
Metro Olografix Hacking Party

# *Security by Virtualization*

*19 Maggio 2007 – Pescara*

*Marco Balduzzi <embyte@madlab.it>*

# Le ragioni della sfida

- ✓ I convenzionali meccanismi di protezione vengono alterati ed evasi da:
  - gli stessi utenti del sistema (anche involontariamente,
    - » *personal antivirus e firewall / wireless hot-spot*)
  - intrusi esterni
  - software pericoloso *(virus e malware)*
- ✓ Gli stessi sono talvolta inefficaci *(VPN)*

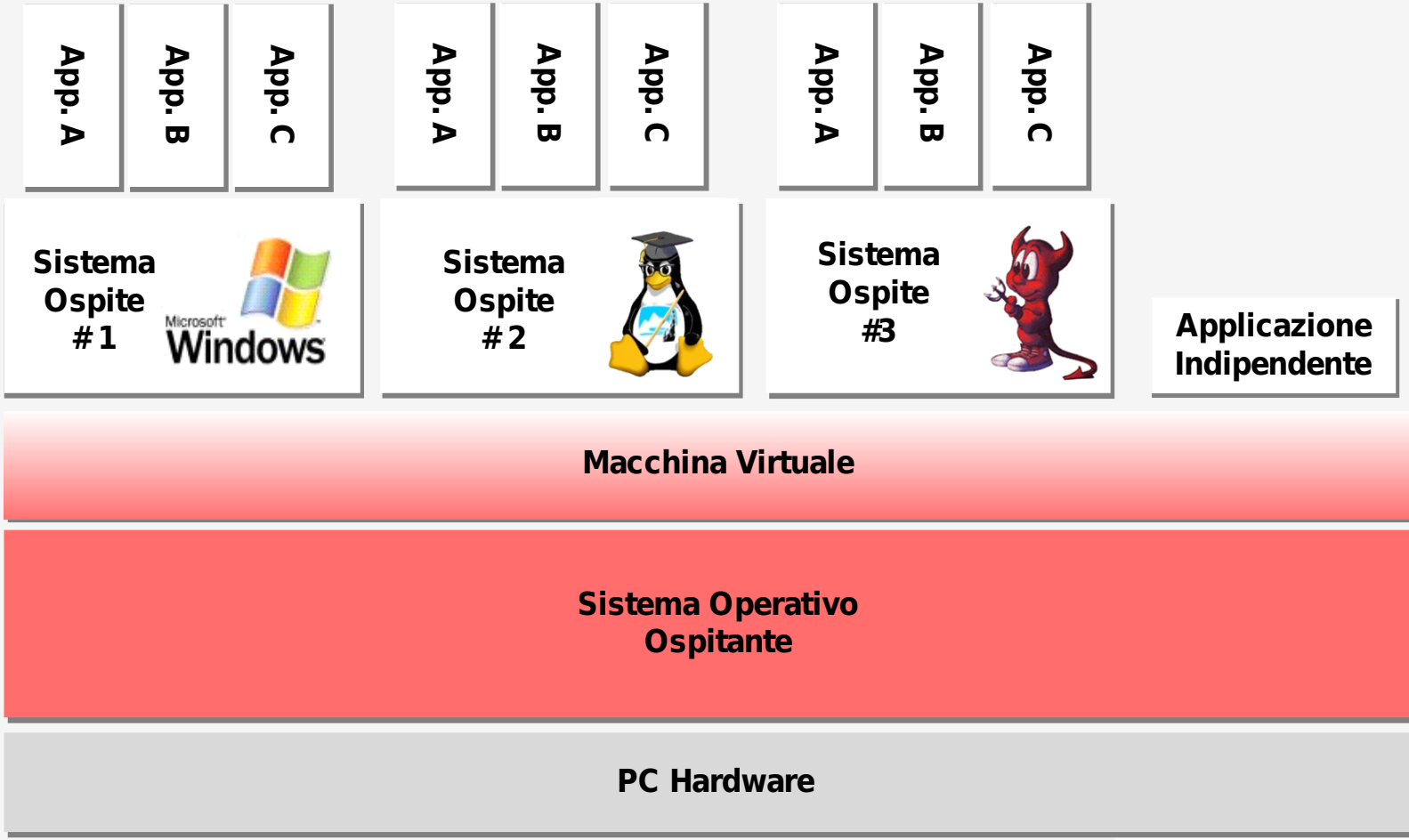
- ✓ Furti e perdite compromettono la confidenzialità delle informazioni

# Il concetto di virtualizzazione

- ✓ Creazione di una versione “virtuale” dell’hardware per poter eseguire contemporaneamente (più) sistemi operativi *guest* su uno stesso sistema *host*
- ✓ Separazione sistema guest e host
- ✓ Gestione delle risorse *(memory/CPU limiting)*

- ✓ Emulazione harware: emaulazione del completo set di istruzioni della CPU per un particolare hardware *(Bosch)*
- ✓ Virtualizzazione completa (nativa): *(VmWare)*
- ✓ Para-virtualizzazione: driver virtualizzazione integrati nel sistema guest; supporto hardware *(XEN)*

