



Virtualizzazione & sicurezza ICT

11 novembre 2010

La virtualizzazione ed i suoi aspetti di sicurezza

Sergio Sagliocco
Responsabile SecureLAB – Direzione R&D
CSP

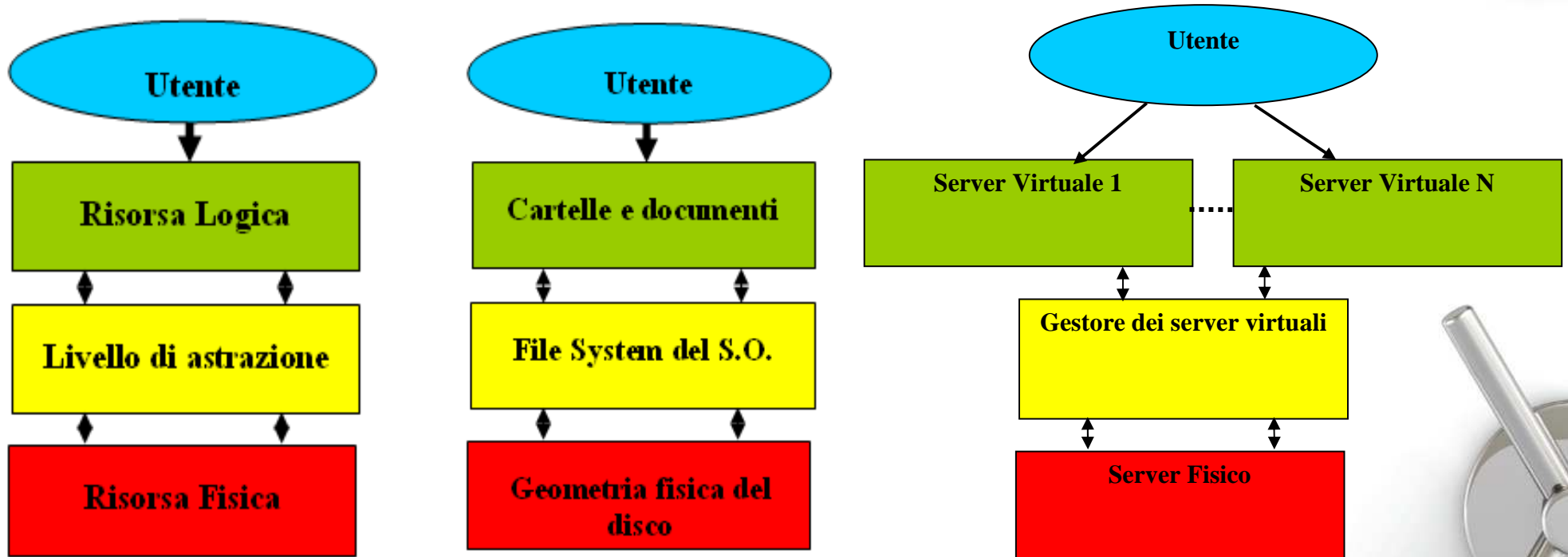
Presentazione della Monografia

- CAP 1: La virtualizzazione: concetti di base
- CAP 2: La virtualizzazione mediante partizionamento
- CAP 3: Prodotti per la virtualizzazione
- CSP 4: Aspetti per il dimensionamento di una struttura
- CAP 5: La sicurezza negli ambienti virtualizzati
- CAP 6: Nuovi orizzonti per la virtualizzazione



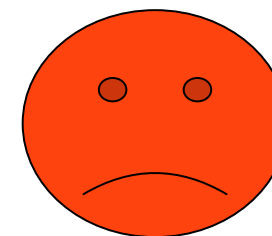
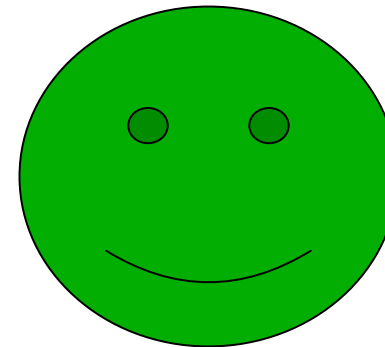
La virtualizzazione – Concetti di base – Che cosa è?

