Un sistema di recommendation per la cybersecurity basato su Collaborative Filter

Andrea Michele Albonico (matricola 886667)

/02/2020

RELATORE
Prof. Valerio Bellandi

CORRELATORE
Prof. Claudio A. Ardagna

Il Cloud Computing è ormai diventato il paradigma dominante nell'ICT, tuttavia permangono problematiche legate alla mancanza di fiducia e trasparenza. Tali criticità ancora rendono gli utenti esitanti nel migrare completamente a questo nuovo approccio. Una delle strategie utilizzate per affrontare questa mancanza di fiducia è la *Security Assurance*, ovvero un insieme di tecniche per la verifica che un certo sistema ICT rispetti o meno delle proprietà di sicurezza.
Moon Cloud è un framework di *Security Assurance* il quale garantisce che un sistema ICT soddisfi certi requisiti di sicurezza prestabiliti da appropriate politiche precedentemente definite. Esso opera seguendo un processo olistico e continuo di raccolta di evidence presso i sistemi oggetto di verifica garantendo l'uniformità di quell'asset a una o più politiche.
Il lavoro di tesi ha l'obiettivo di rendere le attività di *Security Assurance* di Moon Cloud accessibile anche ad utenti meno esperti, mediante lo sviluppo di un sistema di raccomandazione di verifiche di sicurezza. Il lavoro svolto si può articolare come segue.

1. Studio della piattaforma Moon Cloud, in particolare dei concetti di *Controlli* ed *Evaluation*. Essi sono i due componenti base del processo di verifica di Moon Cloud, sui quali si intendono effettuare le raccomandazioni.

2. Studio dei diversi approcci utilizzabili per la catalogazione di *Controlli* ed *Evaluation* in un database relazionale, per creare delle tassonomie. In particolare, è stato necessario trovare il modo migliore per memorizzare tali tassonomie all'interno di un modello di dati di tipo relazionale.

3. Studio delle diverse tipologie dei sistemi di raccomandazione e valutazione di quali fossero i più adeguati per il problema in questione. Si sono analizzati in particolare i sistemi *Content-based filter* e i *Collaborative filter*, nello specifico si osservarano quali fossero i punti di forza e debolezza, e i motivi per cui è stato scelto il secondo tipo rispetto al primo.

4. Creazione di un microservizio che implementa un sistema di raccomandazione. Tale componente è in grado di offrire raccomandazioni basandosi su i) la tipologia di target obiettivo della verifica di sicurezza, ii) la categoria delle Evaluation applicate all'asset in questione, iii) Evaluation simili usate da altri

utenti e iv) la categoria di appartenenza delle Evalution unitamente a quelle simili usate da altri utenti. Il servizio inoltre offre una serie di API per facilitare il mantenimento della coerenza tra il database principale di Moon Cloud e quello usato dal servizio stesso.

Al termine dello sviluppo, la soluzione offre delle raccomandazioni di tipo basico, tuttavia è in grado di supportare gli utenti nell'utilizzo del framework Moon Cloud.Offre altresì spunti di miglioramento, ad esempio l'introduzione di un sistema di valutazione delle Evaluation o dei Controlli da parte dell'utente così da incrementare la precisione del sistema di raccomandazione, il quale terrebbe conto anche di queste valutazioni.