Universita' degli studi di Roma "Tor Vergata"
Teoria della sicurezza e crittografia

Author: Marcello Politi, Samir Salman, Angelo Silvestri

Novembre 2019

1 Introduzione alla sicurezza WEB

Le procedure sul web sono sempre a tutela di chi fornisce il servizio di rete. Tuttavia definire un modello web che sappia quali sono le informazioni che devono essere difese e tutelate può risultare non banale. Ad esempio un servizio web potrebbe essere "ingannato" da uno user che esegue un accesso e apre una sessione, banalmente una carta condivisa con il server per definire l'identità dello user potrebbe non essere veritiera, in altre parole gli utenti potrebbero dichiarare il falso e il server potrebbe essere all' oscuro della vera identità di chi sta usufruendo dei suoi servizi.

2 Modello di sicurezza

Un modello di sicurezza evoluto è caratterizzato dalle seguenti procedure:

- **Osservare** l'evoluzione del sistema
- **Comprendere** cosa si sta verificando
- **Reagire** se si verificano *situazioni* "pericolose"

Definiamo meglio cosa intendiamo per *situazioni*. Queste a loro volta si suddividono in diverse tipologie:

- **Legali** : riguardano la usability, non sono da vedere come un attacco
- **Attacco** : in seguito ad un attacco attiverò delle contromisure quanto possibile per limitare i danni
- **Anomalie** : questa è l' unica situazione in cui possiamo veramente ancora intervenire in quanto il vero e proprio attaccato ancora non si è verificato

Uno dei più semplici e comuni esempi è quello del *CAPTCHA* che ha lo scopo di difendere il sistema contro automi.
Se il captcha viene sbagliato piu volte si avverte una *anomaly detection*.

3 Modellazione di un sistema attraverso un Generatore

Un sistema è modellabile con quello che possiamo chiamare **Generatore**. Ogni

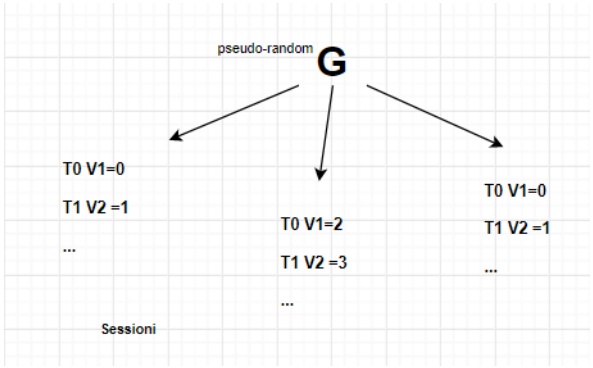

Figura 1: The Universe

sequenza di bit generata (in maniera pseudorandomica) corrisponde ad una sessione di lavoro, e ogni sessione è definita da una succesioni di variabili, ogni variabile fa riferimento ad un dato istante di tempo t_i
Possiamo quindi pensare che G generi sequenze di bit a seconda delle azioni che un utente esegue sul servizio web.
La domanda fondamentale da porsi in ambito di sicurezza è la seguente:
"se al tempo t_k osservo una cosa, cosa osservero al tempo $t_{t+\Delta}$?"

4 Proprietà e problematiche del Generatore

Al tempo t_0 tutti gli eventi sono ancora possibili, mentre al tempo t_1 restringo il campo degli eventi possibili (si veda firuga 2).

- N definito da un insieme di variabili
- N1 definito come un sottoinsieme di N

La cardinalità delle possibili entità e quindi di tutte le possibili generazioni di G è 2^k Dopo un numero di osservazioni L > K sono in grado di distinguere un' entità dalle altre, possiamo dire che siamo in grado di **apprendere**, e ovviamente la prima cosa che si fa quando si apprende, è quella di riuscire a distinguere le cose.

$\exists$ L s.t. dopo L passi posso decidere

Se conosco la distribuzione della popolazione allora L è calcolabile in modo preciso.

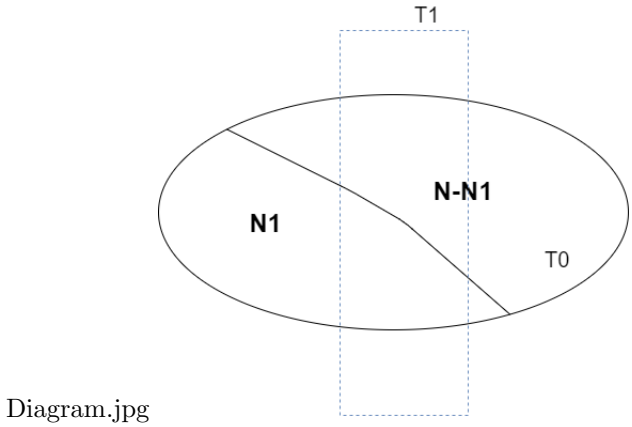

Diagram.jpg

Figura 2: The Universe

Le anomalie osservate le suddividiamo a loro volta in:

- **Attacco**
- **Legali**

Se dopo L passi della traiettoria ancora non riesco a distinguere l'azione, allora la probabilità che sia un attacco diventa maggiore, perchè so che le azioni legali in L passi dovrebbero terminare. Prima di L passi non conosco nulla, ogni azione è equiprobabile.

$\frac{n_{ij}}{n}$ = frequenza di osservazione di una sola popolazione

5 Introduzione all'Entropia

L'**entropia** formalmente viene definita come segue:

$$E = -\sum^{n} \ln p_i \tag{1}$$

Qualitivamente l'entropia ci dice quando non conosco, cioè la quantità di randomness di una variabile aleatoria. Quindi se l'entropia del sistema scende, vuol dire che noi stiamo conoscendo sempre di più di quanto sta accadendo. In questo modo possiamo valutare la qualità del nostro lavoro in termini di conoscenza di quanto sta succedendo.