



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

Relatore:

Dott. Mattia Monga

Correlatore:

Dott. Lorenzo Cavallaro

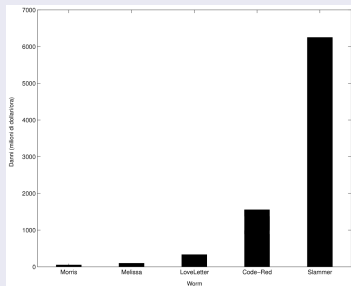
Dott. Andrea Lanzi

Tesi di Laurea di:

Luca Mayer
mat. 685174

Scenario

Le epidemie di **worm**, ed in particolare quelle di worm **polimorfici**, rappresentano una minaccia crescente che non può essere trascurata.

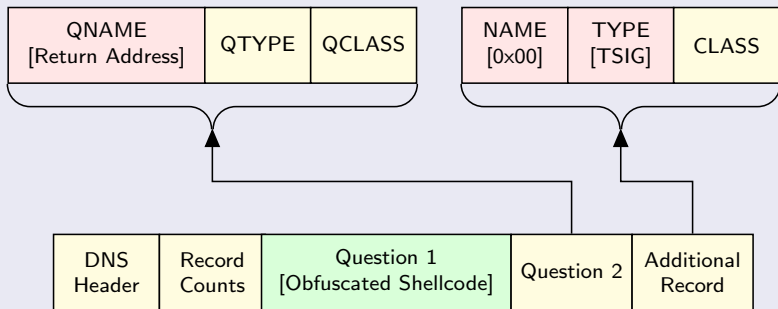


Obiettivi

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

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

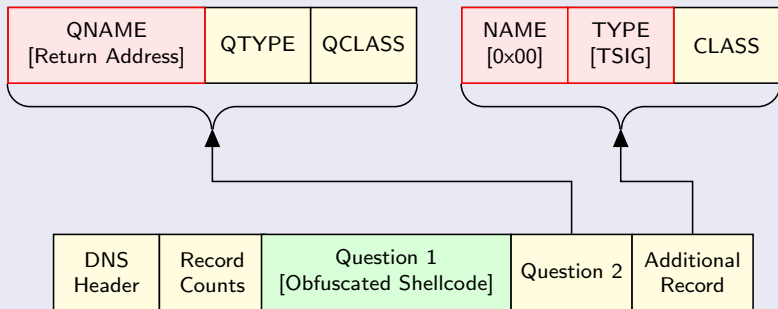
Esempio: Lion worm



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

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

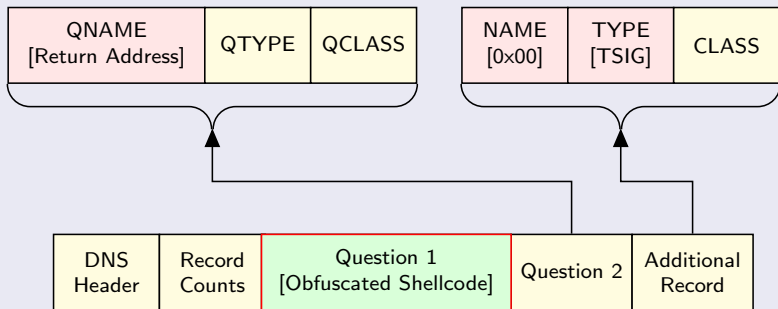
Esempio: Lion worm



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

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

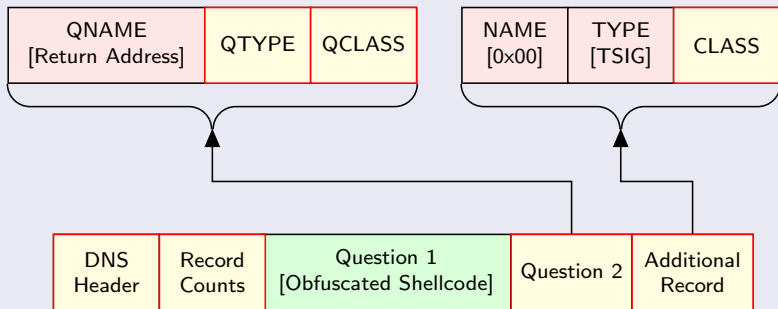
Esempio: Lion worm



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

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

Esempio: Lion worm



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

Caratteristiche del sistema

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**

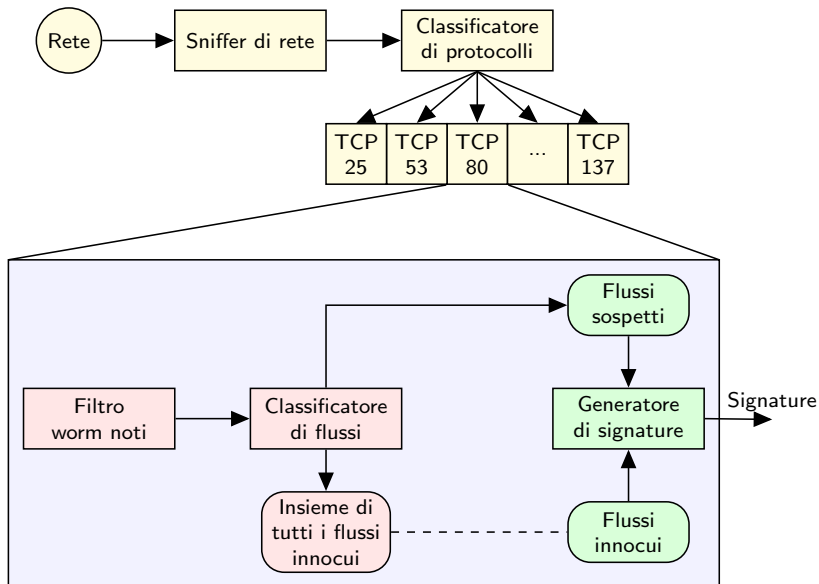
Espressività delle signature

Un sistema può essere efficace solo se genera signature espressive come nel caso delle *multiset signature* in cui:

$$s = \{(t_1, n_1), (t_2, n_2), \dots, (t_k, n_k)\}$$

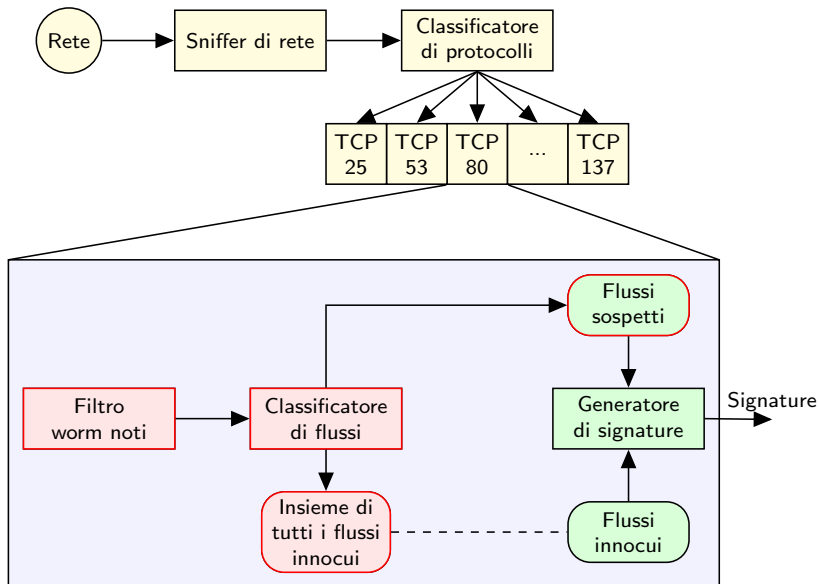
Stato dell'arte: Hamsa

Architettura generale



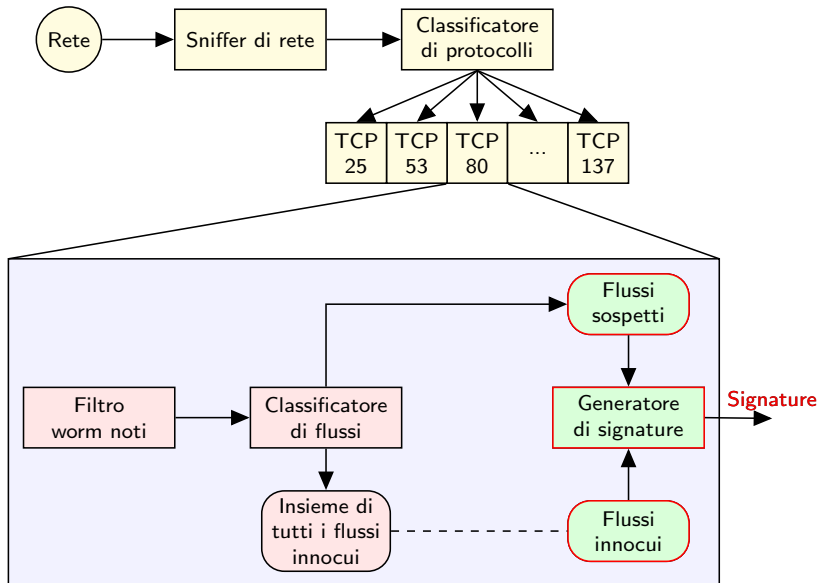
Stato dell'arte: Hamsa

Architettura generale



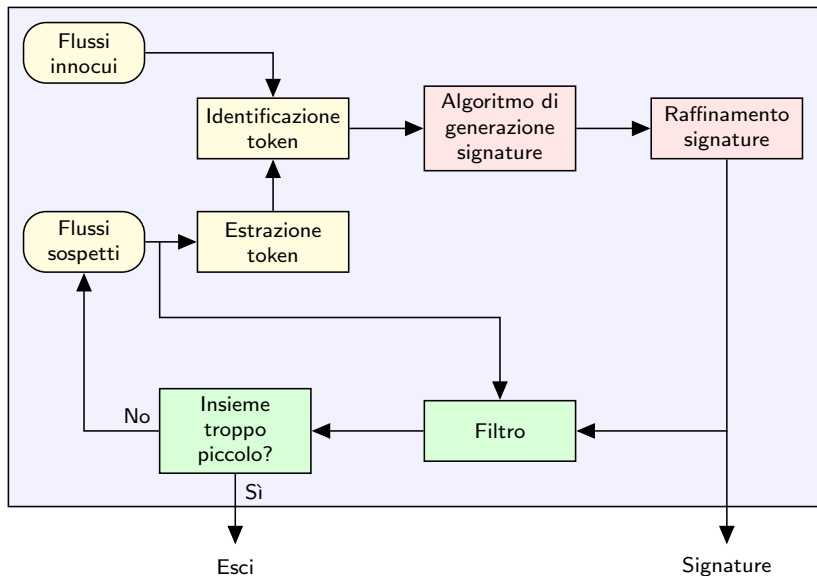
Stato dell'arte: Hamsa