# *Server consolidation* - L'approccio tradizionale



# Altre applicazioni

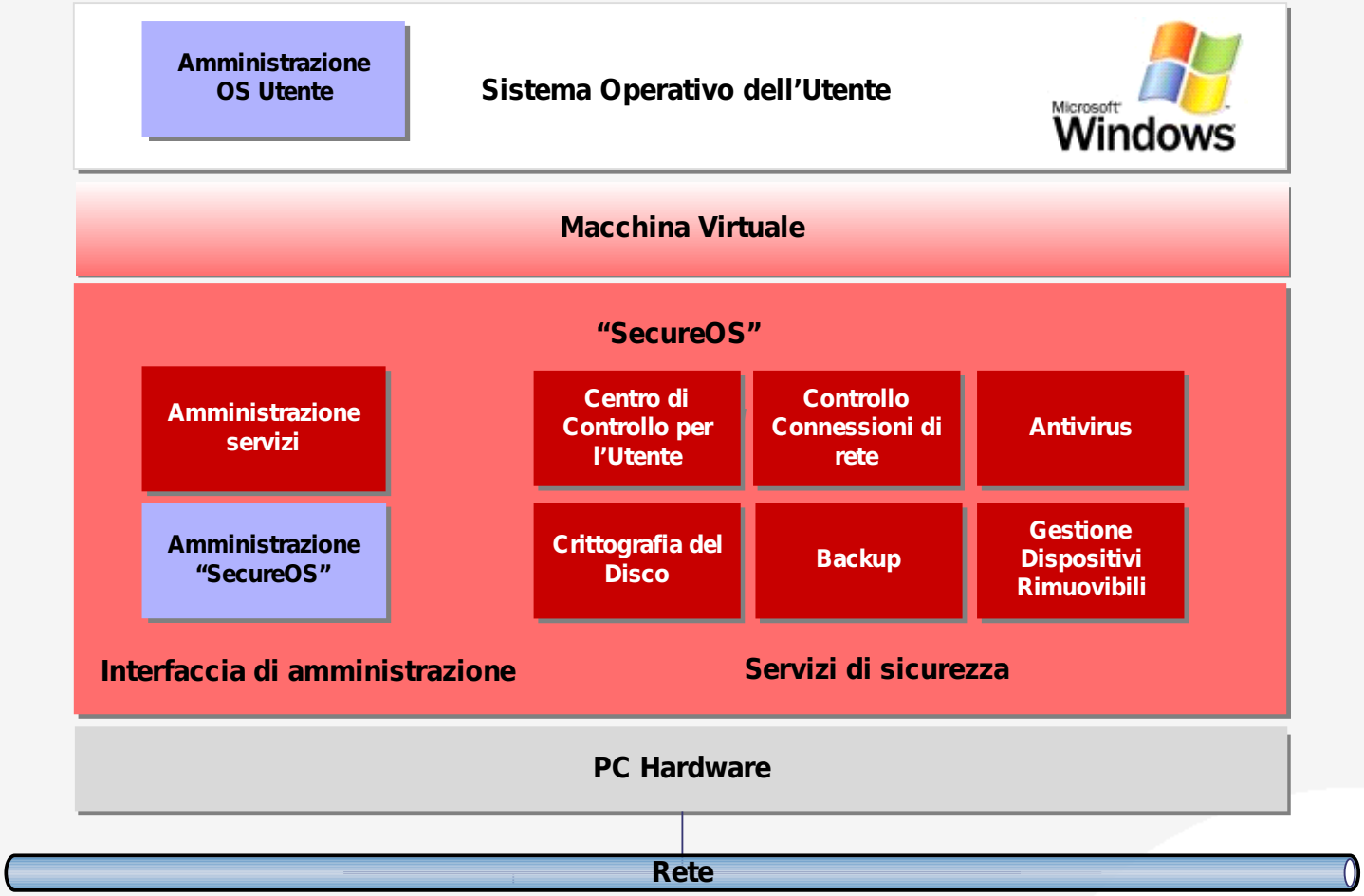
- ✓ Ambienti di simulazione distributi
- ✓ Test di software particolare *(driver, firmware, kernel)*
- ✓ Implementazione di sistemi esca *(honeypot)*
- ✓ Distribuzione di sistemi *ready-to-use:* copie di valutazione/demo, “capture the flag”

# *Security by Virtualization*

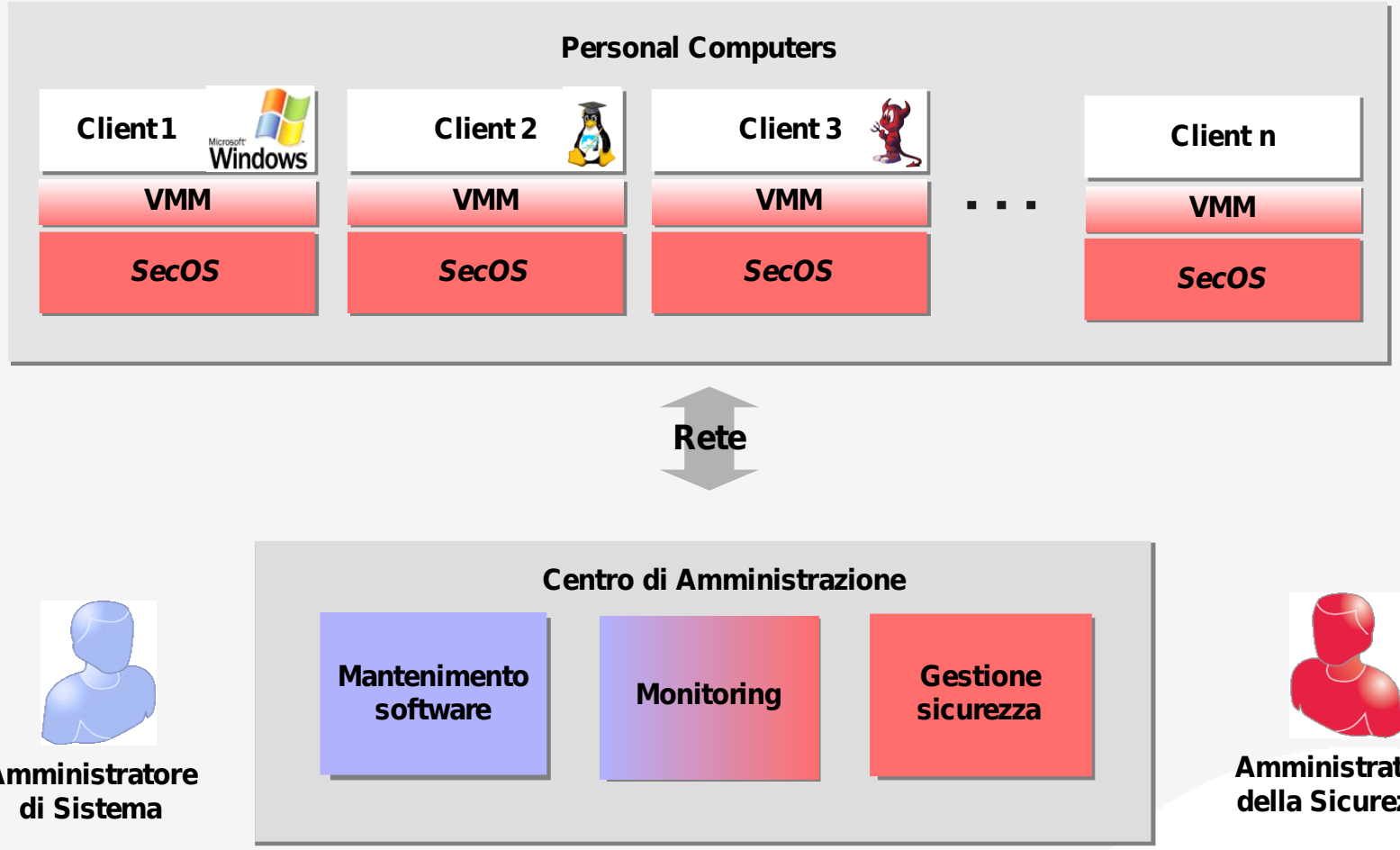
- ✓ Uso della virtualizzazione per separare i meccanismi di sicurezza dal sistema utente in un sottosistema isolato

