour :

- La protection de ses metadonnées *(properties)*
  Il est très facile d'antidater un fichier *(TouchPro, …)*

- Les données ne sont pas effacées; seul un bit *(flag)* est inversé *(busy – free)*

- Il est facile de cacher des données, des exécutables dans ADS *(Alternate Data Streams)*
  http://www.securityfocus.com/infocus/1822

Principes de sécurité

6 Défense périmétrique

- Utilisateur à domicile protégé par un routeur ADSL (qui intègre un *firewall*) , utilisateur dans l'*intranet* de l'entreprise
- Par défaut, toutes les communications sortantes sont autorisées alors que tout paquet entrant est refusé

→ Les techniques d'attaque exigent la participation active (clic, …) de la victime

7 Défense en profondeur

- Antivirus, *Windows Defender (antispyware)*, …
- *Personal Firewall* pour l'utilisateur protégé par un *firewall*

8 Mises à jour

- Elles sont trop nombreuses (MS, …) !
- Utilisateur / 1000 postes utilisateur en entreprise / 10-100 serveurs

Principes de sécurité

9 Hardening

- User Right, Security Options, regedit, services, paramètres réseau
- Imposer une politique des mots de passe
- Activer l'audit
- Certains affirment qu'un serveur configuré par défaut révèle un manque de compétence en sécurité

10 Logs

- Le système effectue des tests et reportent des anomalies telles que le processus n'a pas démarré, le pilote *(driver)* n'est pas présent, …

  Il ne peut donc pas signaler des événements qu'il oublie de tester !

  → Faux négatifs = attaque réelle non détectée

  Faux positifs = intrusion signalée sans dégât → fausse alerte

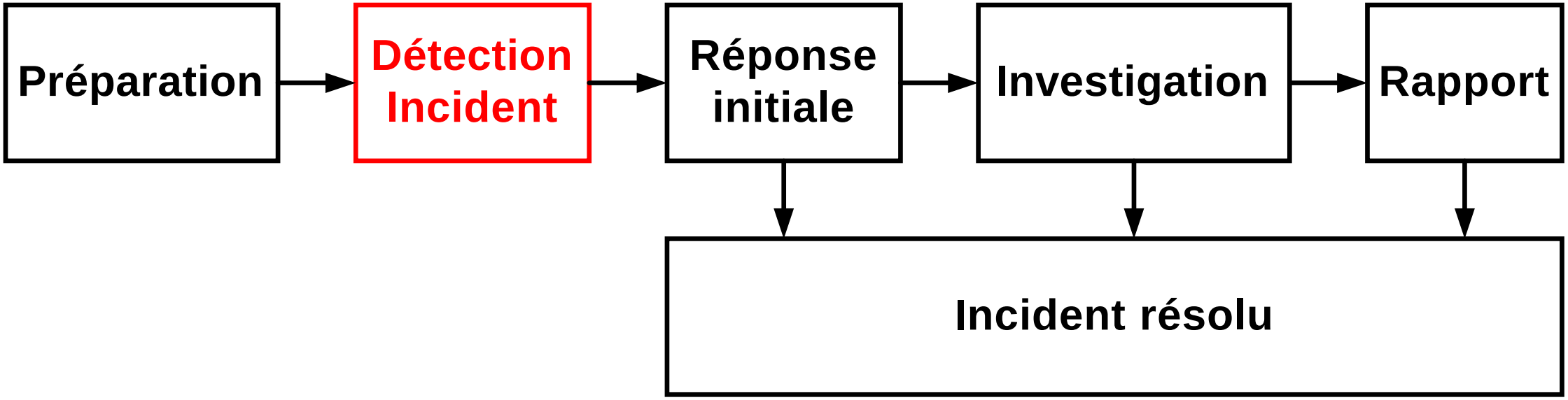
Forensics

- Les sciences forensiques se définissent comme l'ensemble des **principes scientifiques** et des **méthodes techniques** appliqués à l'investigation criminelle, pour prouver l'existence d'un crime et aider la justice à **déterminer l'identité de l'auteur et son mode opératoire**

- Risques à analyser (my PC / mail server), pertes financières, …
- Collecter les données volatiles (qui auront disparu au prochain boot)
- Ne pas écrire sur le disque du système investigué
- Faux négatifs et faux positifs

- Méthodologies et outils à définir et à utiliser

Méthodologie (Foundstone)



- Préparation → posséder une référence (processus, ports TCP, …)
- Un incident (vol de données) non détecté = faux négatif
- Qui détecte l'incident ?

