Unità di Ricerca
Modena e Reggio Emilia

Progetto PRIN
“Autonomic Security”

Il progetto Autonomic Security

- **Obiettivi del progetto**
  - Integrazione della “self-protection” nei sistemi geograficamente distribuiti
  - Modelli ed algoritmi per la rappresentazione ed il self-monitoring dello stato interno di un sensore
  - Modelli ed algoritmi per l'identificazione dei cambi di stato e delle anomalie
  - Strategie di protezione e di contrasto agli attacchi
    - Contesto specifico: Self-protection contro le botnet

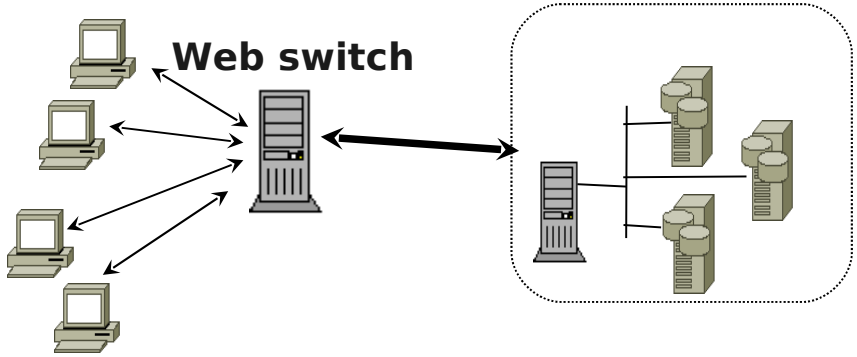
L'unità di ricerca UniMO

- **Partecipanti al progetto**
  - Mauro Andreolini (ricercatore)
  - Claudia Canali (ricercatrice)
  - Sara Casolari (assegnista di ricerca)
  - Michele Colajanni (professore ordinario)
  - Mirco Marchetti (assegnista di ricerca)
- **Competenze**
  - Gestione di sistemi distribuiti su larga scala
  - Monitoraggio di sistemi distribuiti
  - Virtualizzazione
  - Sicurezza