Architettura generale



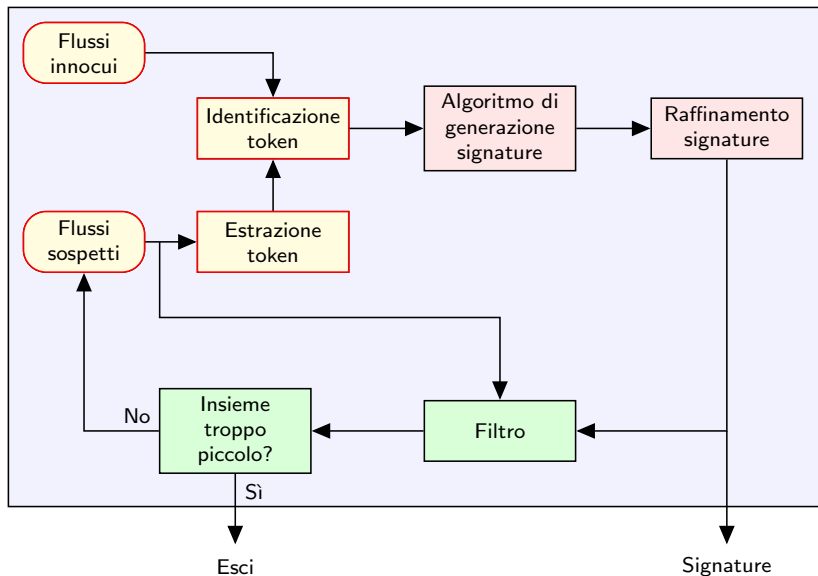
Stato dell'arte: Hamsa

Generatore di signature



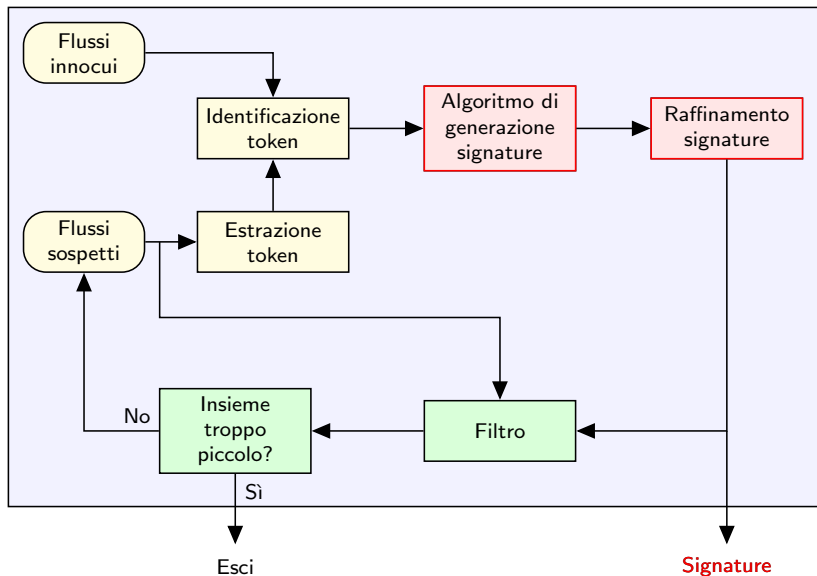
Stato dell'arte: Hamsa

Generatore di signature



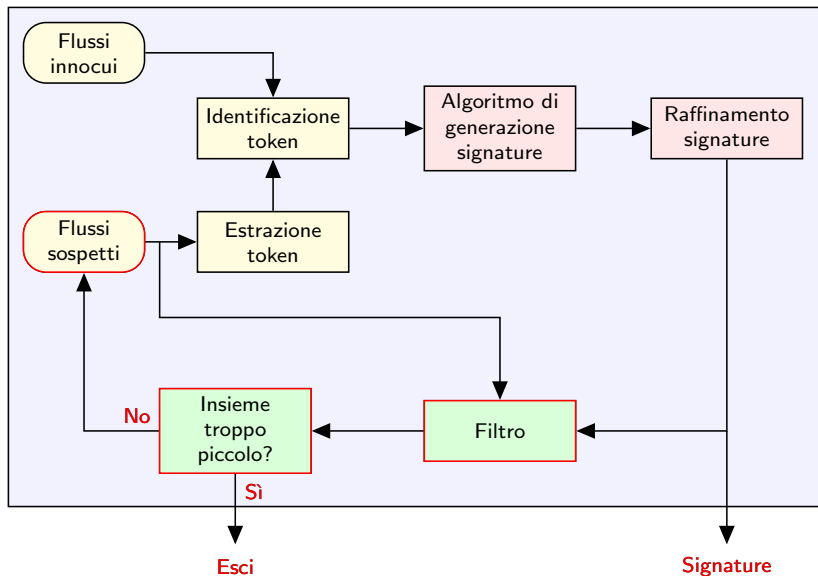
Stato dell'arte: Hamsa

Generatore di signature



Stato dell'arte: Hamsa

Generatore di signature



Algoritmo di generazione delle signature

- Algoritmo greedy
- Determina ad ogni iterazione quale token offre il miglior risultato se aggiunto alla signature precedente
- Restituisce una sola signature che include il numero massimo di invarianti