- ✓ Protezione e amministrazione sicura delle funzionalità di sicurezza
- ✓ Applicazione rigida delle politiche di sicurezza
- ✓ Sicurezza trasparente al sistema utente
- ✓ Miglioramento delle soluzioni di protezione convenzionali *(disk encryption)*
- ✓ Ulteriori servizi di sicurezza *(controllo dei dispositivi rimuovili)*
- ✓ Infrastruttura di gestione omogenea e integrata

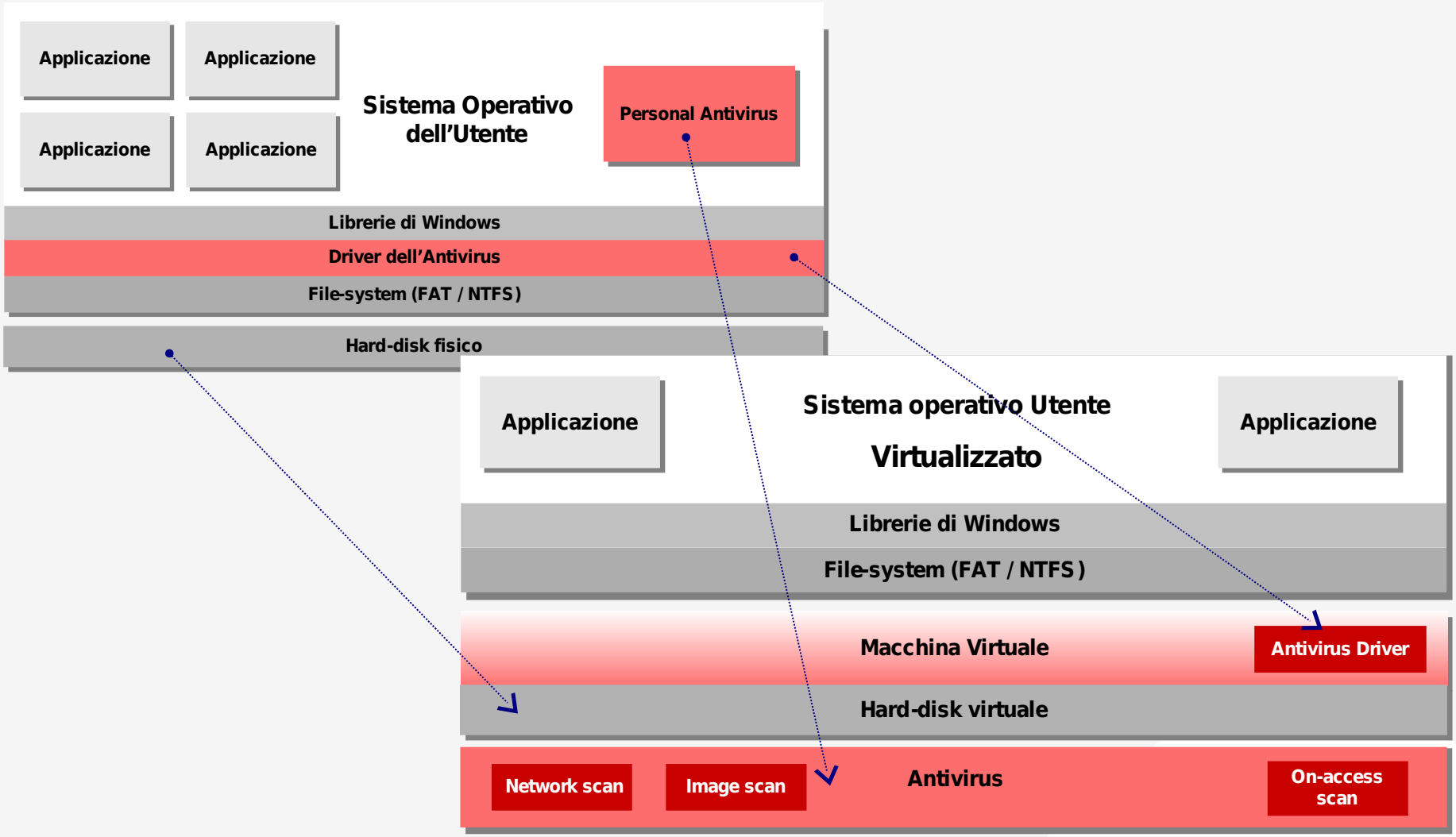
# *Security by Virtualization* – Il nuovo paradigma