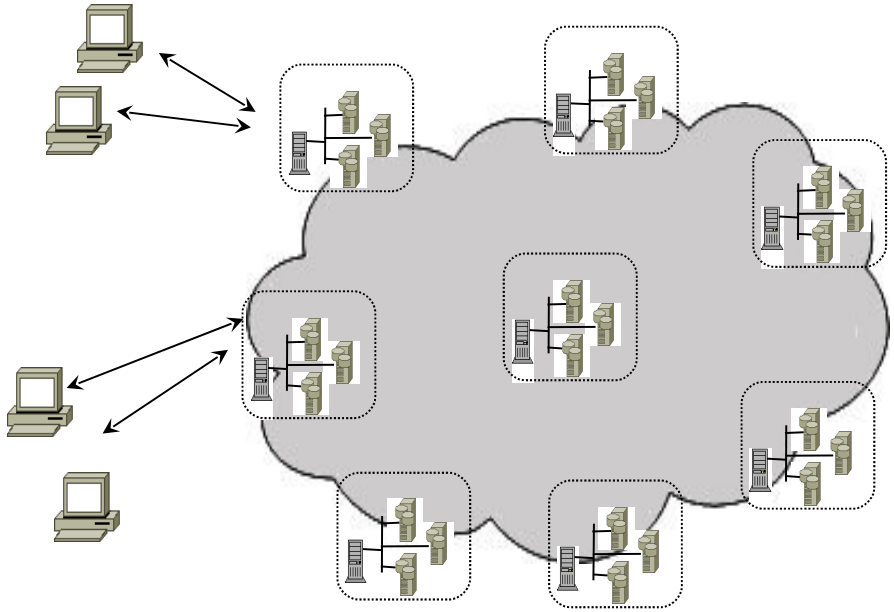
Architetture di riferimento

- **Sistemi distribuiti**

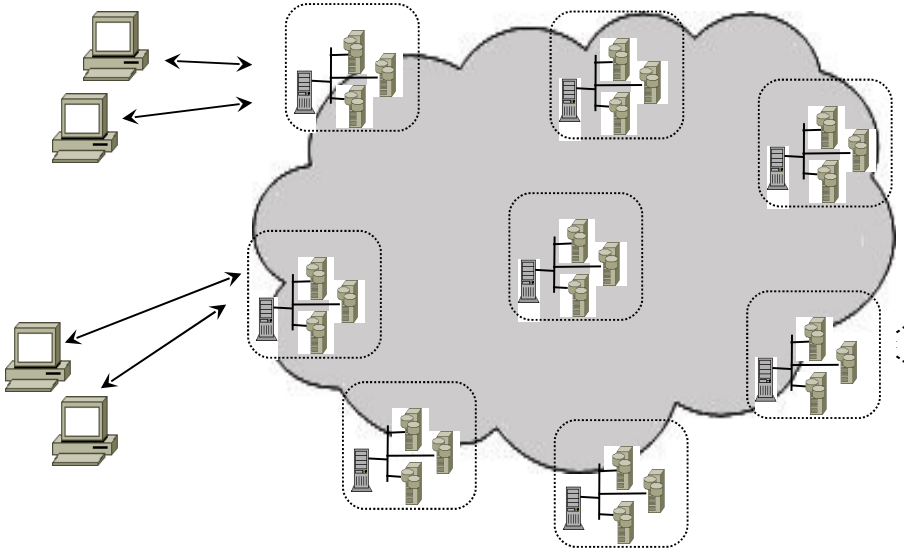
  su scala locale

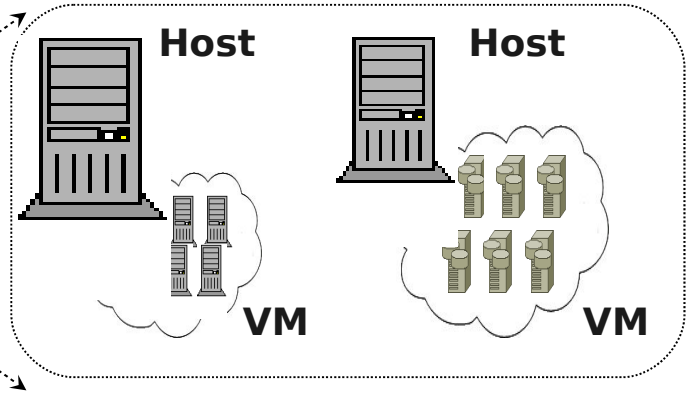


  su scala geografica



- **Sistemi virtualizzati**





Competenze specifiche

- **Monitoraggio**
  - Filtraggio misure grezze
  - Trasformazione misure → **informazione**
  - Algoritmi decisionali (cambi di stato, periodicità ed anomalie)
  - Modelli predittivi (breve/lungo termine, off/online)
- **Virtualizzazione**
  - Architetture virtualizzate (Xen, KVM, OpenVZ)
  - Monitoraggio di sistemi guest e host
  - Migrazione a caldo di sistemi guest
- **Sicurezza**
  - Sviluppo di architetture ed algoritmi per l'intrusion detection parallela
  - Bilanciamento del carico in ingresso

Contributi al progetto

1. **Algoritmi e meccanismi per la detection distribuita di minacce e anomalie**
   - Particolare enfasi sulla **early detection** (scoperta di una possibile minaccia)
   - Particolare enfasi sugli **early warnings** (comunicazione di potenziali minacce)
2. **Strategie coordinate e distribuite per la reazione agli attacchi**
   - Protezione dei servizi
   - Contrasto alle minacce

1. Detection distribuita: Raccolta dei dati

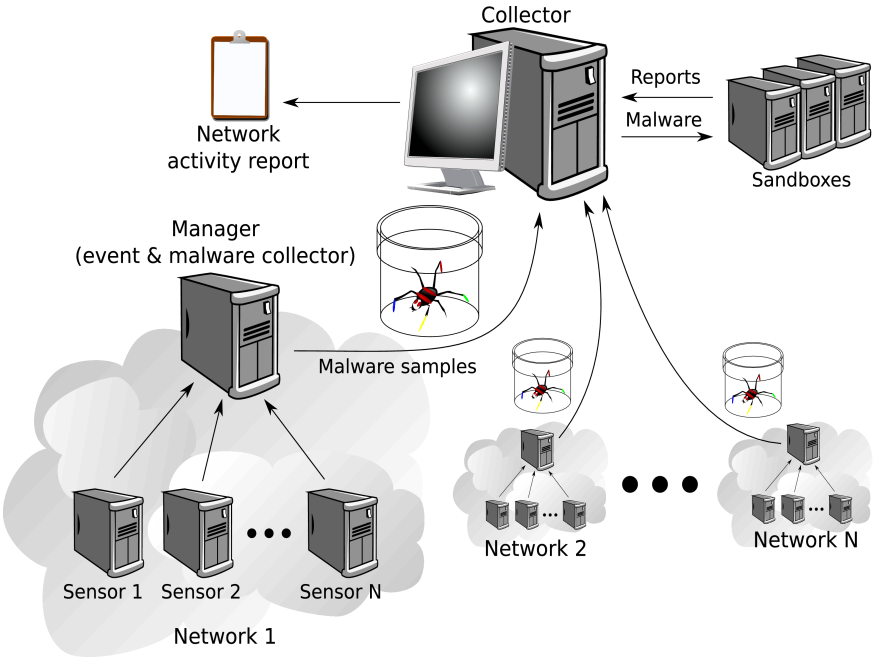
- **Raccolta distribuita di grandi quantità di dati legate ad un elevato numero di eventi**
- **Applicazione di tecniche di “pulizia”**
  - Controlli di significatività dei dati (presenza, validità)
  - Filtraggio statistico (eliminazione dei rumori)
- **Applicazione di algoritmi stocastici per l'individuazione di un andamento pulito del carico**