In generale si può definire virtualizzazione qualunque processo in grado di astrarre i dettagli fisici di una risorsa reale al fine di permettere ai suoi utenti un accesso più semplice, efficiente o sicuro.

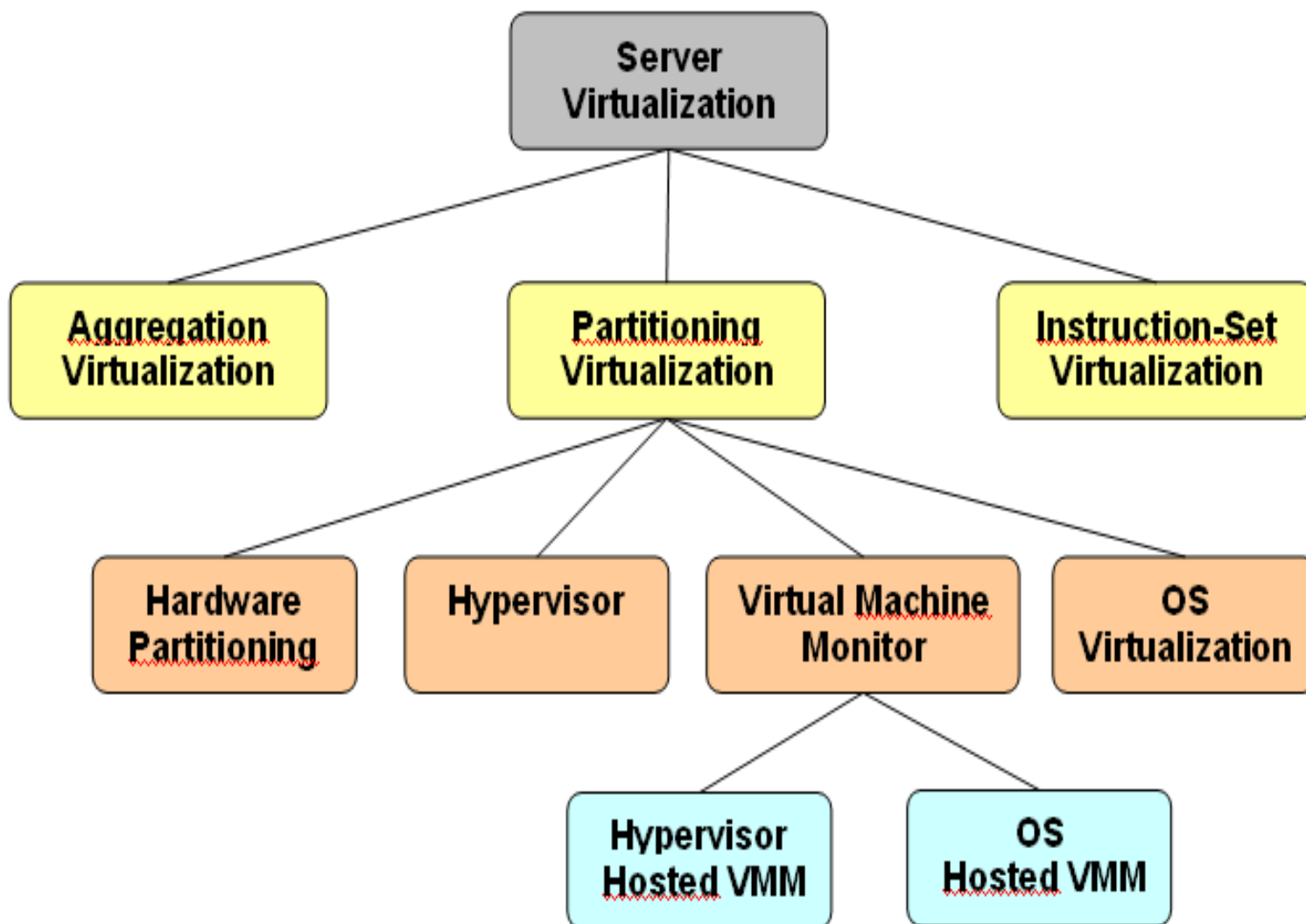


La virtualizzazione – Concetti di base – I vantaggi/svantaggi

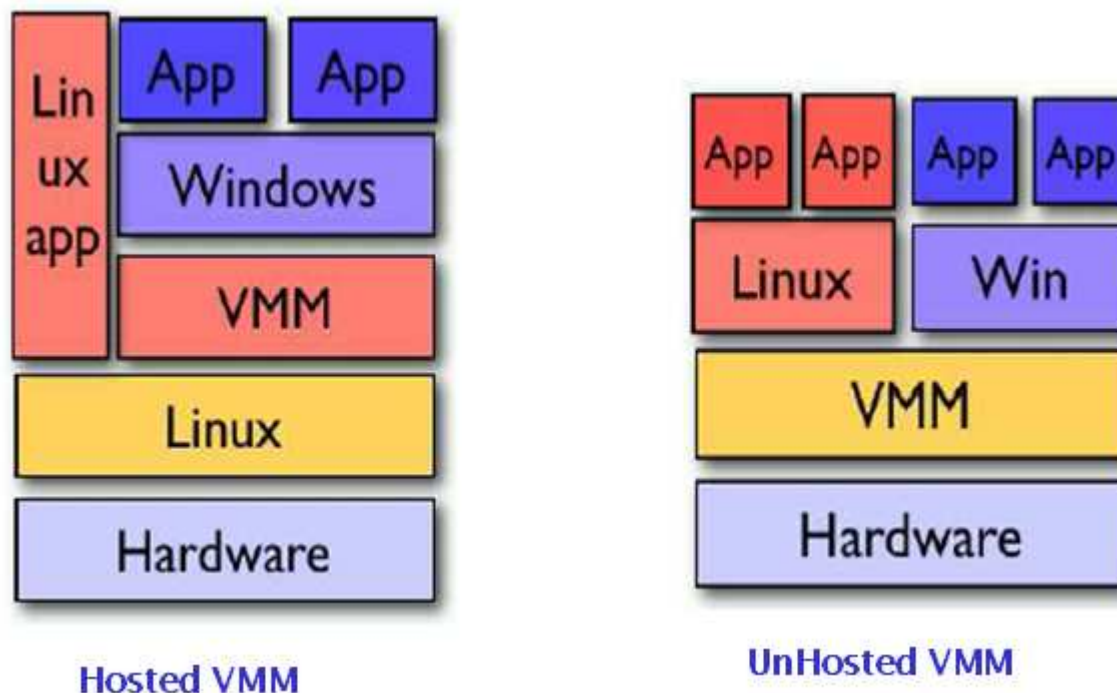
- Riduzione dei server fisici
- Consolidamento dei server
- Indipendenza hardware
- Adattabilità
- Supporto applicazioni legacy
- Standardizzazione delle installazioni
- Creazione di ambienti di test
- Overhead
- Hardware non virtualizzabile



La virtualizzazione – Concetti di base –Le tecniche



La virtualizzazione tramite partizionamento



La tecnica della **virtualizzazione completa** prevede che il VMM mostri alla macchina virtuale tutto l'hardware necessario all'esecuzione di un sistema operativo tradizionale; il VMM, quindi, tramite un BIOS virtuale, espone la/le CPU, le memorie, i dispositivi di memorizzazione e così via.

I VMM **paravirtualizzati**, a differenza di quelli descritti in precedenza, non emulano l'hardware della macchina fisica, ma definiscono e implementano un'interfaccia applicativa tra VMM e sistema operativo della macchina virtuale (anche nota come Virtual Hardware API).

