

Fabrizio Baiardi - Intervista al Forum ICT Security 2018

Author : Redazione

Date : 13 novembre 2018



Fabrizio Baiardi

Professore associato di Informatica, Università di Pisa

La principale problematica legata da un penetration test è data dall'impossibilità di seguire tutti i possibili percorsi per attaccare un sistema. Esistono più percorsi ma il penetration test per sua natura ne analizza solo alcuni, ci dà informazioni sì utili ma parziali; paradossalmente si potrebbero bloccare i percorsi più complessi lasciando aperti quelli più semplici rendendo la vita dell'attaccante più facile.

Una soluzione potrebbe essere quella di sostituire l'uomo con la macchina che non stancandosi analizzerebbe tutte le possibili strade. A quel punto avremmo una copertura molto elevata, un test ripetibile e chi commissiona il test avrebbe la certezza che gli vengano fornite tutte le informazioni e non il dubbio che il tester possa avergli nascosto qualcosa

Oggi è possibile una valutazione automatica e si può ottenere applicando il penetration test fatto da un programma non al sistema reale ma ad un modello dello stesso; è la cosiddetta ingegneria basata sui modelli in cui si costruisce un modello del sistema e lo si fa attaccare da un altro programma. Questo sistema ci dà maggiori garanzie e sicurezze. Un penetration test basato su modelli permette di superare tutti i limiti del penetration test.

1. Oggi i penetration test rappresentano una delle principali risorse per la prevenzione dei cyber attacchi. Tale strumento, però, presenta anche taluni aspetti problematici. Quali?
2. Come ritiene che possano essere superate queste difficoltà?
3. Ampliando la prospettiva, è possibile – all'attuale stato evolutivo della tecnologia – valutare automaticamente la sicurezza di un sistema informatico?