Sicurezza nei modelli peer-to-peer

F.Baiardi
Dipartimento di Informatica, Centro Serra
Università di Pisa
f.baiardi@unipi.it

Credits

- Stefano Suin (unipi serra)
- Claudio Telmon
- Laura Ricci (di unipi)
- Paolo Mori (iit cnr)
- Gli studenti del corso Sicurezza delle reti

Peer-to-peer

- condivisione
  - A livello di risorse logiche
  - A livello di risorse fisiche

  nel range da file exchange al grid computing, la condivisione è comunque presente
- autonomia
  - dei singoli nodi
  - sull'unirsi o lasciare una rete p2p

Sicurezza peer-to-peer

- Due prospettive
  - Chi fornisce la risorsa condivisa
  - Chi accede la risorsa condivisa
- Entrambe importanti per poter definire un modello di business
- Per ora risolte mediante autenticazione ed in base alla fiducia tra gli utenti
- é realistico se la fiducia dipende non dalla persona ma da come la persona (o chi per la persona) gestisce un sistema????

Asimmetria fondamentale p2p

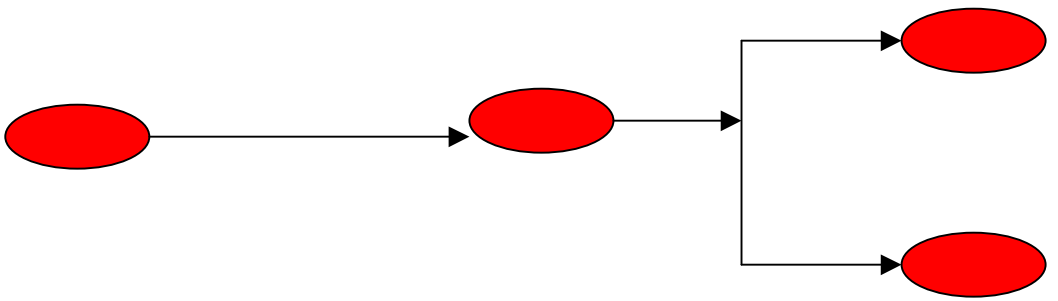
- A (utilizzatore) esegue
  - un programma P
  - con dati D

  sulle risorse fornite da B (fornitore)
- B può evitare side effects inattesi monitorando D e P
- A ha pochi mezzi per difendersi da B anche la crittografia non è adeguata poiché se si usano risorse di calcolo D e P ad un certo istante saranno in chiaro

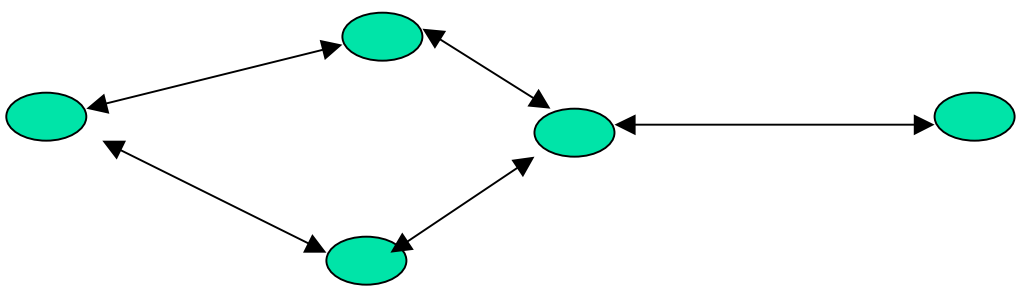
Sicurezza del fornitore

- Può essere migliorata mediante una generalizzazione il concetto di overlay che è alla base del p2p
- Passare dal concetto di overlay della topologia di interconnessione a quello di overlay completo tra reti