  Utilisateur se plaint de lenteur, admin consulte les logs, IDS, …
- Réponse initiale basée sur *live analysis*
- Investigation basée sur *post-mortem analysis*

Données volatiles (perdues lors du boot)

- Illustration pour un serveur DNS

- Durée d'exécution *(uptime)*
- Liste des processus et threads présents en RAM
- Charge CPUs
- Liste des sessions utilisateur établies (accès physqiue / réseau)
- Occupation disque et partitions → % d'espace libre
- Configuration réseau → adr IP, …
- Services actifs
- …

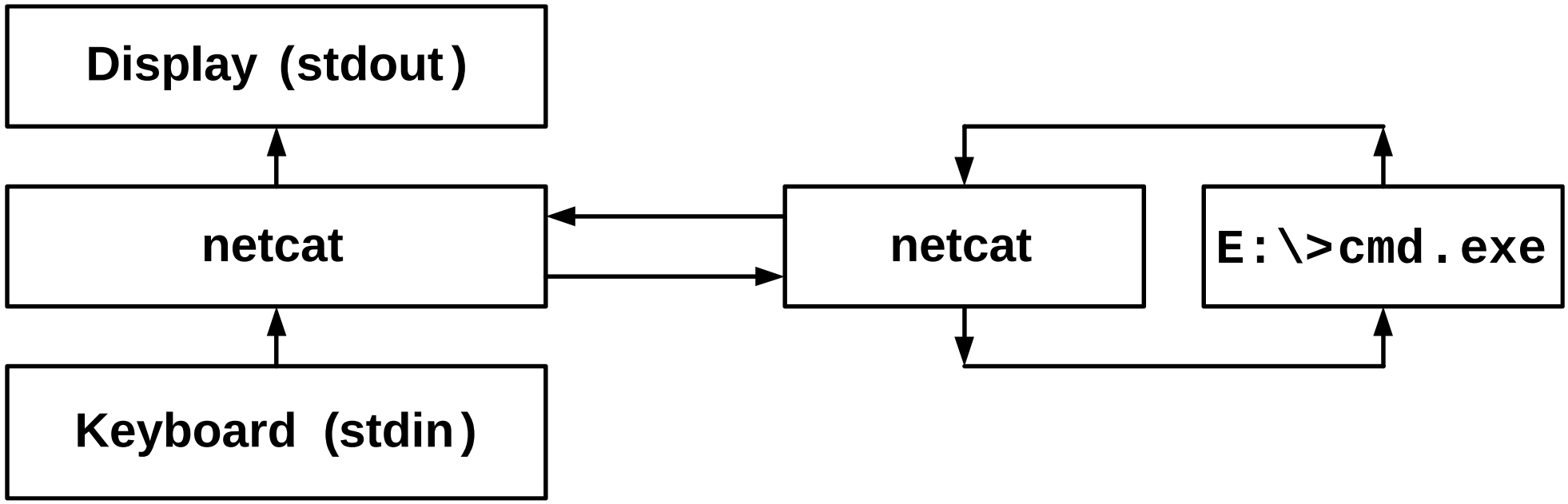
- Le travail consiste à comparer ces éléments (processus, charge, occupation mémoire, services, …) avec une **référence**

  → slide précédent

Minimiser l'interaction avec le système investigué

- PC_Distant – PC_Investigué
- Redirection clavier-écran avec netcat
- Commandes (binaires) stockées sur CD de PC_Investigué → **`E:\`**
- Automatisation → script basé sur *Command Line Interface (CLI)*

