



## Analisi e studio di modelli per il rilevamento di intrusioni di worm polimorfici

*Relatore:*

Dott. Mattia Monga

*Correlatore:*

Dott. Lorenzo Cavallaro

Dott. Andrea Lanzi

*Tesi di Laurea di:*

Luca Mayer

## Definizione: Worm

Agente infettivo autonomo, in grado di replicarsi in autonomia e capace di individuare nuovi host vulnerabili e di infettarli attraverso la rete.

*J. Nazario, 2006*

## Definizione: Worm polimorfico

Un worm si dice polimorfico quando, utilizzando tecniche di offuscamento o di cifratura, è in grado di modificare la sequenza di byte che costituisce il proprio corpo.

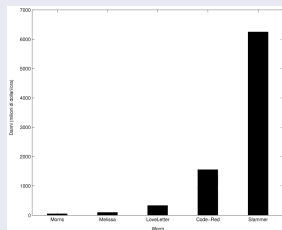
### Scenario

La costante migrazione verso un modello computazionale orientato alla rete ha portato alla creazione di infrastrutture sulle quali si fa regolarmente affidamento nella vita di tutti i giorni.

La facilità con cui è possibile scambiare dati tra macchine differenti però, risulta essere anche un vantaggio per i malintenzionati che intendono provocare danni diffusi.

### La minaccia

In questo scenario, le epidemie di worm, ed in particolare di worm polimorfici, rappresentano una minaccia che non può essere trascurata.



L'orientamento principale che si sta seguendo per quanto riguarda il contenimento di epidemie di worm è quello di implementare sistemi in grado di filtrare il traffico di rete alla ricerca di comportamenti sospetti.

La descrizione del traffico sospetto viene detta *signature*.

I sistemi di contenimento possono essere divisi in:

### *Content-based*

Caratterizzano i worm sulla base delle sequenze costanti di byte contenute nel traffico generato dagli stessi.

### *Semantic-based*

Analizzano i byte del codice del worm o le azioni eseguite dallo stesso per definire un modello del suo comportamento.

### Caratteristiche richieste

Un buon sistema di generazione deve essere:

- Automatizzato
- Resistente contro i worm polimorfici
- Computazionalmente efficiente
- Efficace
- Posizionato a livello di rete
- **Resistente agli attacchi di evasione**

### Obiettivi della tesi

- Studio di Hamsa e delle relative vulnerabilità
- Progettazione ed implementazione di un sistema di contenimento più efficace ed efficiente

### Tipologie di byte

Tipicamente ogni worm polimorfico presenta tre tipologie di byte: *invariant*, *code* e *wildcard* byte.

### Assunzione

**Hamsa** caratterizza il traffico generato dai worm attraverso **signature** contenenti le sequenze di *invariant* byte in esso contenute.

### Tipologie di byte

Tipicamente ogni worm polimorfico presenta tre tipologie di byte: *invariant*, *code* e *wildcard* byte.

### Assunzione

**Hamsa** caratterizza il traffico generato dai worm attraverso **signature** contenenti le sequenze di *invariant* byte in esso contenute.

### Tipologie di byte

Tipicamente ogni worm polimorfico presenta tre tipologie di byte: *invariant*, *code* e *wildcard* byte.

### Assunzione

**Hamsa** caratterizza il traffico generato dai worm attraverso **signature** contenenti le sequenze di *invariant* byte in esso contenute.

### Tipologie di byte

Tipicamente ogni worm polimorfico presenta tre tipologie di byte: *invariant*, *code* e *wildcard* byte.

### Assunzione

**Hamsa** caratterizza il traffico generato dai worm attraverso **signature** contenenti le sequenze di *invariant* byte in esso contenute.

### Algoritmo di generazione delle signature

- Classificazione preventiva in flussi sospetti e innocui
- Algoritmo greedy: determina ad ogni iterazione quale token offre il miglior risultato se aggiunto alla signature precedente

L'approccio utilizzato e il tentativo di creare signature molto specifiche espone Hamsa ad un insieme di vulnerabilità.

### Attacchi efficaci

- Attacchi di *Normal Pool Poisoning*
- Attacchi di *Suspicious Pool Poisoning*
- **Nuovo attacco**

L'attacco evade l'algoritmo di generazione delle signature spingendolo a creare signature contenenti solo *finti invariant byte*.