Overlay della topologia



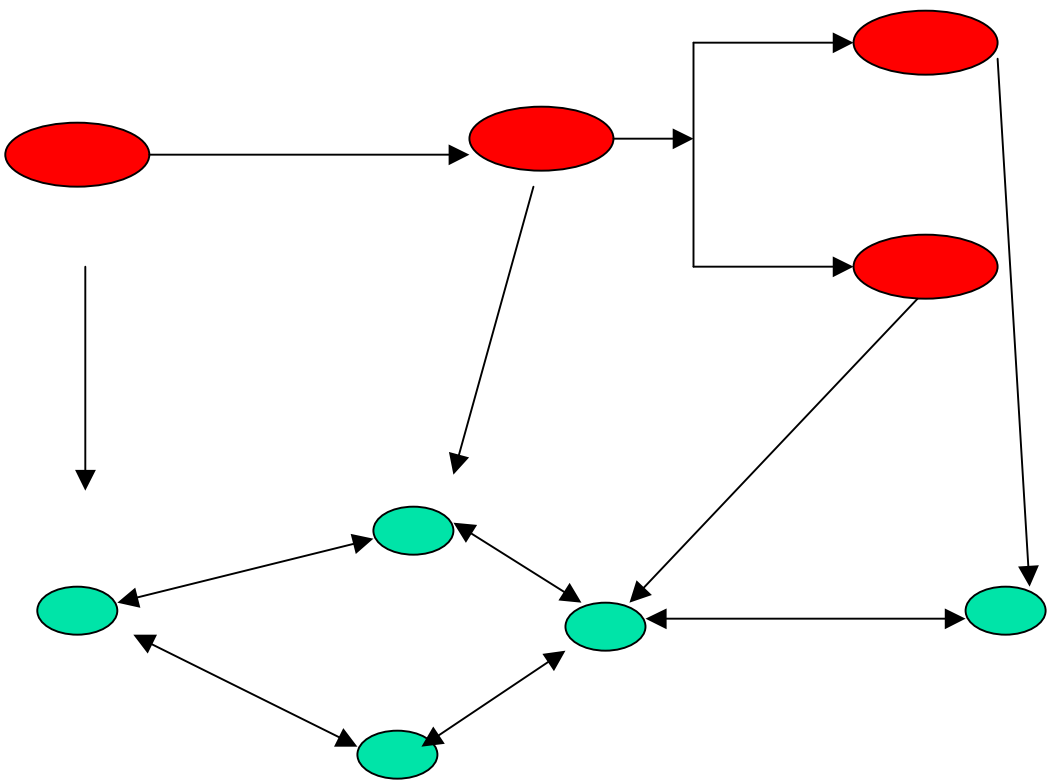
da mappare su



Nuova topologia

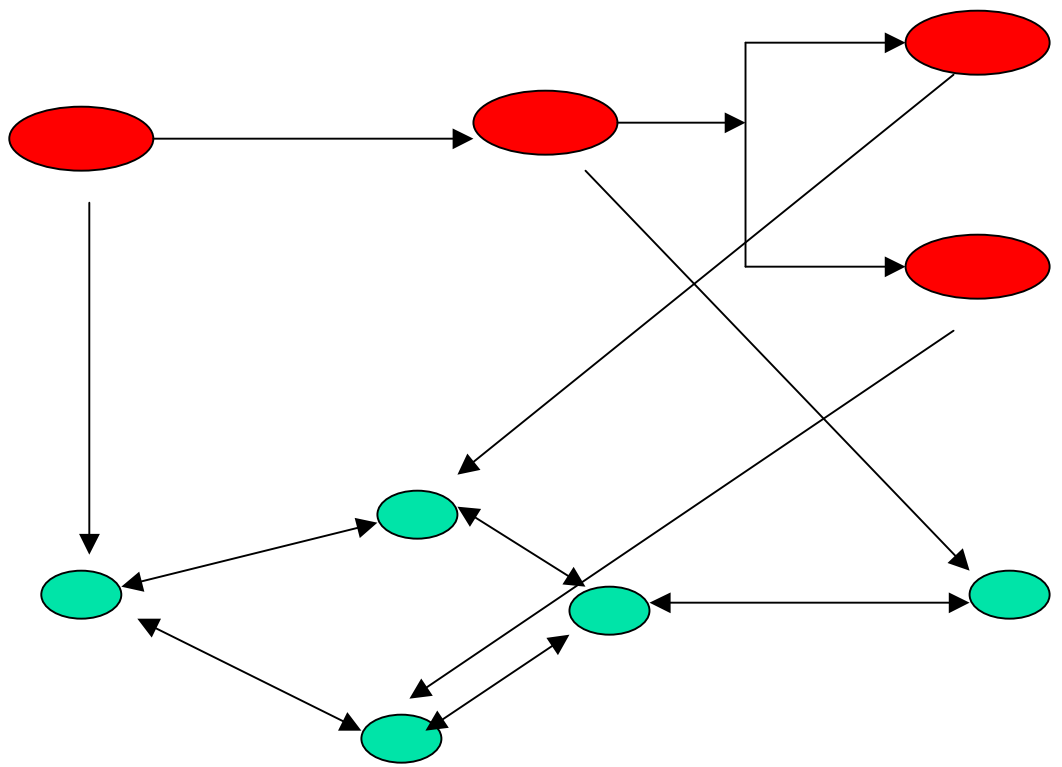
- Nuovo spazio dei nomi
  - Strutturato
  - Piatto
- Nuove regole di indirizzamento
- Nuove regole di instradamento
- Nuove bande di comunicazione
- Nuove regole di filtraggio

Overlay della topologia



Overlay efficiente

Overlay della topologia



Overlay inefficiente

Overlay ed efficienza

- È comunque possibile
  - individuare i punti di inefficienza
  - riorganizzare overlay
- Vantaggi
  - è spesso più semplice misurare l'utilizzo della nuova topologia che della rete fisica
  - si possono definire attributi di sicurezza della nuova topologia (overlay= vpn)

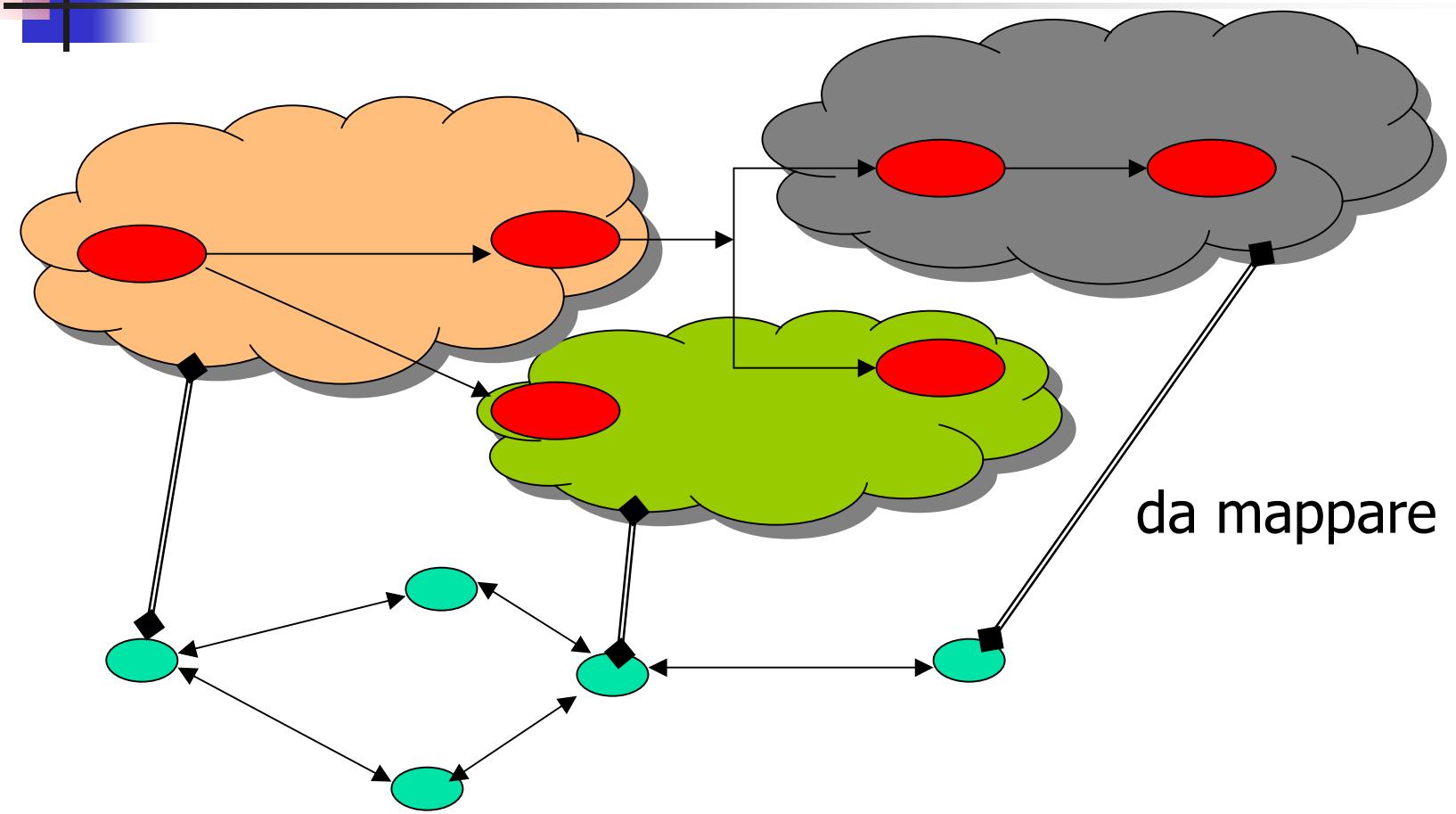
Overlay Completo

- Le tecnologie di virtualizzazione permettono definire reti virtuali complete date da
  - nodi virtuali
  - connessioni virtuali = overlay della topologia
- Un applicazione definisce ed utilizza una propria rete (overlay completo) che viene poi allocata sui componenti di un sistema reale