# *Security by virtualization* – Decentralizzazione



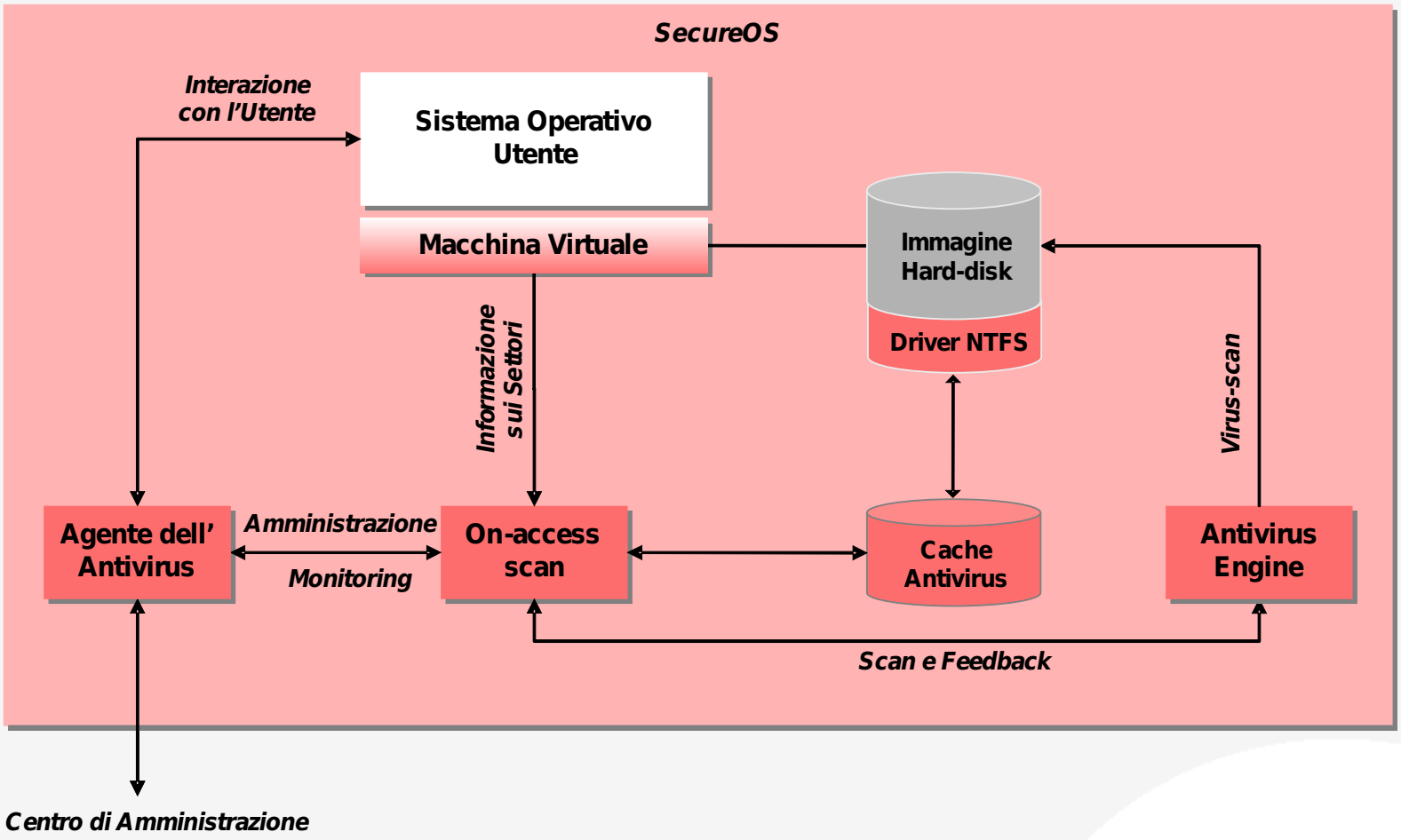
# Mettiamo in sicurezza l'Antivirus



# Tre tipologie di Antivirus

- ✓ *On-access scan:* analisi in tempo reale dei file acceduti
- ✓ *Network scan:* scansione automatica delle connessioni di rete; comprese le VPN, alcuni protocolli crittografici *(https)* e su dispositivi rimuovibili *(PCMCIA Wireless)*
- ✓ *Image scan:* analisi completa del sistema utente e protezione copie di backup; scansione *offline* per evitare problemi (corruzione file-system, salto di dati)

# *On-access scan:* analisi ad accesso



# Problematiche affrontate (1)

- ✓ Efficiente sincronizzazione tra cache dell'antivirus, file-system sistema-utente e contenuto del disco
- ✓ Cache veloce: struttura dati ad albero bilanciato (AVL). Sovraccarico di bilanciamento compensato da un miglioramento del 70% nella gestione di dati non casuali (accessi ripetitivi e sequenziali)

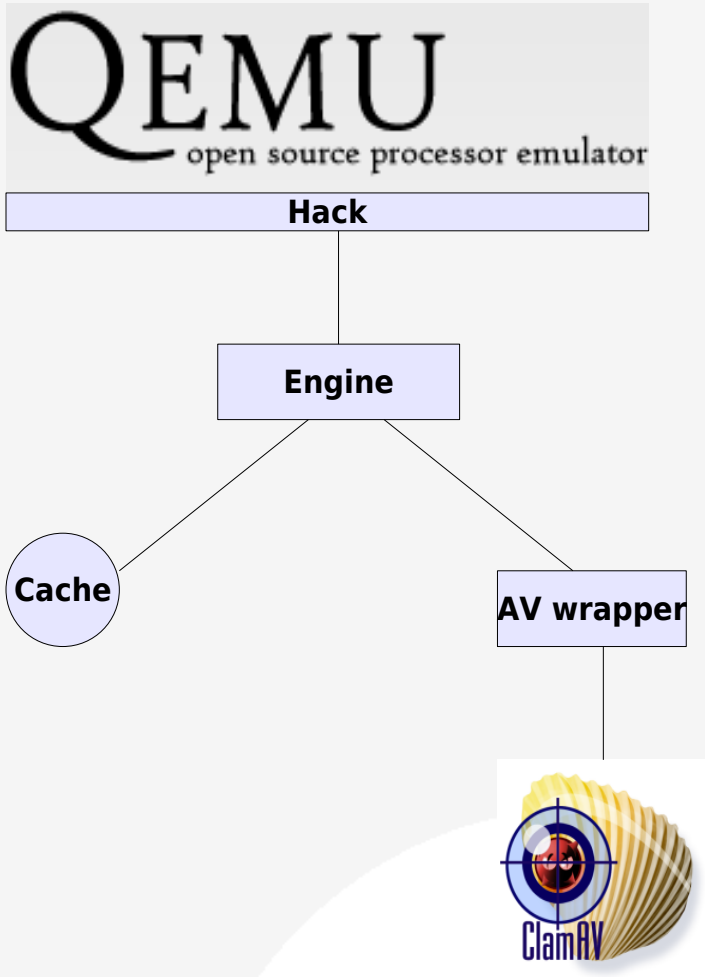
# Problematiche affrontate (2)

- ✓ Algoritmo veloce: flag di modifica dei file / singoli blocchi, “preload” della cache con strutture dati ricorrenti (file di avvio), scansione di file significativi per estensione (no metadata) o sorgente (dispositivi)

- ✓ Cache efficiente: ricostruzione del contenuto solo quando necessario (reverse engineering dell’NTFS)
- ✓ Antivirus efficiente in termini di memoria e affidabilità

# Implementazione: accenni

- ✓ Hack alla macchina virtuale QEMU 0.8.2
- ✓ Engine dell'agente
- ✓ File cache
- ✓ AV wrapper via libclamAV
- ✓ ClamAV 1.13.1