### Fasi dell'attacco

- 1 Inserimento tra i flussi sospetti di veri worm e di flussi creati ad arte
- 2 La signature generata non contiene invarianti
- 3 Invio di altri worm cambiando insieme di flussi creati ad arte

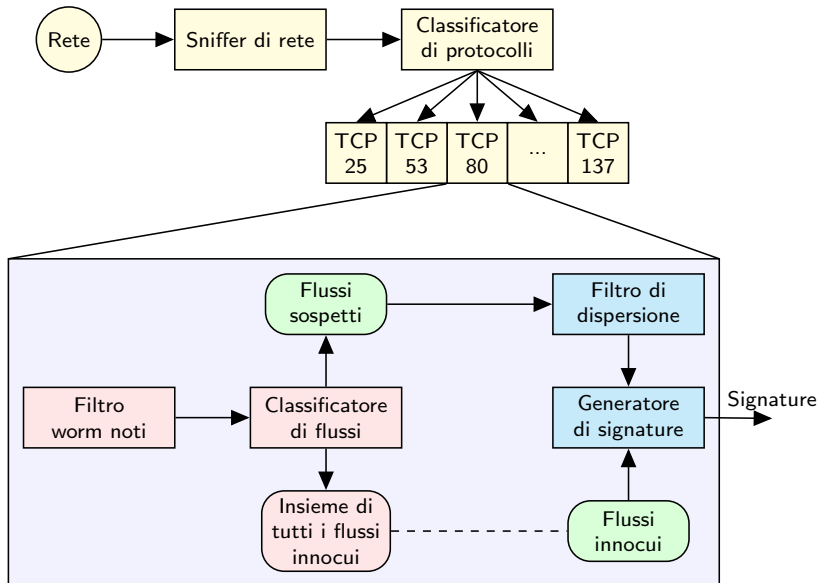
Il nuovo attacco offre **migliori risultati** di quelli precedentemente individuati.

### Vantaggi offerti dal nuovo attacco

- Assenza di invarianti nella signature
- Non richiede sincronizzazione tra diversi esemplari dello stesso worm
- Minor traffico generato rispetto ad altri attacchi dello stesso tipo

