Verifiche di Assurance in Architetture di Nuova Generazione: uno Schema di Certificazione per Sistemi Basati su DevOps

Nicola Bena (matricola 938353)

RELATORE
Prof. Claudio A. Ardagna

CORRELATORE
Prof. Marco Anisetti

L'avvento del cloud computing ha rivoluzionato molte delle pratiche IT. Da un lato, si sono affermati nuovi paradigmi di sviluppo software, in cui lo sviluppo, la sicurezza e le *operations* vengono unificate **in un unico processo** (*DevSecOps*). Dall'altro lato, **la crescente richiesta di affidabilità (*reliability*), fiducia (*trust*) e sicurezza ha introdotto la necessità di un ripensamento delle tecniche di *security assurance*** esistenti, in particolare delle tecniche di certificazione, verso **scenari** sempre più **complessi, dinamici e adattivi**.

Una delle principali problematiche delle metodologie di certificazione esistenti risiede nel fatto che **tali tecniche sono state progettate per verificare il prodotto finale** di un processo di sviluppo software, **tralasciando completamente il processo di sviluppo e le sue peculiarità**.

Scopo di questa tesi è **la definizione e l'implementazione di un nuovo schema di certificazione** in grado di certificare **non solo il prodotto finale ma anche il processo di sviluppo software corrispondente**. **La tesi si concentra su *DevOps* e *DevSecOps***, le cui **attività di certificazione** possono essere **svolte durante il processo di sviluppo** oggetto di certificazione.

Il lavoro svolto si può articolare come segue.

1. **Studio dello state dell'arte delle metodologie *DevOps* e *DevSecOps***, per comprenderne i principi di base. Successivamente, è stato effettuato uno studio dello stato dell'arte delle metodologie di certificazione, come base per l'estensione presentata in questa tesi.

2. **Definizione di un nuovo schema di certificazione per processi di sviluppo *DevOps* e *DevSecOps***. Il nuovo schema considera due dimensioni, il processo di sviluppo software oggetto di certificazione, e il modo con cui le verifiche vengono effettuate. Entrambe le dimensioni, infatti, intervengono nelle proprietà non funzionali che vengono certificate. Sulla base di ciò, **vengono definiti i requisiti che guidano** l'implementazione della metodologia.

3. **Realizzazione dello schema di certificazione.** Il punto di partenza è Moon Cloud, un framework di *assurance* già esistente, modificato ed esteso per supportare il nuovo schema e favorire l'inserimento delle pratiche di certificazione in un processo di sviluppo *DevOps*. Il nuovo framework fornisce i) una nuova interfaccia basata su API standard, ii) un *container* per l'esecuzione delle attività di certificazione in una *pipeline*, iii) controlli di sicurezza *trustworthy*, iv) un paradigma per ri-eseguire le certificazioni a seguito di cambiamenti nel contesto di sicurezza.

4. **L'istanziazione della metodologia di certificazione in un caso di studio**, in cui i diversi aspetti del framework vengono testati in uno scenario basato su un *marketplace*.

Il lavoro di tesi lascia spazio a diversi sviluppi futuri. Dapprima, lo studio di **nuove evoluzioni dello schema di certificazione**, riguardanti il ciclo di vita dei certificati. In seguito, lo studio di un **paradigma di esecuzione distribuito**, in cui la computazione che porta al rilascio di un certificato è divisa tra il framework di certificazione e il framework in cui avviene lo sviluppo del software.