`$nc IP_Investigue 2000` **`E:\> nc -l -p 2000 cmd.exe`**



Post-mortem analysis

- Récupérer des preuves sur le disque

  → Eteindre PC_I, enlever le disque, le brancher sur PC-D

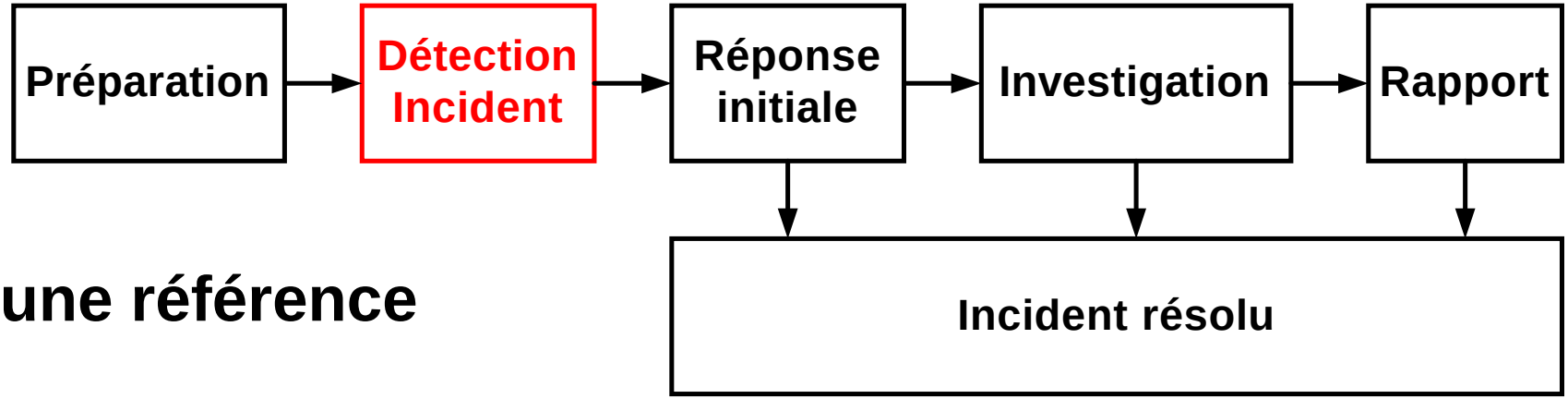
  ou

  → Copier le disque avec dd et netcat

  ```
  PC_D : nc -l -p 9000 > disk1.dd
  PC_I : dd if=\\.\Drive0 bs=2k | nc -w 3 IP_D 9000
  ```

- Fichiers effacés
- Fichiers supplémentaires (malware, …) dus à l'incident
- Recherche dans les meta-données : date, heure, …
- Recherche dans le contenu → data carving

Vue d'ensemble (suite slide 72)



- **Préparation**

  Construire une référence

- Détection

  Qui ? Quoi ? Comment ? Incident reproductible ?

- Live analysis → slide 73

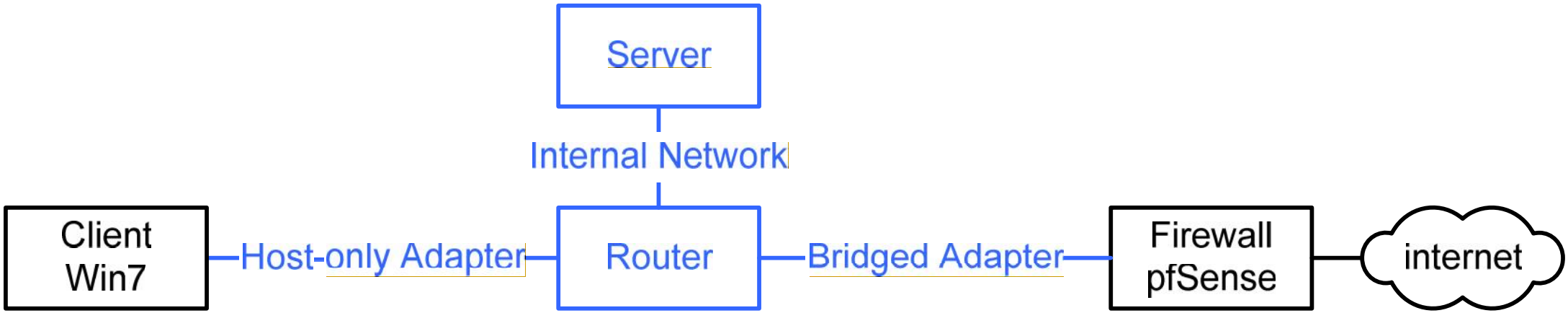
  Récupérer les données volatiles sans modifier le système