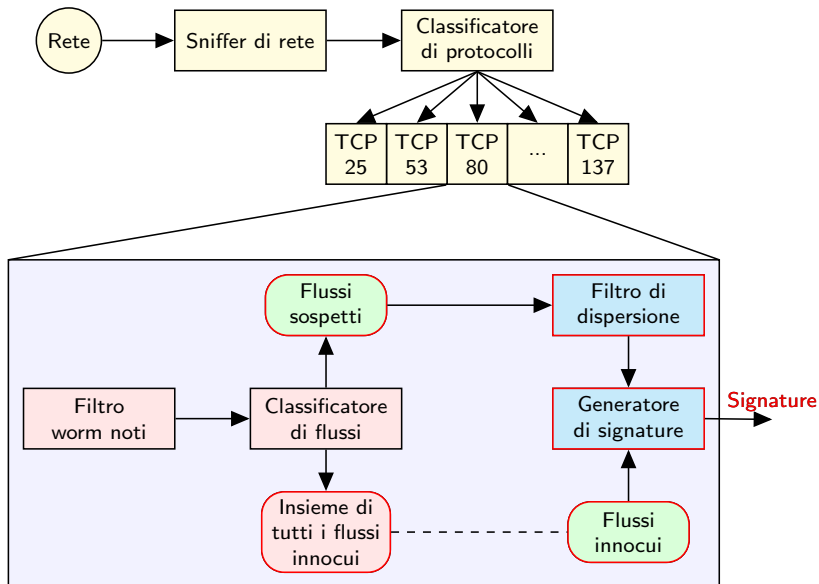
# Il nuovo modello

## Architettura generale



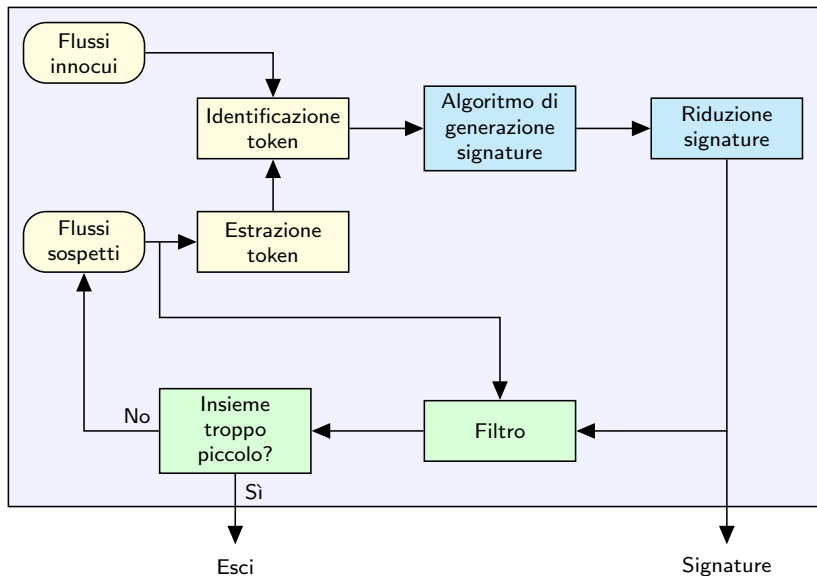
# Il nuovo modello

## Architettura generale



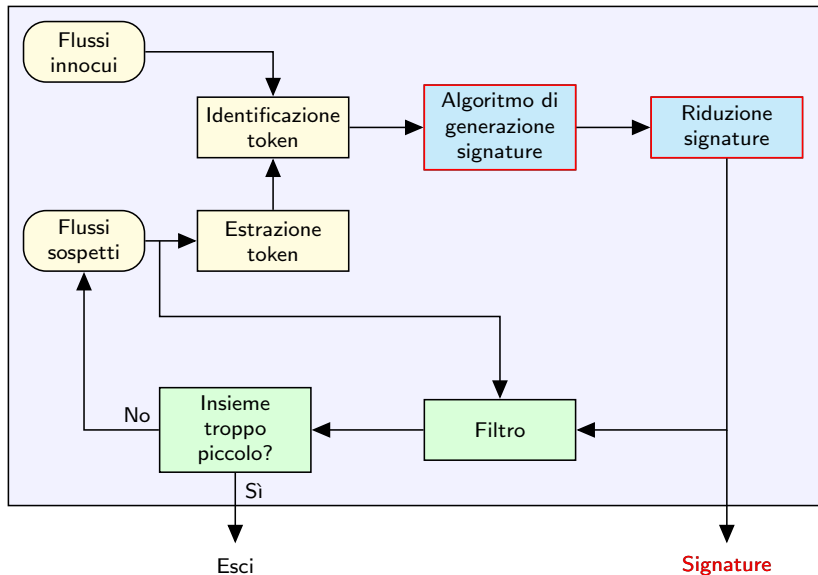
# Il nuovo modello

## Generatore di signature



# Il nuovo modello

## Generatore di signature



Restringe al massimo l'insieme delle assunzioni sul comportamento dell'attaccante

### Algoritmo di generazione del nuovo modello

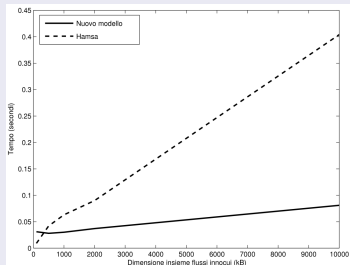
- Presenza di un insieme di invarianti ricorrente
- Generazione di più signature in caso di incertezza
- Visione globale di tutte le signature possibili

### Efficacia

- Tollerante ai disturbi (fino a 50%)
- **Basso tasso di falsi positivi** (0.095%) e falsi negativi
- **Resistente** a molti attacchi di *Suspicious Pool Poisoning*
- Più robusto nei confronti dei *Normal Pool Poisoning Attack*

### Efficienza

- **Più efficiente** di Hamsa su insiemi di flussi innocui di grandi dimensioni
- Uguale sensibilità alle dimensioni dell'insieme dei flussi sospetti



### Contributi

- Individuazione di un nuovo attacco su Hamsa
- Progettazione di un nuovo modello per la generazione delle signature che migliori i precedenti in efficienza, efficacia e robustezza
- Realizzazione di un prototipo che integra Hamsa e alcune delle contromisure applicabili per aumentarne la robustezza
- Integrazione del nuovo modello proposto nel prototipo

### Sviluppi futuri

- Studio di portabilità del modello in ambiente distribuito
- Studio di applicabilità dell'approccio per l'individuazione di SPAM

Grazie per l'attenzione.

Luca Mayer  
*Security Consultant*  
*in Spike Reply*  
l.mayer@reply.it