# Algoritmo on-access: lettura e scrittura

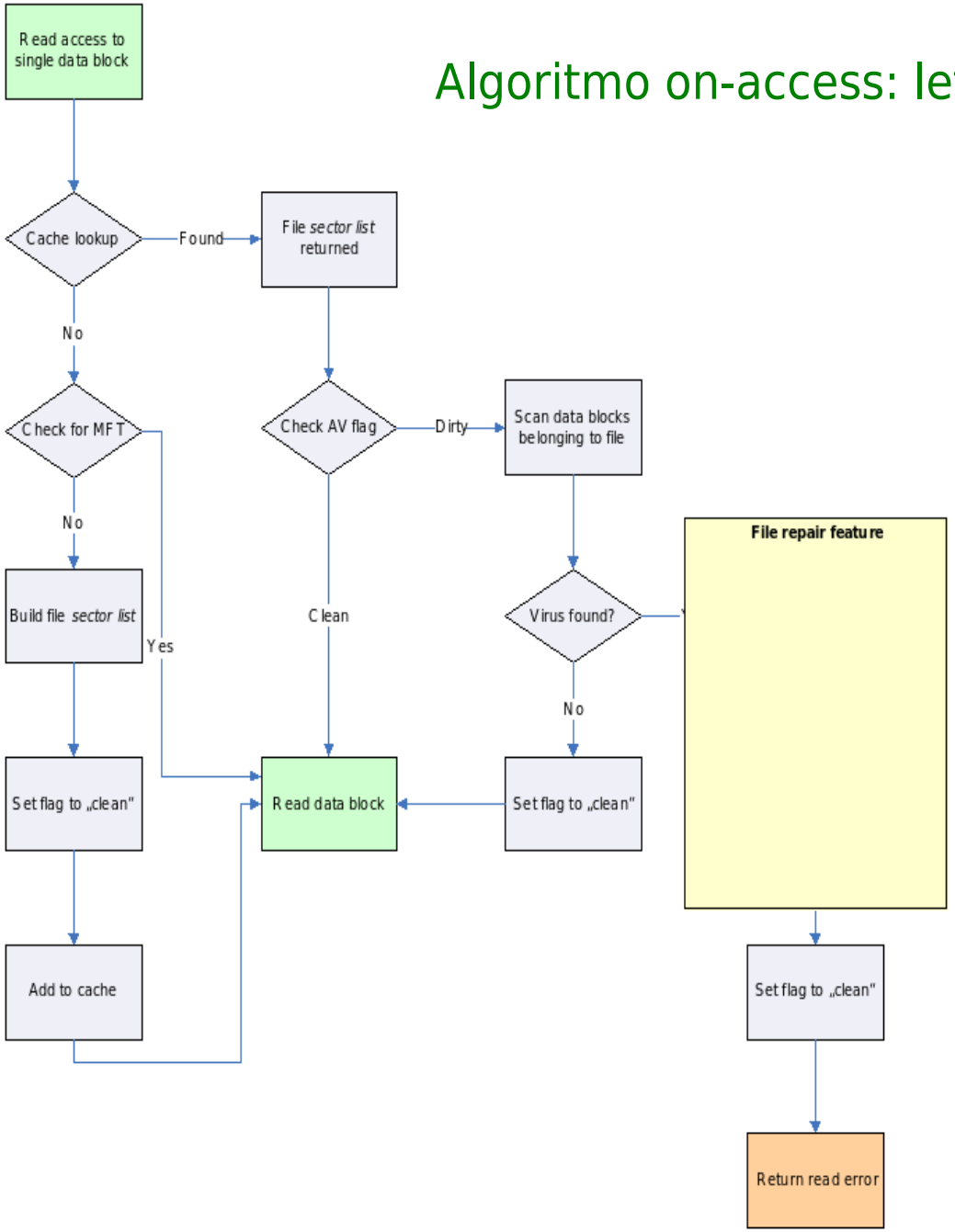



Figure 11 - On-access scan - read algorithm