1. Detection distribuita: Elaborazione dei dati

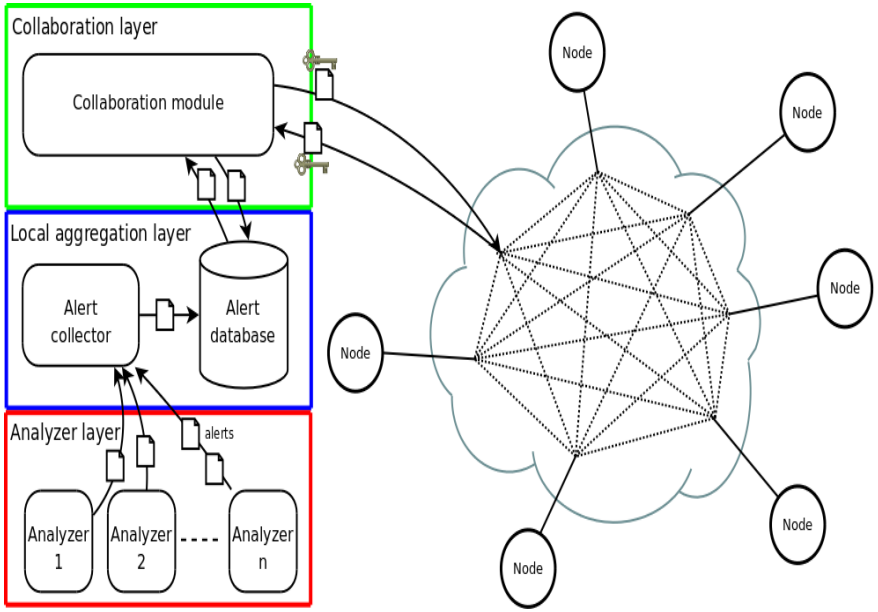
- **Applicazione di tecniche statistiche per il riconoscimento precoce di potenziali minacce (early detection)**
  - Anomaly detection
  - State change detection
  - Correlazione fra dati appartenenti a sorgenti eterogenee
- **Disseminazione precoce di allarmi legati a potenziali minacce (*early warnings*)**
  - Distribuita ai vari componenti dell'infrastruttura
- **Approcci all'elaborazione:**
  - Centralizzato, gerarchico, P2P, ibrido

1. Detection distribuita: Approcci di elaborazione

- **Elaborazione gerarchica**
  - Orientata all'analisi dei malware
  - Riconoscimento precoce attraverso una rete di sensori distribuiti



- **Elaborazione P2P**
  - Condivisione degli allarmi e delle risorse di calcolo attraverso un modulo di collaborazione



2. Reaction distribuita: Protezione dei servizi

- **Implementazione dei servizi su architettura virtualizzata**
- **Migrazione live dei servizi attaccati su reti più sicure**
- **Trasformazione del servizio attaccato in un Honeypot**
  - Attivazione di un Honeypot
  - Alternativa meno costosa: sostituzione del livello back-end associato al servizio

2. Reaction distribuita: Contrasto alle minacce

- **Deviazione del traffico in ingresso basata su DNS**
- **Applicazione di filtri di traffico**
  - Attivazione di regole di firewall
- **Contrasto attivo (laddove possibile) sul canale di comunicazione delle botnet**
  - Comandi IRC