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 con invarianti fittizi
- 2 La signature contiene solo finti invarianti e rimuove tutti i flussi inviati
- 3 Invio di altri worm cambiando insieme di finti invarianti

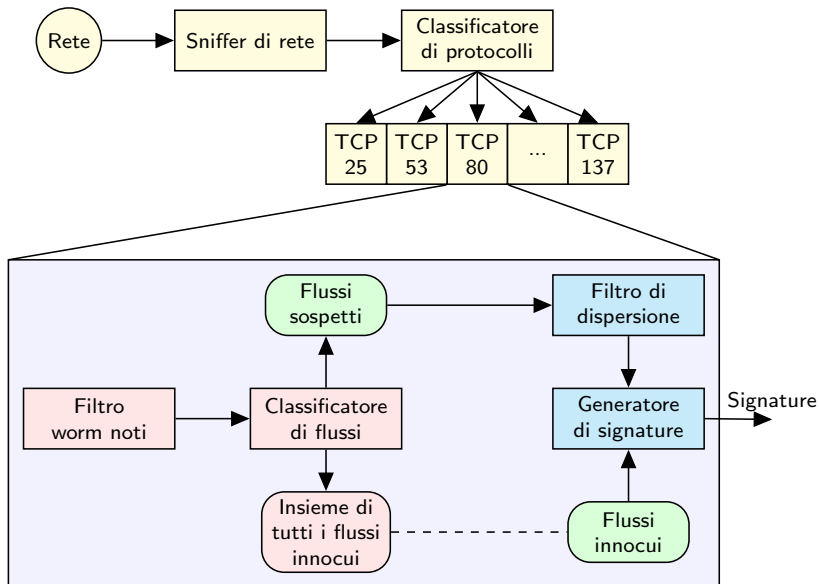
Il nuovo attacco offre **migliori risultati** di quelli precedentemente individuati.