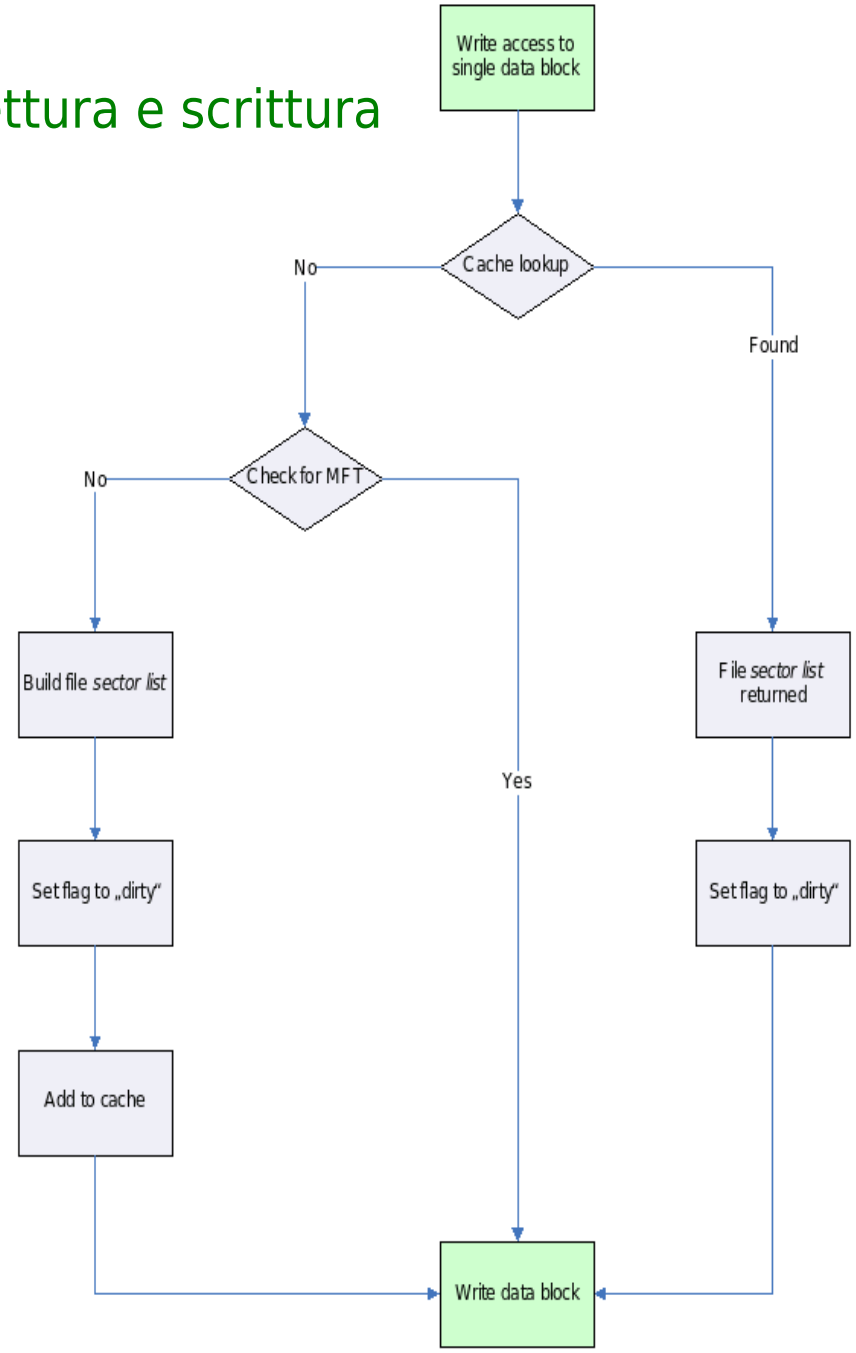
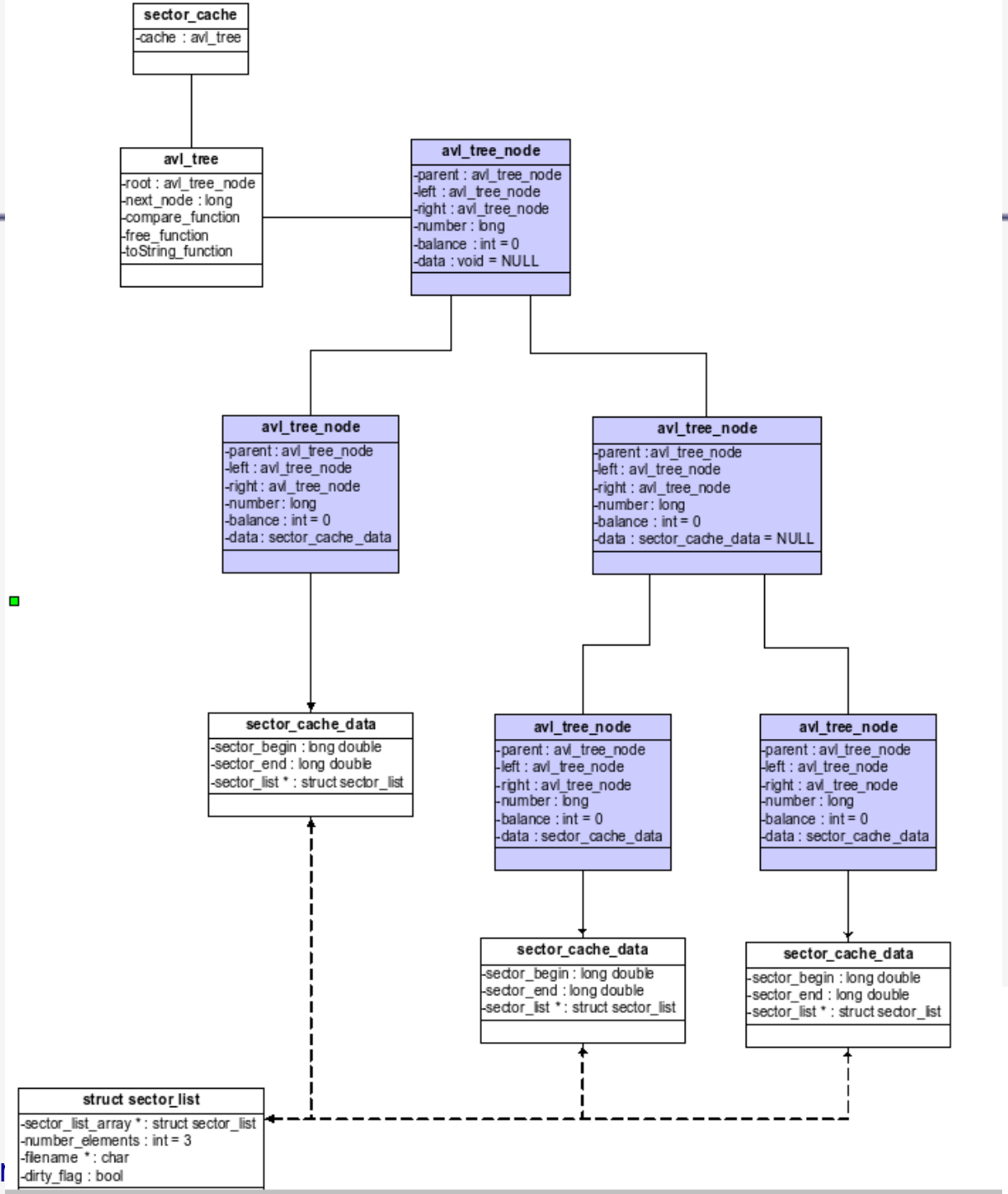
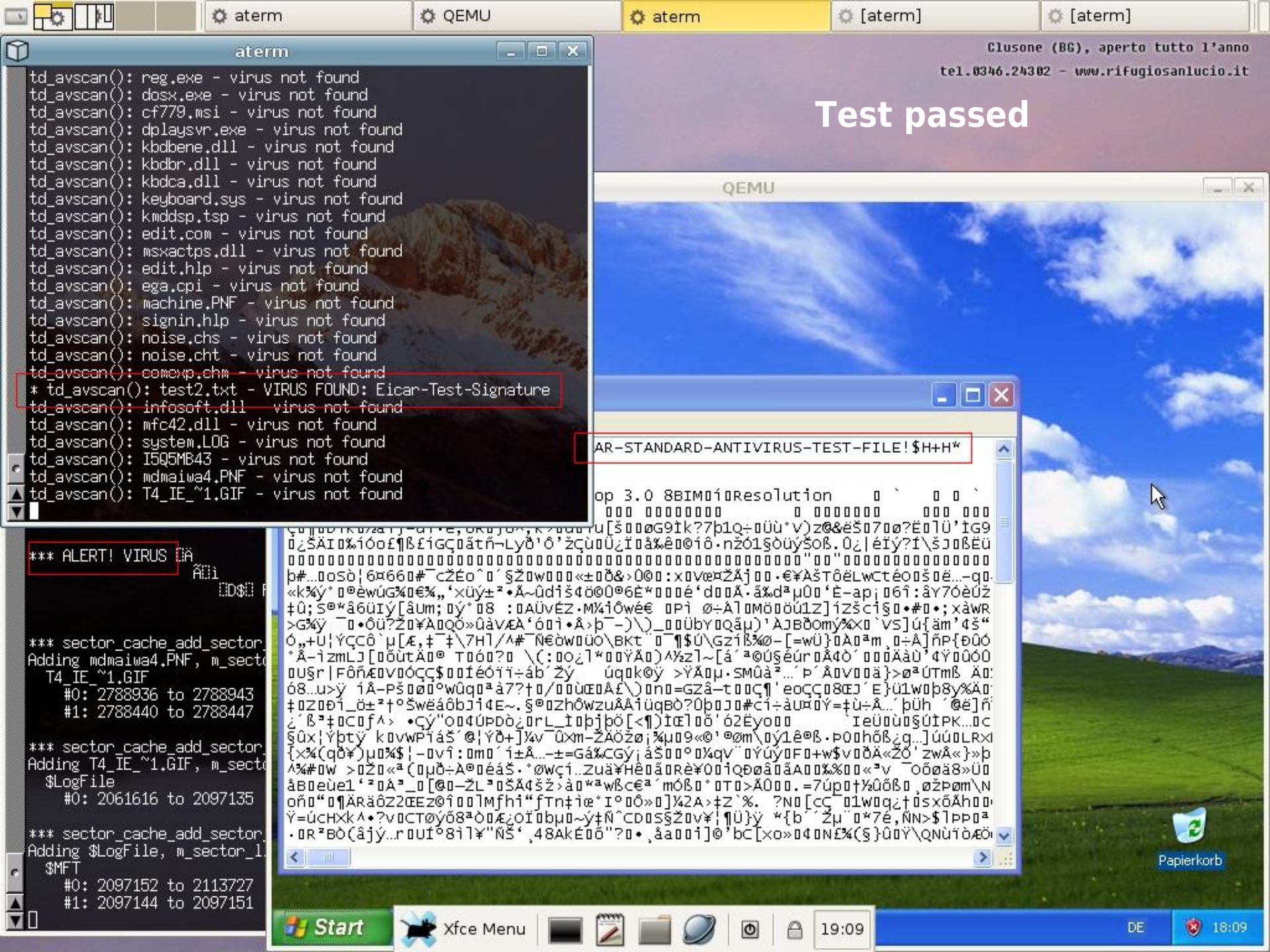



