Università' degli studi di Roma "Tor Vergata"
Teoria della sicurezza e crittografia
Lezione 04

Authors: Angelo Silvestri, Marcello Politi, Samir Salman

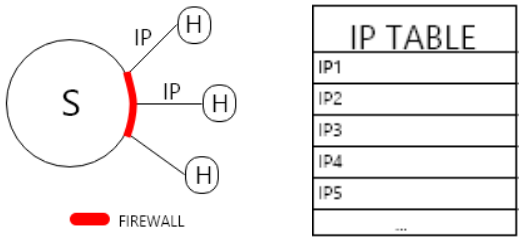
Ottobre 2019

1 Introduzione

Descriveremo i due tipi di sicurezza, Statica e Dinamica, ne analizzeremo i diversi approcci per la protezione del sistema stesso. Inoltre parleremo della Learning Theory applicata alla sicurezza informatica.

2 Identificare gli utenti

Ipotizziamo che ogni utente possieda un indirizzo IP univoco, in questo modello gni utente può essere identificato univocamente mediante un indirizzo IP che non cambia nel corso del tempo. In un sistema di questo tipo è molto semplice utilizzare un Firewall per la protezione del nostro sistema, il quale autorizza solo una serie di IP autorizzati a noi ben noti, contenuti nell'IP Table del Firewall.



Ma questa visione in cui ogni utente posside un ip univoco è alquanto utopica, poichè gli indirizzi ip da diversi anni a questa parte sono dinamici, ovvero cambiano ad intervalli temporali, in modo "casuale". Come faccio allora a studiare il comportamento di uno specifico utente? Utilizzo una sistema di registrazione, il quale mi permettere di identificare ogni utente mediante un account. Ma come faccio a difendermi dagli attacchi?

3 Sistemi di Sicurezza Statici

Per difendere un sistema si utilizza la tecnica derivante dalla Learning Theory, ovvero: OSSERVARE, PROTEGGERE ed eventualmente REAGIRE. In un modello statico la fase di osservazione viene effettuata mediante osservazioni **atemporali**, attraverso un modello generatore. Il modello generatore ci permette, dato un'insieme di osservazioni, di affermare che un dato modello statico è coerente o meno con questo insieme.

Esempio: Osserviamo 1000 altezze relative alla popolazione italiana e le confrontiamo con un modello (per esempio la curva normale). Se il modello è accettato allora la variabile normale è il "generatore" delle altezze degli individui di una certa popolazione.

Ma come applico un modello del genere ?

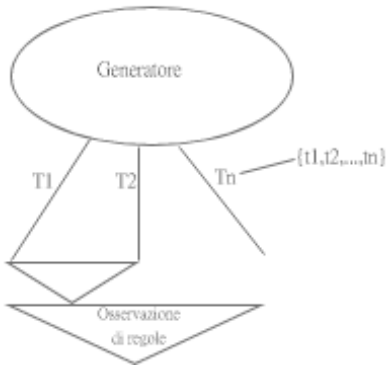
1. Genero una popolazione "simile" a quella appresa
2. Riconosco un elemento come tipico o meno di una certa popolazione
3. Riconosco, dopo aver visto N istanze, se un generatore incognito si sta comportando o meno come il Generatore appreso.

Si preferisce in ogni modo un sistema statico a più variabili, per avere un modello maggiormente affidabile, il modello rimane comunque statico poichè atemporale.

4 Sistemi di Sicurezza Dinamici

In un modello statico molto spesso è complesso riuscire ad apprendere in modo ottimale, poichè tutte le osservazioni sono atemporali. In un sistema dinamico, invece, ogni osservazione è una sequenza di valori osservati in tempi **successivi**.

Data una singola osservazione, quindi, essa è formata da un prima e un dopo, con le osservazioni associate ad ogni intervallo temporale.



L'obbiettivo in sistemi dinamici è quello di definire un generatore che, osservati i primi k eventi, sia in grado di predire l'evento k+1.
Utilizziamo delle regole ben definite, per verificare la presenza di **anomalie** nel comportamento di un utente *U1* osservato.
Nel caso in cui il comportamento sia considerato anomalo, molto spesso viene utilizzato un **Honeypot**, ovvero uno spazio isolato all'interno del nostro sistema grazie al quale possiamo studiare le azioni del nostro attaccante al fine di apprendere.