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 mediante la raccolta continua di evidence presso i sistemi oggetto di verifica.
La soluzione proposta in questa tesi ha come quello obiettivo di rendere le attività di *Security Assurance* di Moon Cloud accessibili 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*.
   Il primo algoritmo analizza direttamente i metadati del item e non considera gli interessi di altri utenti, i quali potrebbero suggerire altri prodotti che non verrebbero notati con questo approccio. Per quanto riguarda il CF, non prende in considerazione i contenuti e proprietà associati agli item ma una raccomandazione viene fatta sulla base dell'uso che gli utenti fanno degli item e questo è il suo punto di forza perché non si trova a dover analizzare item ricchi d'informazioni. Allo stesso tempo è anche il suo punto debole, perché può portare suggerimenti che potrebbero essere considerati poco adatti sulla base della poca relazione con i profili di alcuni utenti.

Infine, è stato scelta la tipologia dei *Collaborative filter* perché si è voluto dare importanza e mettere in primo piano ciò che pensano gli utenti, così da cercare di colmare il problema della mancata fiducia in questi sistemi.

4. Creazione di un microservizio che implementa il sistema di raccomandazione. Esso 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 *Evaluation* unitamente a quelle simili usate da altri utenti. Inoltre, il servizio offre una serie di API per facilitare il mantenimento della coerenza tra il database principale di Moon Cloud e quello usato dal servizio stesso.

La soluzione sviluppata offre delle raccomandazioni non sofisticate, tuttavia può fornire buon supporto all'utilizzo di Moon Cloud. Come prospettiva futura vi è l'introduzione di un sistema di *rating* di *Evaluation* e *Controlli*, al fine di incrementare la precisione del sistema di raccomandazione.