- Post-mortem analysis → slide 75

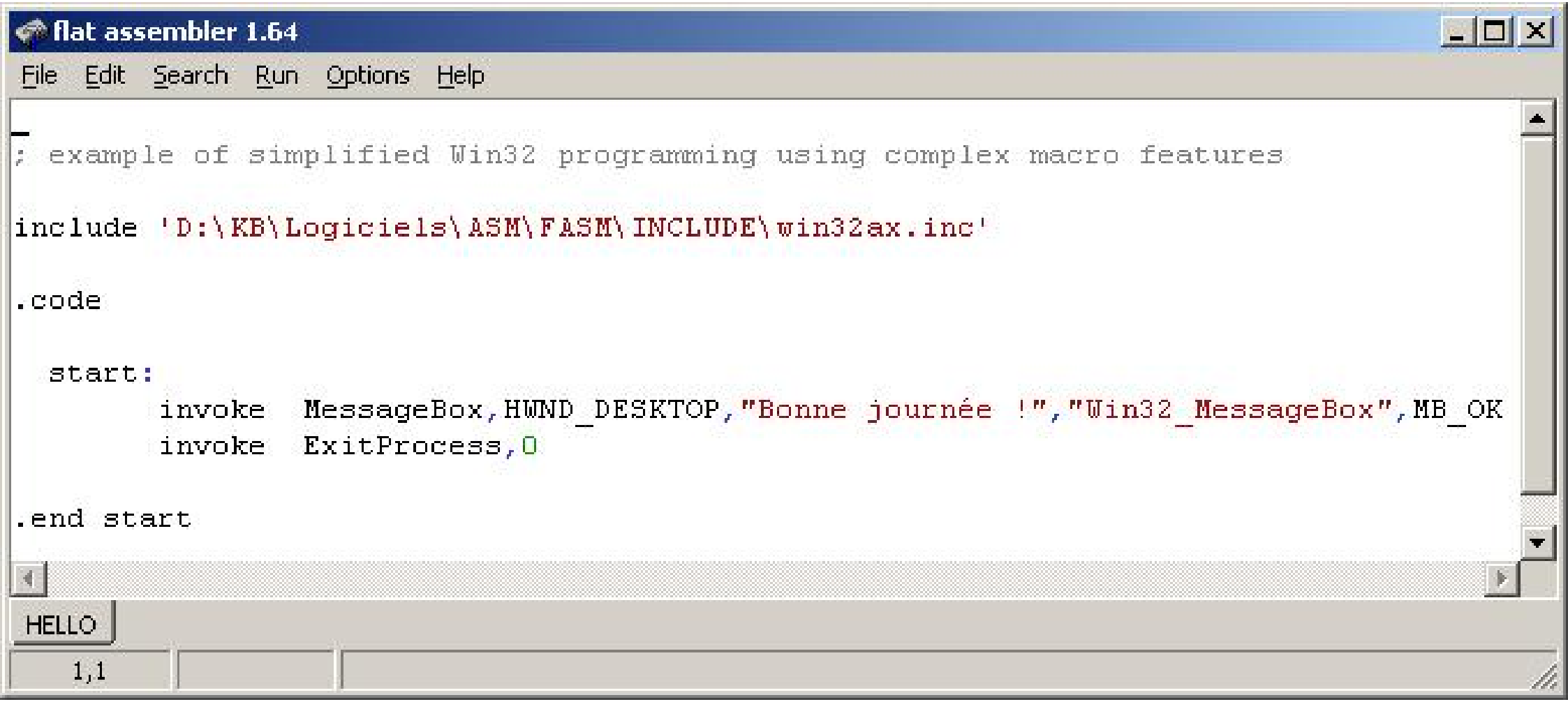
→ http://en.wikipedia.org/wiki/Computer_forensics

