Università' degli studi di Roma "Tor Vergata"
Teoria della sicurezza e crittografia
Lezione 06

Authors: Angelo Silvestri, Marcello Politi, Samir Salman

Novembre 2019

1 Introduzione

In questa lezione parleremo dell'entropia legata alla sicurezza di un sistema, in particolare della relazione che c'è tra l'entropia e la conoscenza di un determinato sistema.

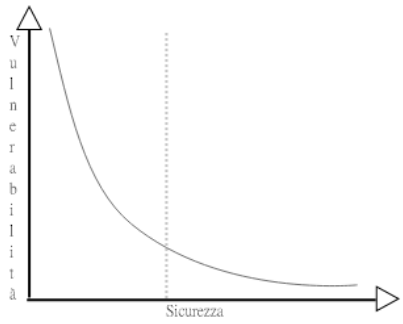
2 Entropia e Osservatore

Supponiamo di avere un osservatore X che possiede una propria conoscenza C relativa ad un sistema, formata da diversi elementi e diverse osservazioni in un certo arco temporale: $C = c1, c2, \ldots, cn$. L'entropia di un determinato sistema varia in base alla conoscenza dell'osservatore, o meglio il Δ, varia in relazione alla conoscenza C dell'osservatore X di un determinato sistema.

Quando si parla di conoscenza pregressa di un certo osservatore, si fa riferimento ad una base di conoscenza costruita studiando il sistema.

3 Variazione di Entropia in base alla Conoscenza

Ipotizziamo di costruire un nuovo sistema S (ad.es. Piattaforma WEB), e pubblicarlo sulla rete. Inizialmente S al tempo $t0$ sarà sconosciuto, in termini puramente pratici avrà pochi clienti, ed avrà di conseguenza una vulnerabilità bassa, poichè gli attaccanti non saranno ancora a conoscenza del sistema. Con il passare del tempo, supponiamo in un certo tn, e l'aumentare dei clienti, il sistema diventerà più vulnerabile.



L'obiettivo è quindi di migliorare S **prima di tk**, ovvero nell'intervallo *t0,...,tk-1*, al fine di riuscire ad aumentarne la sicurezza.

4 Osservazione di un Sistema

Dato un sistema S osservo il variare dell'entropia in base a degli eventi.

Esempio: Supponiamo di osservare un aumento di entropia conseguentemente all'evento di backup del nostro sistema. Il backup avviene ogni giorno alle ore 02:00 AM. Osserviamo quindi il sistema per un determinato intervallo di tempo T, ed osserviamo che ogni giorno alle 2 di mattina l'entropia aumenta. L'aumento di entropia però, data la nostra conoscenza pregressa, è normale e non desta alcun sospetto. Ora supponiamo che l'ottavo giorno alle 02:00 AM l'entropia rimane inalterata, a quel punto sappiamo che c'è qualcosa che non va, bisogna intervenire.

Questo esempio dimostra come l'entropia possa essere utilizzata nell'osservazione di un determinato sistema e di eventi ad esso legati.

5 Obiettivo

L'obiettivo finale di questo processo di osservazione è quello di realizzare un ***tool*** in grado di:

1. Osservare
2. Classificare
3. Riconoscere Anomalie

4. Agire

Il problema relativo alla sicurezza negli ultimi anni si è fatto sempre più importante, sopratutto relativamente all'utilizzo di sistemi distribuiti, nei quali la Sicurezza Statica non ha alcuna validità.