I prodotti per la virtualizzazione



Aspetti per il dimensionamento di una struttura

- Viene illustrato un esempio di realizzazione di un'infrastruttura di virtualizzazione complessa, relativo ad una farm
- Obiettivi:
 - ridurre complessivamente il numero fisico di server senza cambiare il numero e la tipologia dei servizi erogati
 - ridurre i consumi elettrici e quelli accessori (condizionamento e spazio occupato)
 - aumentare l'affidabilità e la flessibilità di gestione.
- Nella definizione dell'architettura sono stati considerate le seguenti risorse:
 - Networking
 - Storage
 - Server



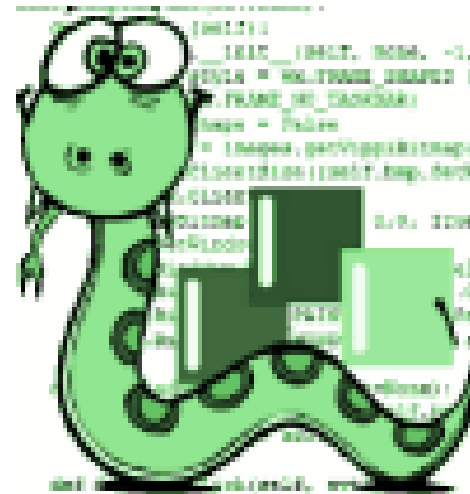
La sicurezza negli ambienti virtualizzati

- Come spesso accade è stata considerata solo quando la tecnologia è ormai matura!
- Ci si deve concentrare sul livello “fisico”
 - i dischi non sono dei dischi!
 - gli switch non sono degli switch!
- È necessario quindi che un ambiente di virtualizzazione si prenda in carico di compensare la perdita di sicurezza conseguente alla perdita di “fisicità” degli oggetti coinvolti

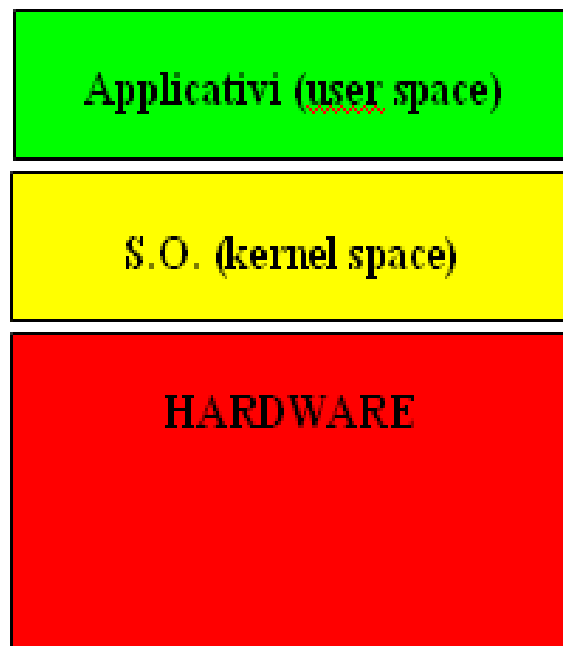


La sicurezza negli ambienti virtualizzati – Le minacce

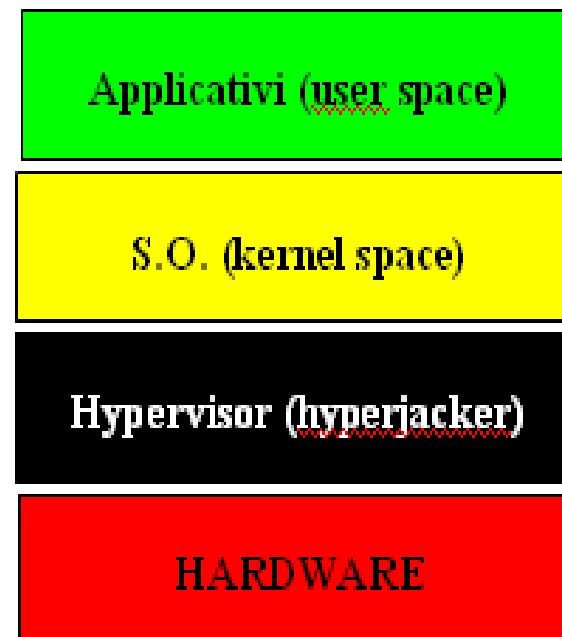
- virus basati sulla virtualizzazione
- rilevamento di un sistema virtualizzato
- riallocazione dinamica delle immagini virtuali (live migration)
- isolamento delle macchine virtuali e denial-of-service
- integrità delle macchine virtuali
- isolamento del traffico di rete.