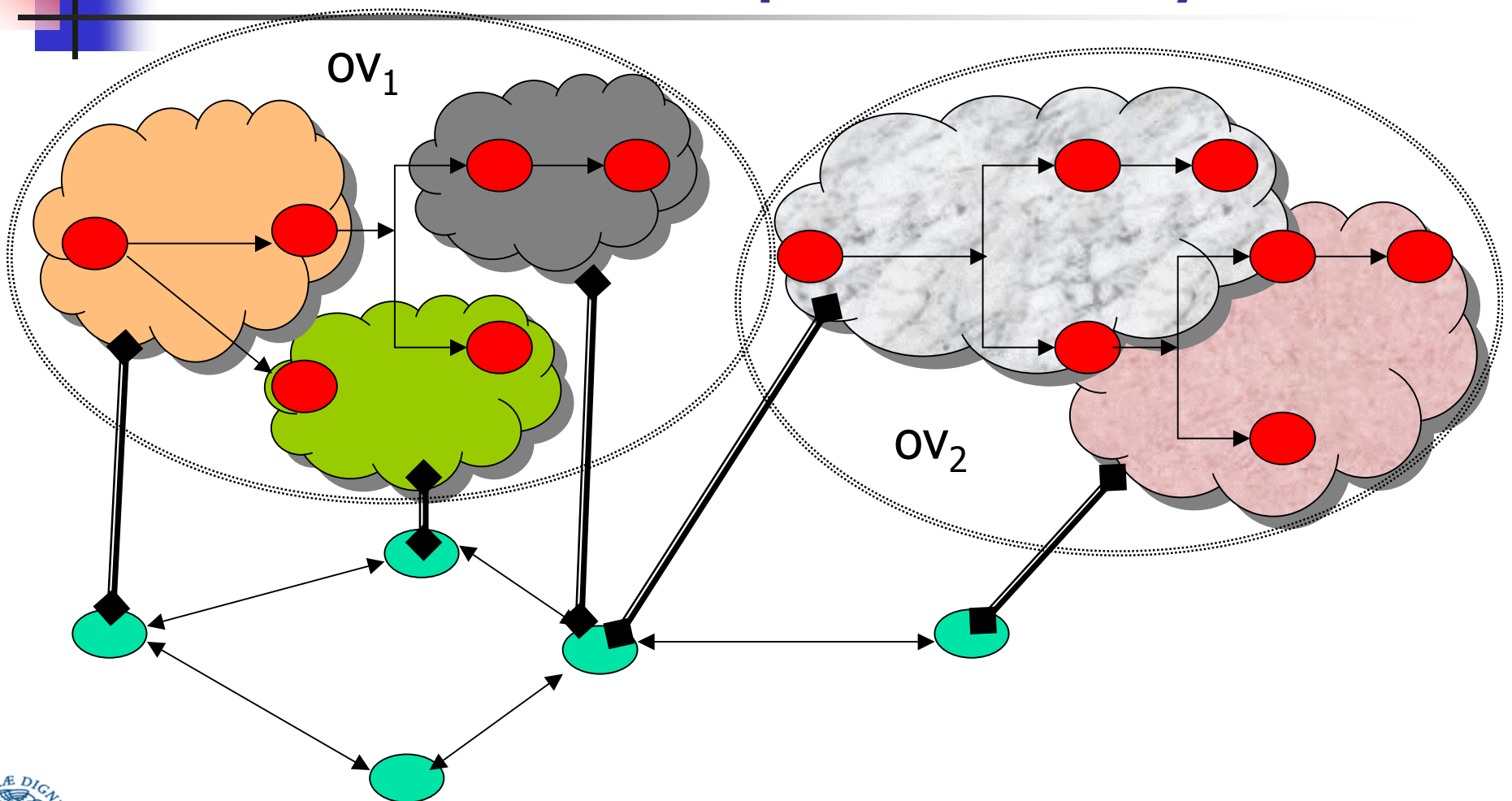
Allocazione di overlay

- In modo statico o dinamico sfruttando adeguatamente i meccanismi di migrazione delle macchine virtuali
- Permette di superare eventuali disomogeneità delle risorse
- Aumenta sicuramente l'efficienza nell'uso delle risorse