Labo Vbox-Linux (90 min)

§1-3	Prérequis à valider avant la séance de labo	
§4	Linux partie Réseau	30’
§5	Linux partie Système	30’
§6	Travail personnel	30’



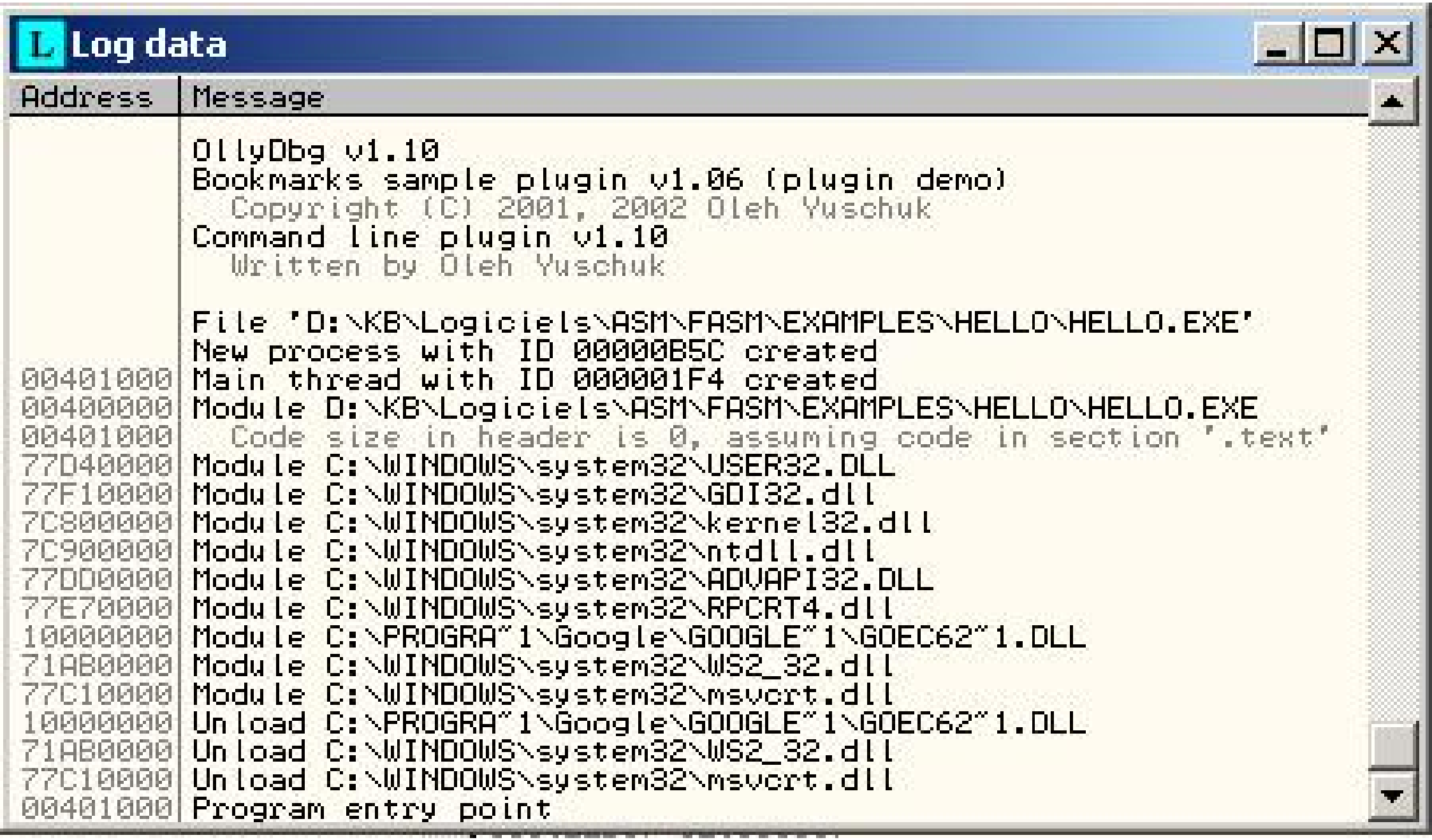
Programme source (assembleur IA32)