Vantaggi offerti dal nuovo attacco

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

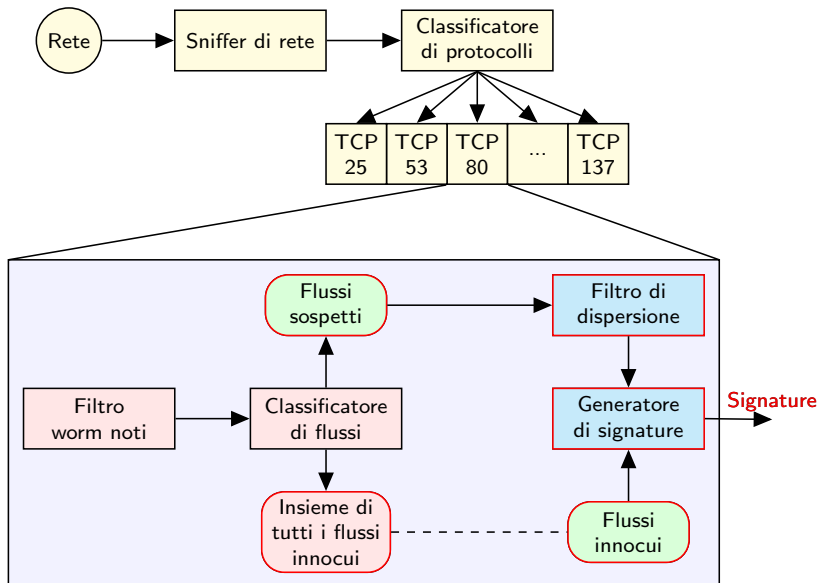
Il nuovo modello

Architettura generale



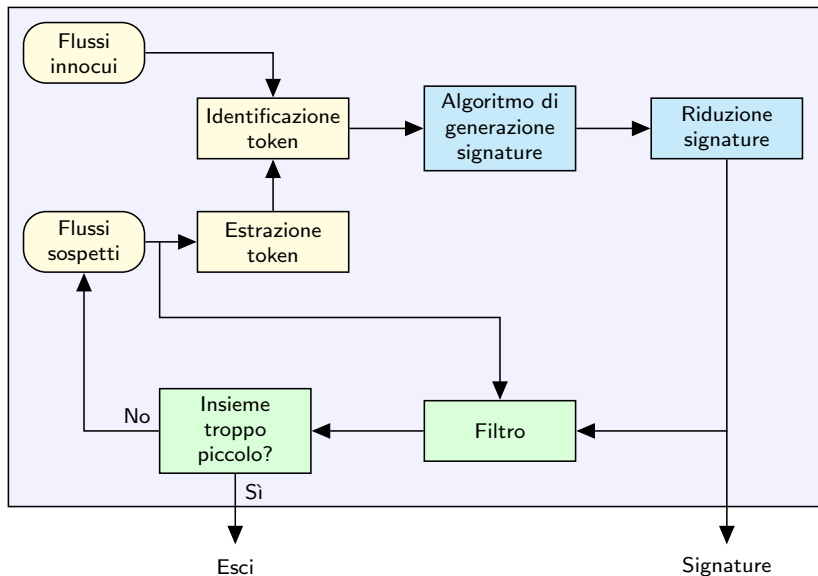
Il nuovo modello

Architettura generale



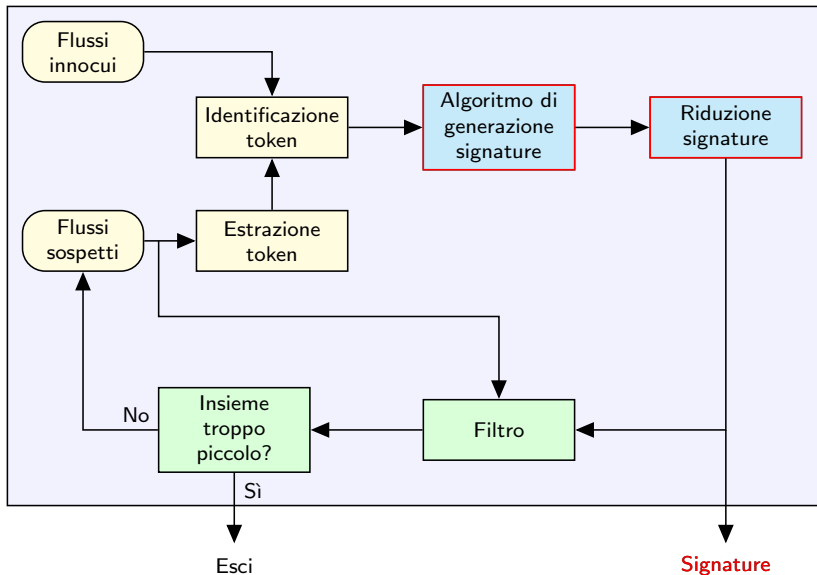
Il nuovo modello

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

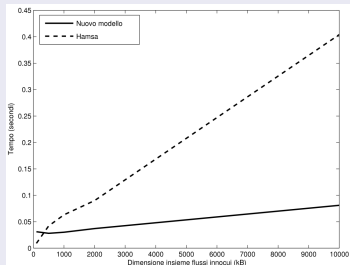
- Presenza di un insieme di invarianti ricorrente
- Generazione di più signature in caso di incertezza
- Visione globale di tutte le signature possibili
- Nessun vincolo sulle signature parziali

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

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

Grazie per l'attenzione.