Borsa di studio dal titolo:
Studio sull'automazione del processo di reverse engeneering di protocolli industriali

Obiettivo del Progetto:
L'obiettivo principale di questo progetto di ricerca è analizzare e sviluppare tecniche avanzate di reverse engineering specificamente applicate ai protocolli industriali. Ciò include la decodifica di protocolli non documentati o protetti, l'identificazione di vulnerabilità di sicurezza e la proposta di metodologie per rafforzare la resilienza degli ambienti industriali contro attacchi informatici.

Descrizione:
In un contesto industriale, la sicurezza e l'affidabilità della comunicazione tra dispositivi è fondamentale. Molteplici protocolli, spesso proprietari o poco documentati, governano questi scambi di informazioni. Il progetto mira a esplorare tecniche di reverse engineering per analizzare tali protocolli, comprendendone il funzionamento interno, le strutture dati e i meccanismi di autenticazione e cifratura. L'analisi si concentrerà sui protocolli maggiormente utilizzati nell'automazione industriale, come Modbus, Profibus, e OPC UA, nonché su protocolli emergenti o meno conosciuti che presentano sfide uniche in termini di analisi e sicurezza.

Metodologia:
Fase 1: Raccolta dati e preparazione. Questa fase include la raccolta di campioni di traffico di rete reale e la configurazione di ambienti di test sicuri per l'analisi dei protocolli.
Fase 2: Reverse engineering. Applicazione di tecniche di reverse engineering, inclusi disassemblaggio, debugging e analisi di traffico di rete, per svelare i dettagli operativi dei protocolli target.
Fase 3: Analisi di sicurezza. Identificazione di vulnerabilità di sicurezza nei protocolli analizzati, sfruttando le informazioni ottenute durante il reverse engineering. Questo include la ricerca di punti deboli nel design, implementazione e configurazione.
Fase 4: Sviluppo di contromisure. Progettazione di raccomandazioni e strumenti per mitigare le vulnerabilità scoperte, migliorando così la sicurezza dei protocolli industriali.Impatto:
Il progetto contribuirà significativamente alla comprensione dei protocolli industriali e alla loro sicurezza. Fornendo strumenti e tecniche per il reverse engineering, si potrà non solo identificare e mitigare vulnerabilità esistenti, ma anche guidare lo sviluppo di nuove soluzioni di comunicazione industriale più sicure e resilienti.