Allocazione di overlay



Allocazione di più overlay



Allocazione di overlay

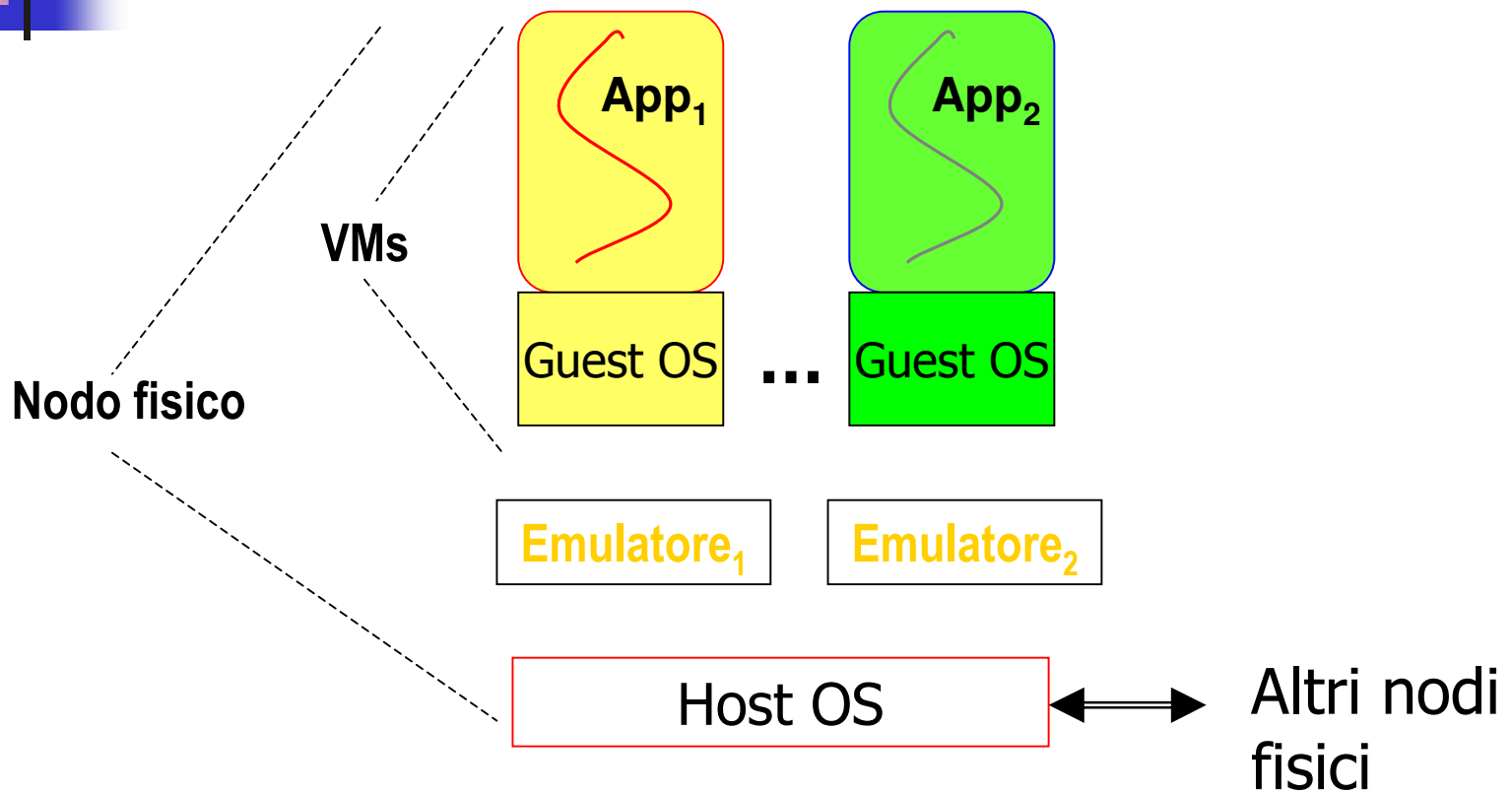
- In generale le risorse virtuali sono mappate quelle fisiche mediante uno schema molti a uno e mai uno a molti
- Lo schema uno a molti è interessante teoricamente ma con l'avvento di chip multi core diventa poco importante perché il problema è come sfruttare la potenza del singolo nodo

Overlay completo: un punto di vista

In un primo punto di vista

- nodo di elaborazione
  - è un sistema tradizionale
  - esegue mediante host os un insieme di applicazioni ognuna delle quali è una macchina virtuale
  - Ogni vm esegue guest os+applicazioni
- overlay della topologia avviene in una delle strategie standard di p2p

Un primo punto di vista



Vantaggi

- Portabilità
- Confinamento
- Gestione più semplice dei diritti in host os
- Scelta del guest os anche in base al livello di fiducia nell'applicazione da eseguire
- Garanzia di quote di risorse condivise è ottenuta sfruttando, se esistono, i meccanismi host os

Vantaggio unico

- È possibile definire condizioni globali sullo stato complessivo del so e della applicazione per scoprire
  - Malfunzionamenti
  - Attacchi
- Proprietà spesso sfruttata per definire honeypot o honeynet

