

Progetto e Piano di Formazione

Metodologie e tecniche per l'analisi delle vulnerabilità di sicurezza in ambito blockchain

Le attività di questo assegno di ricerca, della durata di 12 mesi, si concentreranno principalmente sullo studio delle metodologie e tecniche per l'analisi delle vulnerabilità di sicurezza relative alle blockchain impiegate nelle smart city. Questo progetto si inserisce nell'ambito dell'iniziativa "Approccio sistemico alla prevenzione e mitigazione dei rischi relativi a cybersecurity, cyber resilienza e safety (EcoCyber)" all'interno del progetto "SEcurity and RIghts in the CyberSpace" (SERICS). Gli obiettivi principali comprendono la progettazione, implementazione e validazione di nuovi meccanismi per rendere sicure le piattaforme basate su blockchain e smart contract, che sono sempre più utilizzate nei moderni centri urbani. In particolare, l'assegnista si concentrerà sull'individuazione di potenziali vulnerabilità negli smart contract eseguiti su blockchain, utilizzando varie tecniche di analisi come:

- **Code Review:** Revisione manuale e automatica del codice.
- **Security Testing:** Test unitari e di integrazione per verificare la sicurezza delle funzioni e dei moduli.
- **Fuzzing:** Generazione automatica di input casuali per rilevare comportamenti anomali.
- **Analisi Statica:** Analisi del codice senza esecuzione per trovare errori sintattici e semantici.
- **Analisi Dinamica:** Esecuzione controllata del codice per osservare comportamenti anomali.

L'assegnista dovrà sviluppare nuovi meccanismi di sicurezza per mitigare le vulnerabilità identificate e validare le soluzioni proposte. Il programma di formazione dell'assegno prevede le seguenti attività organizzate nel periodo di un anno:

- **Ricerca sullo Stato dell'Arte:** Analisi della letteratura e delle tecniche attuali di sicurezza per blockchain e smart contract.
- **Progettazione di Soluzioni:** Sviluppo di metodi innovativi per l'identificazione e la mitigazione delle vulnerabilità negli smart contract.
- **Sviluppo Software e Test sul Campo:** Implementazione pratica delle soluzioni progettate e verifica della loro efficacia tramite test sul campo.

Sono inoltre previste attività di gruppo orientate alla predisposizione di materiali e prototipi. Durante il periodo dell'assegno, l'assegnista acquisirà anche competenze significative in:

- **Redazione di Documenti Divulgativi:** Preparazione di relazioni e articoli per condividere i risultati della ricerca con la comunità scientifica e le aziende del settore.
- **Presentazione di Risultati:** Presentazione dei prototipi e dei risultati della ricerca a conferenze scientifiche e meeting di gruppo.