La sicurezza negli ambienti virtualizzati – HVM Rootkits



Sistema pulito



Sistema infetto

La sicurezza negli ambienti virtualizzati – Detection

Due aspetti contrastanti fra di loro:

- E' utile per l'utente rilevare se un ambiente è virtualizzato in quanto potrebbe essere utile all'identificazione di HVM rootkits
- E' utile ai VIRUS (tradizionali) per non essere dannosi all'interno di un ambiente virtualizzato!
- Tecniche di rilevazione:
 - Ricerca di artefatti specifici dell'hypervisor
 - Analisi dei tempi di esecuzione di determinate istruzioni
 - Utilizzo di hardware embedded
 - Analisi remota dello stack di rete



La sicurezza negli ambienti virtualizzati – Live migration

- Possibilità da parte del VMM di trasferire l'esecuzione di una macchina virtuale da un server fisico ad un altro
- Potenzialmente molto rischioso: *man in the middle*
- Alcuni ricercatori dell'Università del Michigan hanno dimostrato come sia possibile compromettere la sicurezza di un sistema mentre questo viene migrato da un VMM all'altro.
- Tramite il tool che hanno sviluppato (xensplit) è stato possibile modificare il codice di un eseguibile per modificarne il suo output
- Inoltre è stato possibile modificare il codice del demone SSH (sshd) per consentire l'accesso di root senza alcuna autorizzazione.



La sicurezza negli ambienti virtualizzati – VM Escape & DoS

- Uno dei principi fondamentali dei sistemi virtualizzati è l'isolamento (VM isolation): questo vuol dire che teoricamente non deve essere possibile far comunicare le macchine virtuali tra di loro oppure una macchina virtuale con l'host.

- Eccezioni:

- condividere gli appunti tra host e macchine virtuali;
- condividere cartelle del file system fisico in quello virtuale;
- interconnettere più macchine virtuali tramite una rete virtuale
 - implementando un virtual hub o virtual switch.



La sicurezza negli ambienti virtualizzati – VM Integrity

- I VMM memorizzano le immagini dei dischi sul file system dell'host in quanto sono molto più facili da gestire rispetto all'uso di partizioni dedicate sui dischi fisici dell'host.
- Risulta quindi chiaro come sia importante gestire l'integrità o, ancora meglio, la cifratura dei dischi virtuali da fattori esterni.
- Tre diversi approcci:
 - Cifratura gestita dal VMM
 - Cifratura gestita dal sistema guest
 - Cifratura gestita dal sistema host



Nuovi orizzonti per la virtualizzazione

- E' stato preso in considerazione un nuovo paradigma basato sulla virtualizzazione e su una tecnologia emergente chiamata Trusted Computing.
- Esso è volto ad incrementare la sicurezza di esecuzione di applicazioni e servizi critici
- Tale approccio è ancora prevalentemente confinato nell'ambito della ricerca e della sperimentazione e tende a modificare il rapporto tra virtualizzazione e sicurezza.
- I VMM si avviano a diventare essi stessi strumenti per incrementare la sicurezza dei sistemi.





Virtualizzazione & sicurezza ICT

11 novembre 2010

La virtualizzazione ed i suoi aspetti di sicurezza

Sergio Sagliocco
Responsabile SecureLAB – Direzione R&D
CSP