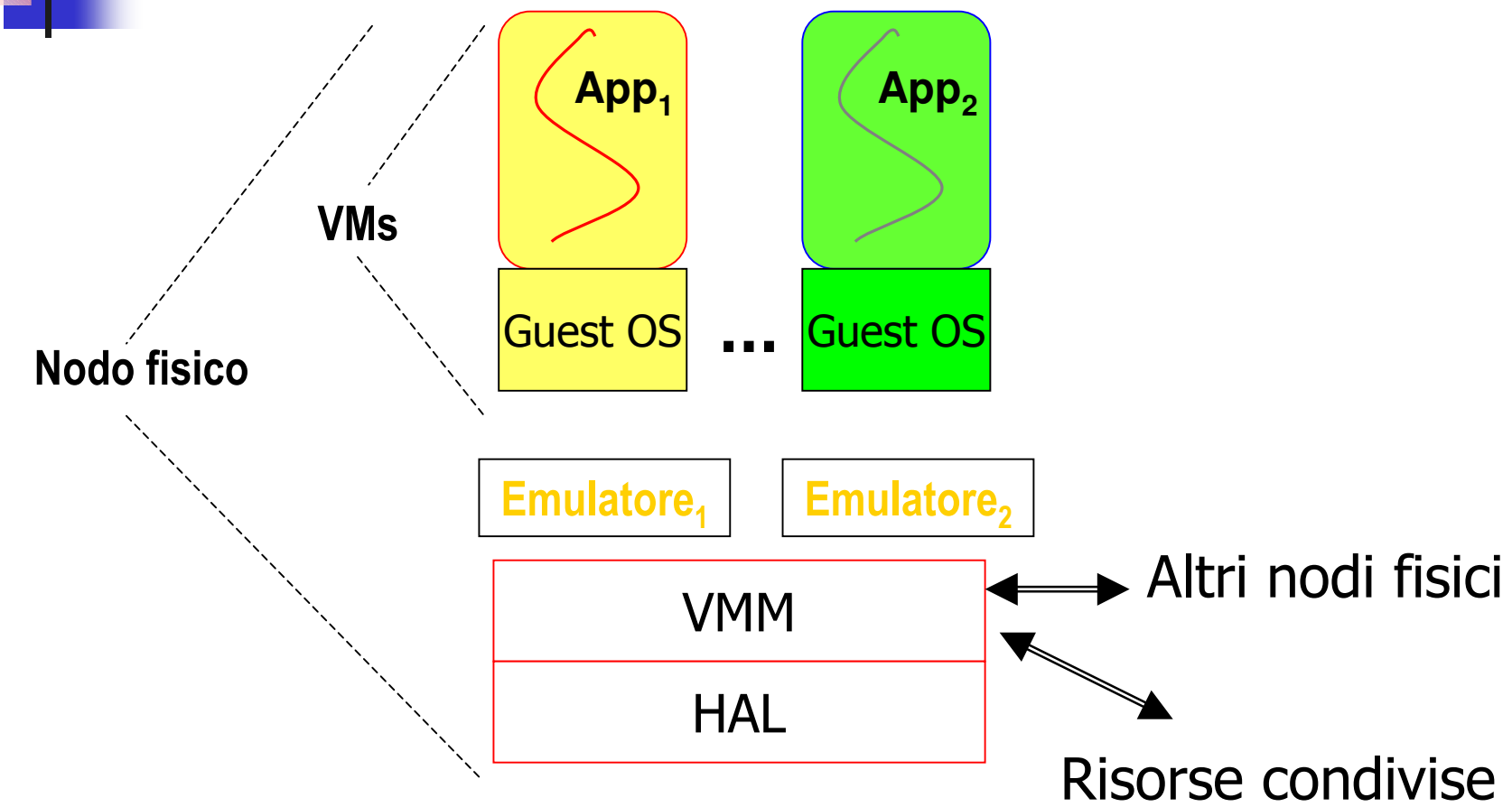
Svantaggio

- Difficile garantire una cooperazione controllata tra overlay diversi
- Il forte confinamento tra overlay diversi è fortemente diminuito se si ammette una cooperazione non controllata tra overlay

Una possibile soluzione - 1

- Il nodo non esegue un full os ma un virtual machine monitor
- Astrazione di componenti per i/o
- Il fornitore definisce una politica di sicurezza per il vmm che definisca
  - Operazioni permesse ai singoli overlay
  - Interazioni permesse tra overlay
  - Gestione delle risorse condivise

Una alternativa



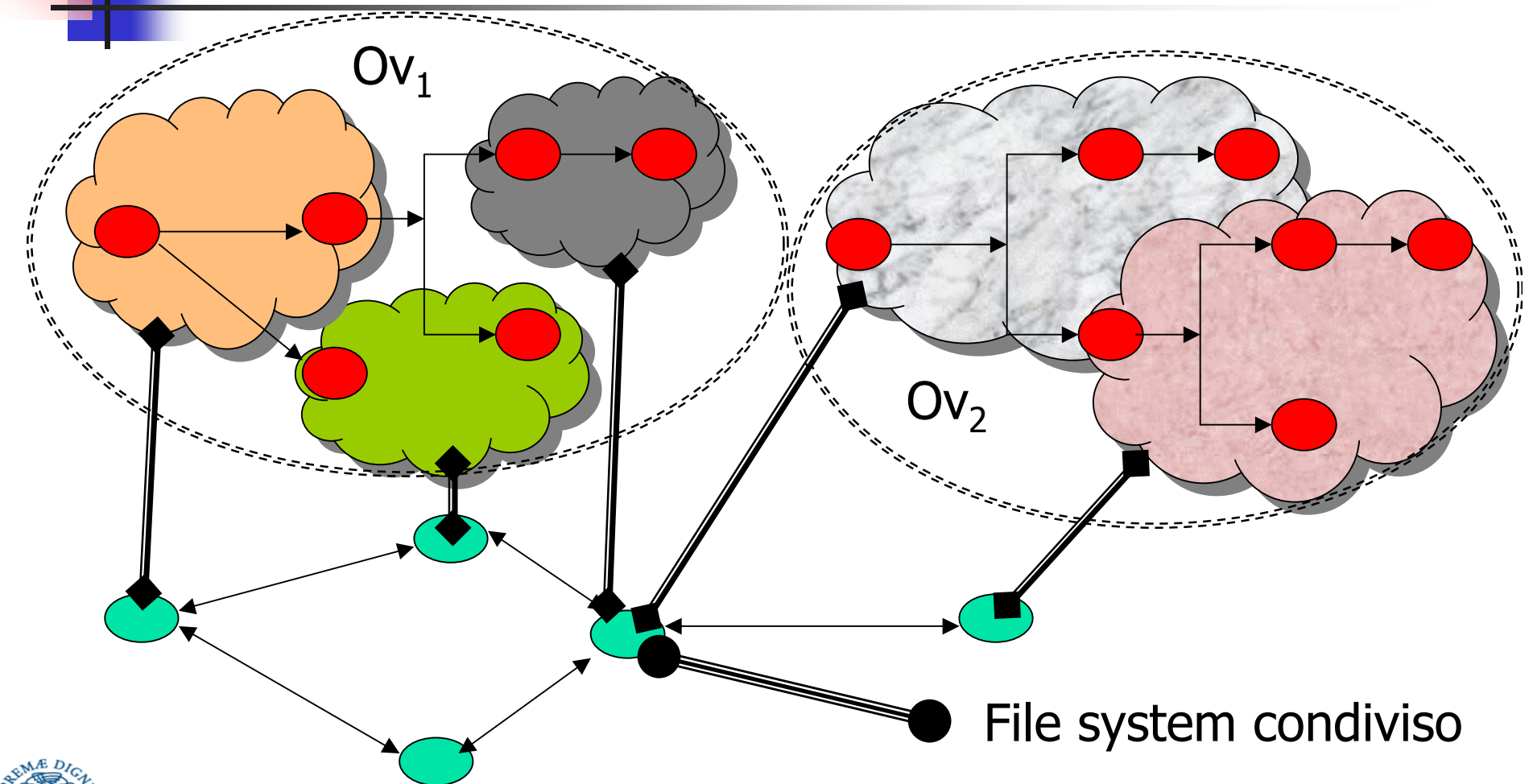
Una possibile alternativa - 2

- Il passaggio da full os a vmm permette
  - L'aumento delle prestazioni
  - La certificazione più semplice delle proprietà vmm
  - L'integrazione dei controlli di guest os e vmm
- Per semplificare la politica di sicurezza i controlli possono essere associati all'overlay e non alle singole applicazioni dell'overlay
- Si conservano i vantaggi di poter misurare semplicemente diversi valori interessanti
- Resta comunque elevata la complessita VMM che incapsula risorse condivise complesse (file etc)