Figure 12 - On-access scan - write algorithm

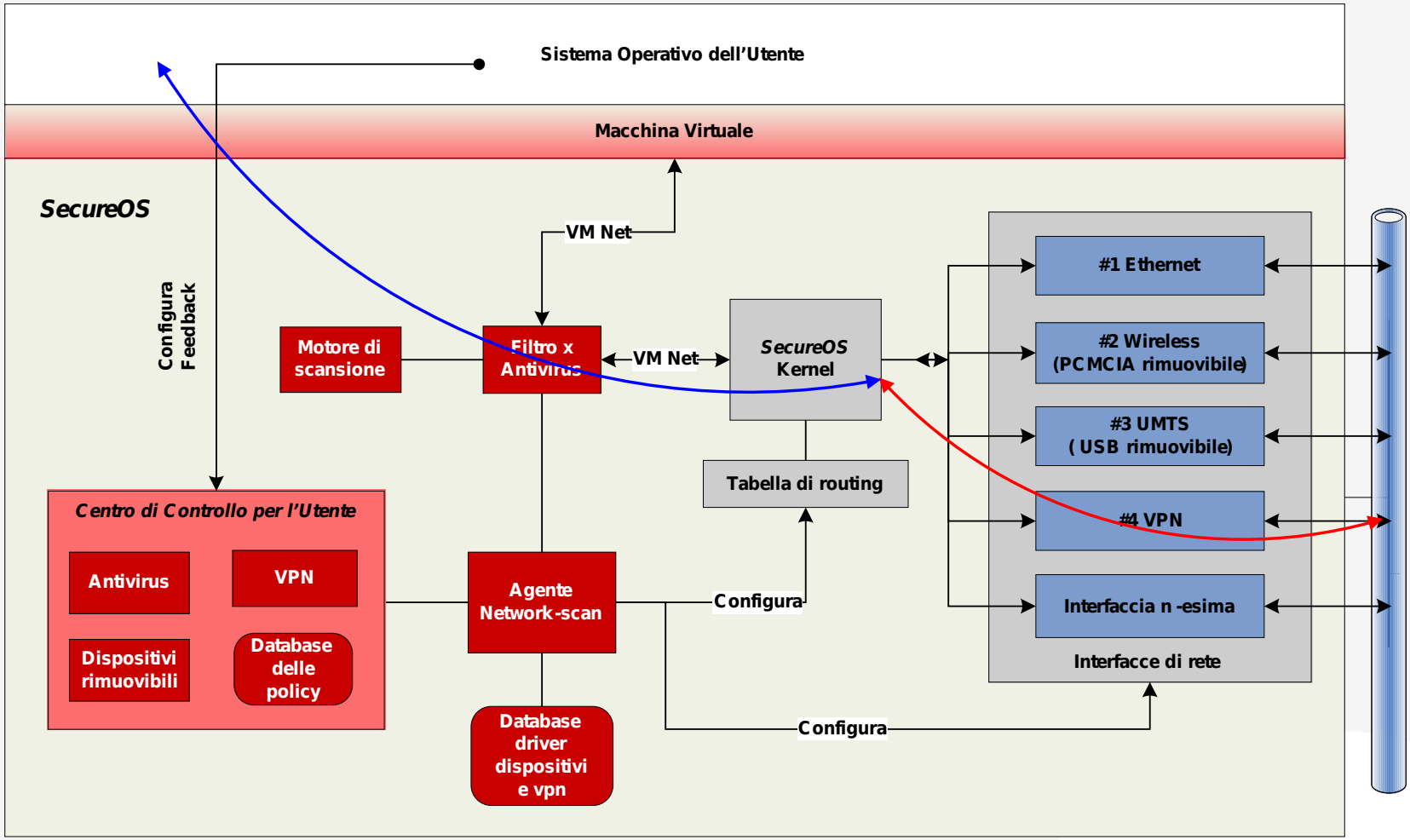
metro olografix

# Schema architetturale della cache




aterm
QEMU
aterm
[aterm]
[aterm]
Clusone (BG), aperto tutto l'anno
tel.0346.24302 - www.rifugiosanlucio.it
Test passed
td_avscan(): reg.exe - virus not found
td_avscan(): dosx.exe - virus not found
td_avscan(): cf779.msi - virus not found
td_avscan(): dplaysvr.exe - virus not found
td_avscan(): kbdbene.dll - virus not found
td_avscan(): kbdbr.dll - virus not found
td_avscan(): kbdca.dll - virus not found
td_avscan(): keyboard.sys - virus not found
td_avscan(): kmddsp.tsp - virus not found
td_avscan(): edit.com - virus not found
td_avscan(): msxactps.dll - virus not found
td_avscan(): edit.hlp - virus not found
td_avscan(): ega.cpi - virus not found
td_avscan(): machine.PNF - virus not found
td_avscan(): signin.hlp - virus not found
td_avscan(): noise.chs - virus not found
td_avscan(): noise.cht - virus not found
td_avscan(): comexp.chm - virus not found
* td_avscan(): test2.txt - VIRUS FOUND: Eicar-Test-Signature
td_avscan(): infosoft.dll - virus not found
td_avscan(): mfc42.dll - virus not found
td_avscan(): system.LOG - virus not found
td_avscan(): I5Q5MB43 - virus not found
td_avscan(): mdmaiwa4.PNF - virus not found
td_avscan(): T4_IE_~1.GIF - virus not found
*** ALERT! VIRUS
*** sector_cache_add_sector
Adding mdmaiwa4.PNF, m_sect
T4_IE_~1.GIF
#0: 2788936 to 2788943
#1: 2788440 to 2788447
*** sector_cache_add_sector
Adding T4_IE_~1.GIF, m_sect
$LogFile
#0: 2061616 to 2097135
*** sector_cache_add_sector
Adding $LogFile, m_sector_l
$MFT
#0: 2097152 to 2113727
#1: 2097144 to 2097151
QEMU
AR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
Papierkorb
Start
Xfce Menu
19:09
DE
18:09