Occupation mémoire de

Address	
0006D000	pile *(stack)*
00400000	Hello *(PE header, code, data)*
77D40000	USER32.DLL *(PE header, code, data)*
77DD0000	ADVAPI32.DLL *(PE header, code, data)*
77E70000	RPCRT4.DLL *(PE header, code, data)*
77F10000	GDI32.DLL *(PE header, code, data)*
7C800000	KERNEL32.DLL *(PE header, code, data)*
7C900000	NTDLL.DLL *(PE header, code, data)*

Chargement des DLLs lors de l'exécution



Exécution

```
Address      HEXA        CODE & DATA

00401000     6A 00       PUSH 0
00401002     E8 11 ..    CALL HELLO.00401018
00401007     57 69 ..    Win32_MessageBox  (ASCII)
00401018     E8 10 ..    CALL HELLO.0040102D
0040101D     42 6F ..    Bonne journée !   (ASCII)
0040102D     6A 00       PUSH 0
0040102F     FF 15 ..    CALL .. USER32.MessageBoxA
00401035     6A 00       PUSH 0
00401037     FF 15 . .   CALL .. KERNEL32.ExitProcess
```

Win32 API (Application Program Interface)

Exécution : Thread & Handle

Threads

Ident	Entry	Data block	Last error	Status	Priority	User time	System time
000001F4	00401000	7FFDF000	ERROR_DLL_INIT_FA	Active	32 + 0	0.0000 s	0.0300 s

Handles

Handle	Type	Refs	Access	T	Info	Name
00000024	Desktop	3886.	000F01FF			\Default
00000008	Directory	81.	00000003			\KnownDlls
00000014	Directory	49.	000F000F			\Windows
00000030	Directory	455.	0002000F			\BaseNamedObjects
0000001C	Event	3.	001F0003			
0000000C	File (dir)	2.	00100020			d:\KB\Logiciels\ASM\FASM\EXAMPLES\HELLO
0000003C	Key	2.	000F003F			HKEY_LOCAL_MACHINE
00000004	KeyedEvent	47.	000F0003			\KernelObjects\CritSecOutOfMemoryEvent
00000018	Port	3.	001F0001			
00000010	Section	46.	000F001F			
00000020	WindowStation	99.	000F037F			\Windows\WindowStations\WinSta0
00000028	WindowStation	99.	000F037F			\Windows\WindowStations\WinSta0

Occupation mémoire de Notepad (extrait des 21 dlls)

```
ListDLLs v2.25 - DLL lister - www.sysinternals.com
notepad.exe pid: 3044
Command line: "C:\WINDOWS\system32\notepad.exe"
  Base       Path
  01000000   C:\WINDOWS\system32\notepad.exe
  7c900000   C:\WINDOWS\system32\ntdll.dll
  7c800000   C:\WINDOWS\system32\kernel32.dll
  77f60000   C:\WINDOWS\system32\SHLWAPI.dll
  77dd0000   C:\WINDOWS\system32\ADVAPI32.dll
  77e70000   C:\WINDOWS\system32\RPCRT4.dll
  77f10000   C:\WINDOWS\system32\GDI32.dll
  77d40000   C:\WINDOWS\system32\USER32.dll
  77c10000   C:\WINDOWS\system32\msvcrt.dll
  7c9c0000   C:\WINDOWS\system32\SHELL32.dll
```

Références

- MS Windows Internals — Russinovich-Solomon
- Malware — Skoudis — ISBN 0-13-101405-6
- Reversing — Eilam — ISBN 0-7645-7481-7
- http://flatassembler.net/ — flat assembler 1.64
- http://www.ollydbg.de/ — Windows debugger
- http://www.sysinternals.com/ — outils