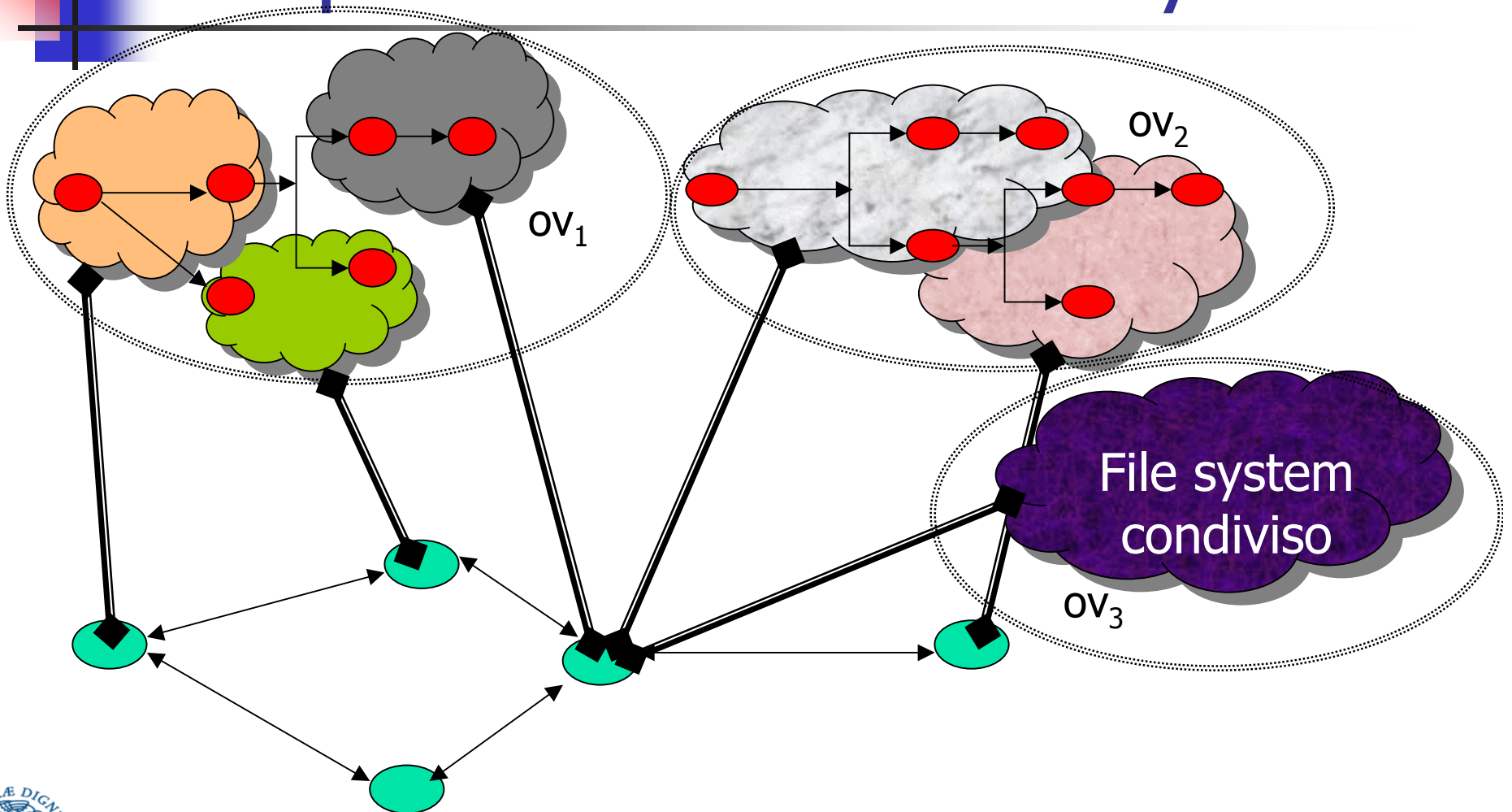
Una possibile alternativa - 3

- La cooperazione tra overlay può sfruttare un ulteriore overlay che implementi la gestione delle risorse condivise
- Controlli del VMM
  - Legalità delle comunicazioni
    - tra overlay
    - Con overlay per risorse condivise
  - Confinamento sulle risorse condivise non gestite dall'ulteriore overlay

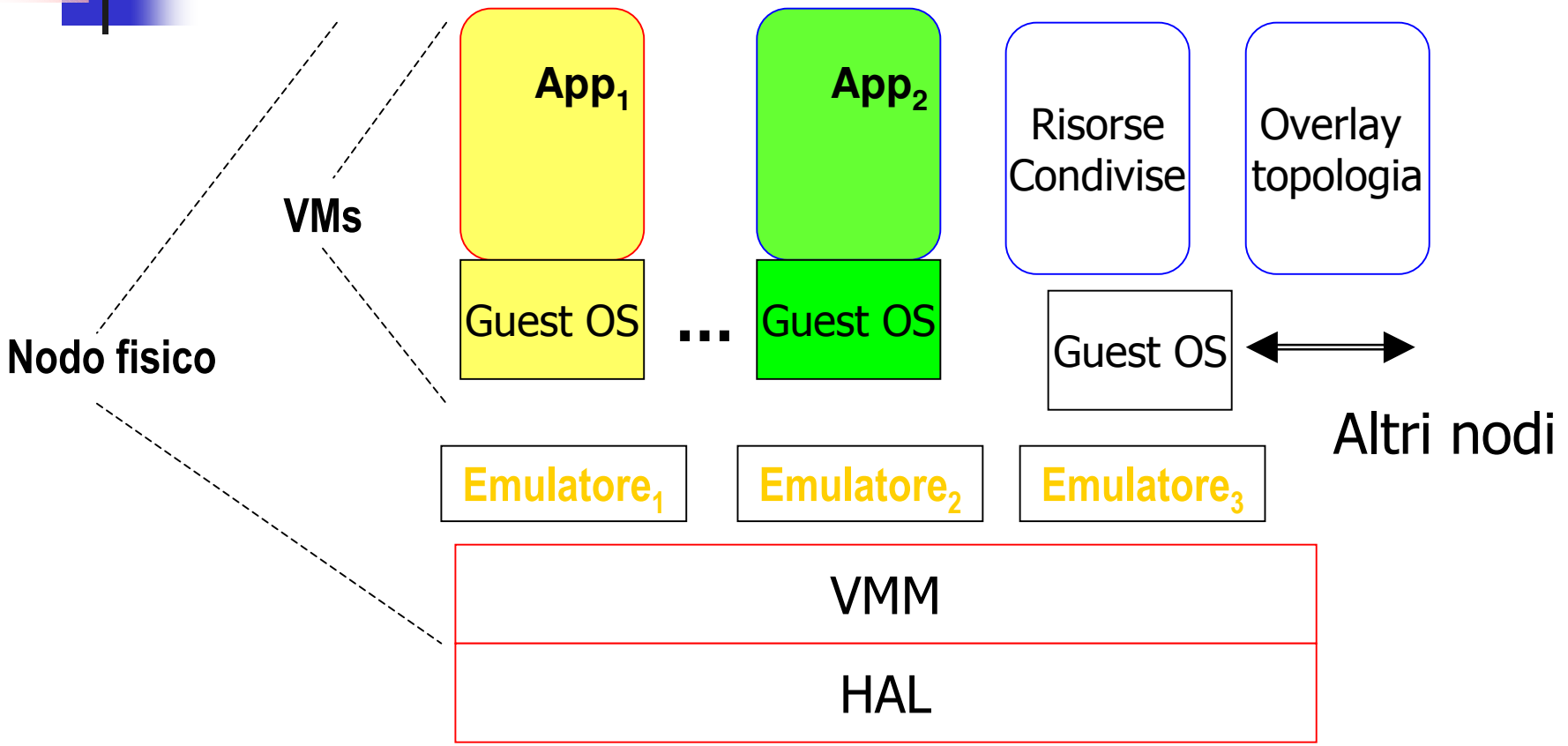
Cooperazione tra overlay



Cooperazione tra overlay



Una alternativa



Cooperazione tra overlay

- Trasmissione delle richieste al nuovo overlay può utilizzare le stesse strategie utilizzate per introdurre un proxy
- Deve comunque rimanere il controllo del VMM sulla interazioni tra overlay