# *Network scan:* protezione di rete



# *Image scan*

- ✓ Il Sistema *guest* è un file immagine (ISO) della macchina virtuale
- ✓ In formato semplice corrisponde alla struttura di un normale disco (partizione C: inizia al 63° settore)
- ✓ Accesso al contenuto in lettura e scrittura per mezzo del supporto LINUX Fat32 e NTFS-3G
- ✓ Scansione *offline* evita problemi quali
  - inefficienza di scansione (contenuto de-sincronizzato)
  - corruzione file-system dovuta a scrittura fisica

# *Controllo dei dispositivi rimuovili*

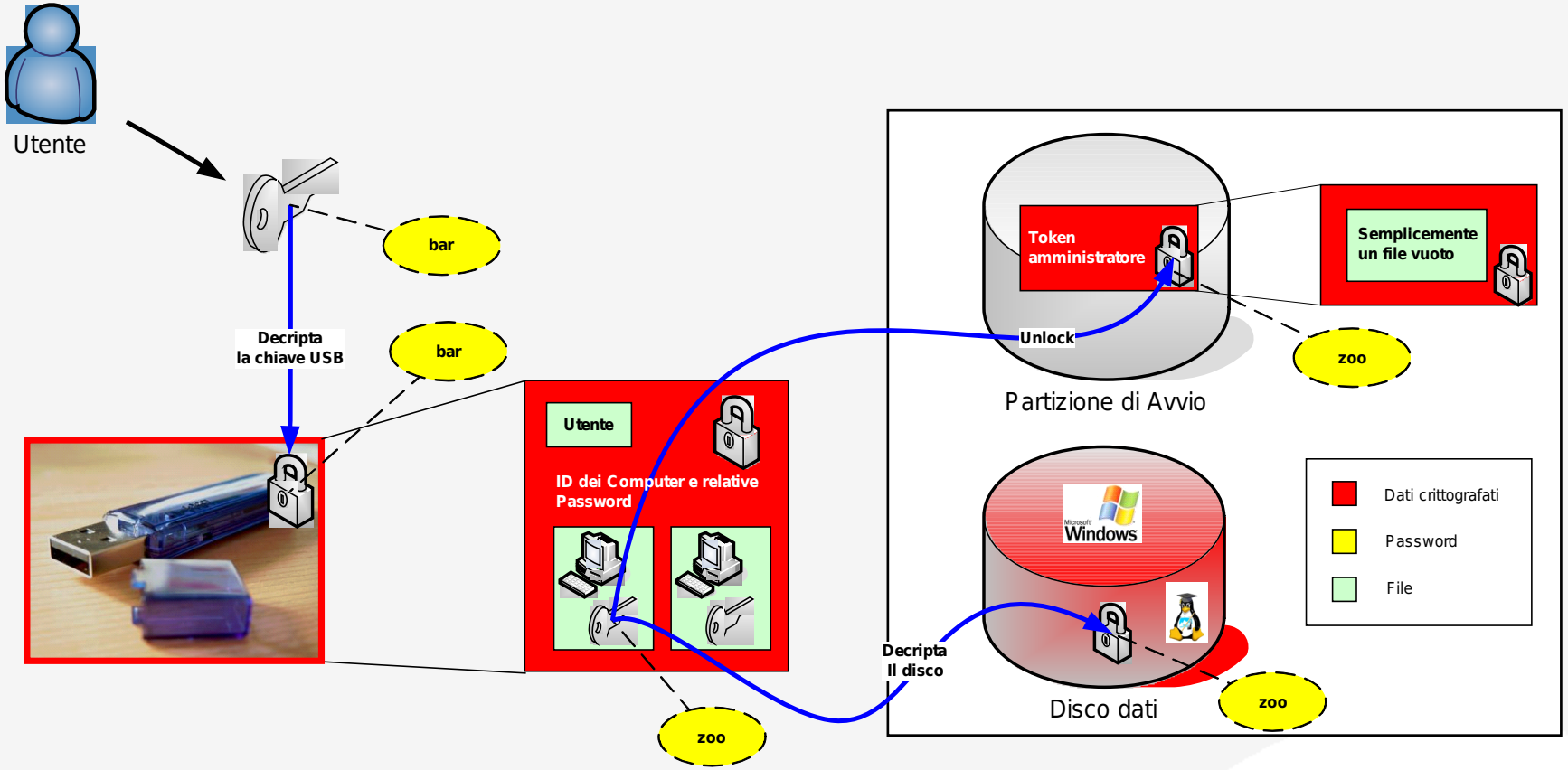
- ✓ Furto di informazioni
- ✓ Installazione software non autorizzato / pericolo (e via Windows *autostart*)

- ✓ Filtro sui dispositivi offerti al sistema utente
  - ACL vendor/categoria/tipologia
  - Controllo attraverso policy XML
- ✓ Crittografia trasparente e single-sign-on dei dispositivi di massa

# *Disk encryption* (1)

- ✓ Impedire il furto di informazioni in caso di furti e smarrimenti (confidenzialità)
- ✓ Protezione globale: “secureOS” e Sistemi Utente
- ✓ Crittografia trasparente al Sistema Utente
- ✓ Crittografia forte: AES128 in modalità CBC-ESSIV
- ✓ Autenticazione pre-boot: password e token hardware
- ✓ Single-sign-on
- ✓ Gestione centralizzata delle credenziali (recupero facile)

# Disk encryption (2)



# Conclusioni

- ✓ Virtualizzazione quale approccio innovativo alla gestione della sicurezza informatica
- ✓ Un nuovo modello di antivirus garantisce una più efficiente e affidabile protezione contro le crescenti minacce di virus e malware
- ✓ Sviluppo di nuove efficaci meccanismi di protezione
- ✓ Evidenti vantaggi per le convenzionali soluzioni di sicurezza

# Riferimenti

- ✓ Sei interessato a collaborare? a essere partner?
- ✓ Proposte, suggerimenti, critiche, test sono ben accettati...
- ✓ Contatti email
  - Marco “embyte” Balduzzi <embyte@madlab.it>
  - Matthias Besch <besch@web.de>