Riassumendo - 1

- Possiamo avere in un overlay più nodi virtuali partizionando tra loro i compiti di
  - Esecuzione applicazione
  - Gestione overlay topologia
  - Gestione risorse condivise
  - Protezione overlay da worm etc.
- Gli overlay possono essere
  - Creati allo start up ed associati a classi di utenti (grid)
  - Creati dinamicamente in base al carico
  - Riallocati (migrare)

Riassumendo - 2

- Possiamo recuperare a livello di nodi virtuali quanto perso in sicurezza nelle interazioni all'interno del nodo
- Stiamo ripercorrendo la strada dei firewall ma all'interno dei nodi
- Forse l'unico modo di sperare in un aumento di sicurezza è la legge di Moore …

E’ una visione realistica???

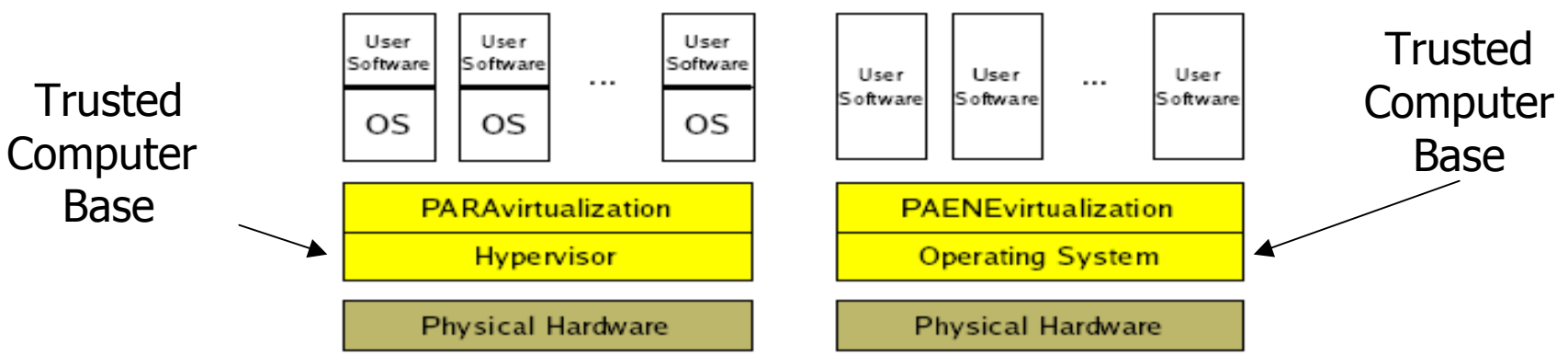
- Numerose tecnologie o prodotti commerciali basati su vm/vmm che hanno come obiettivo il confinamento
  - Vmware
  - Xen
  - User Mode Linux
  - Virtual server
  - Netop
  - …

E' una visione realistica???

- Progetti di ricerca su condivisione controllata
  - Planet Lab Proper
  - Virtuoso
  - Ostia
  - Sharp
- Evoluzione di architetture
  - Intel VT-I, VT-X (ex Vanderpool)
  - Hyperthreading + multicore (adatte per vm)
- Implementazioni alternative di VM
  - Interpretazione pura (con o senza caching)
  - Paravirtualization (Xen)
  - Paenevirtualization

Approcci

- Interpretazione + modifiche dinamiche per problemi x86= VMWare
- Paravirtualization = si espone esistenza di VMM e VM al sistema operativo che può essere modificato (Xen)
- Paenevirtualization = no untrusted os



Hyperthreading + multicore

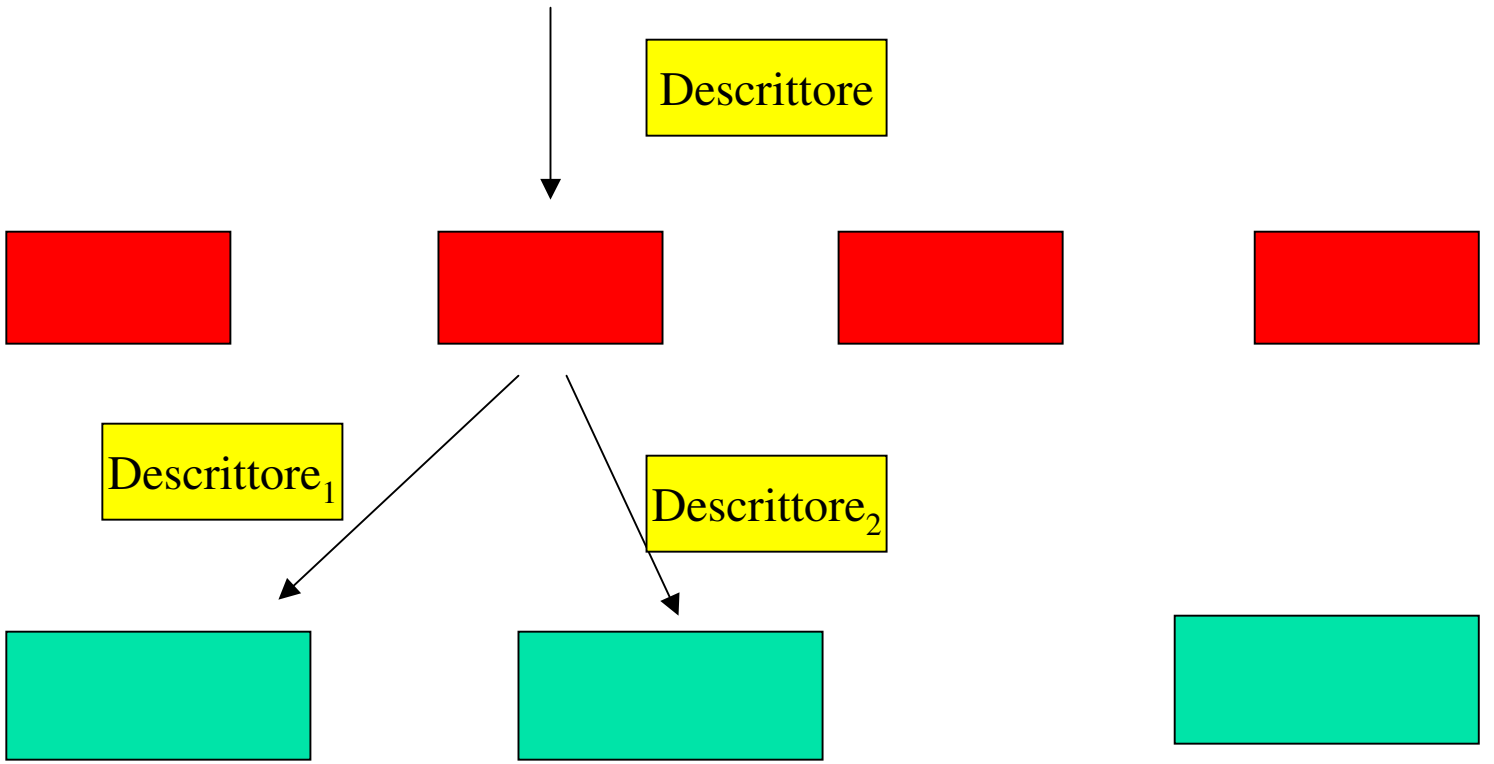
Una soluzione interessante dedica alcuni thread, e quindi alcuni core, a

- personal firewall
- personal honeypot
- personal overlay topology
- ...

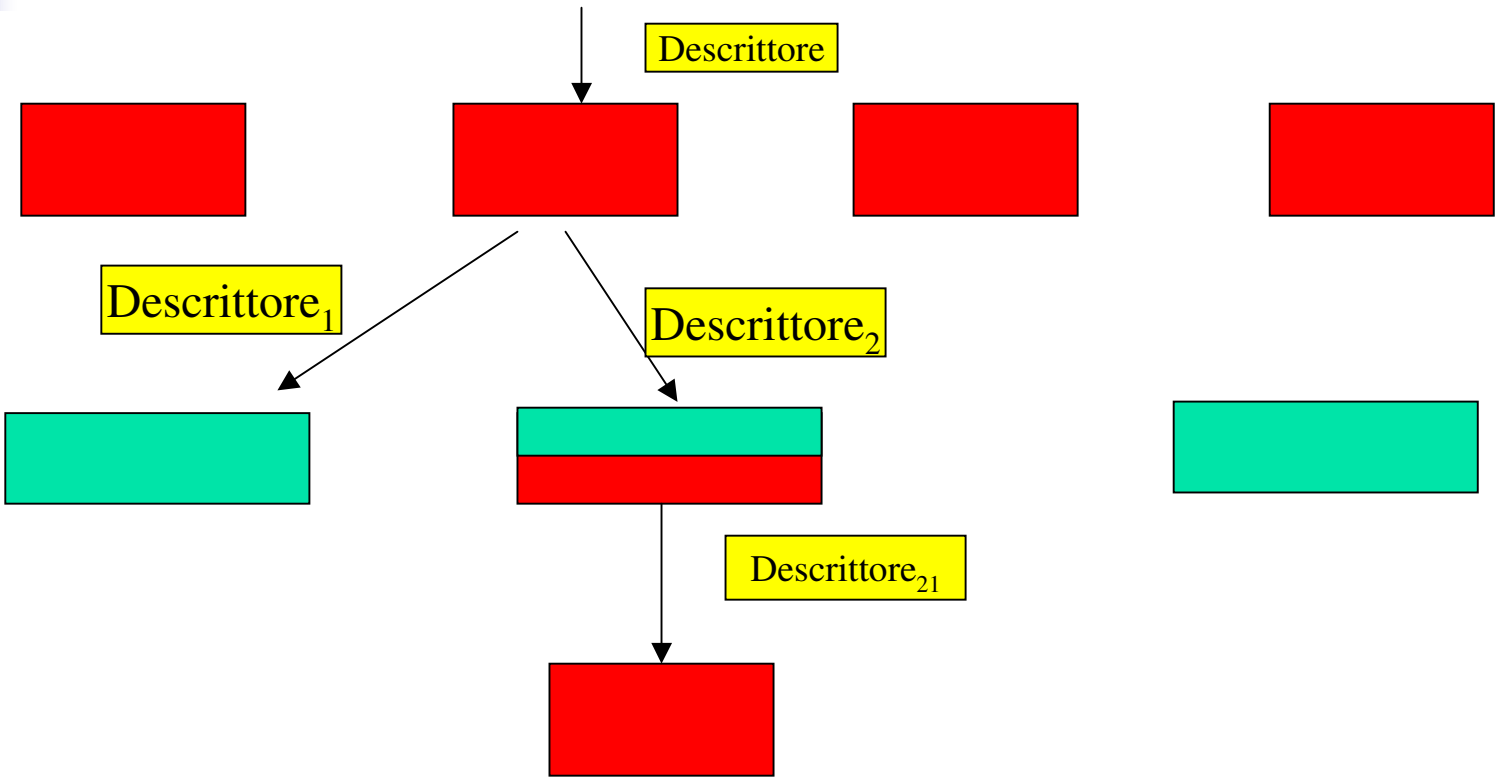
Punti deboli

- Gestione dei dispositivi
  - Auspicabile una visione “a processi” dei dispositivi dove interazione avviene mediante scambio di descrittori
  - Più adatta ad un sistema a “nucleo minimo” (per qualcuno esokernel) in cui il nucleo implementi multiprogrammazione e livello HAL
  - VMM=microkernel done right?????????

Gestione dispositivi



Gestione dispositivi virt[2]



Asimmetria -1

- Quale protezione per chi mappa il proprio overlay = utilizzatore
  - Possibilità di verificare la consistenza dei risultati ottenuti
  - Estremamente difficile garantire la confidenzialità di
    - Input
    - Output
    - Parametri interni

Asimmetria - 2

- Alcuni risultati preliminare su
  - adozione di codifiche one-time pad per proteggere
    - Input
    - Output
  - Uso di frammentazione, encryption ed anonimity per dati memorizzati su supporti di più fornitori
- Più difficile proteggere i parametri dei modelli matematici implementati
- Modello di business commerciale???