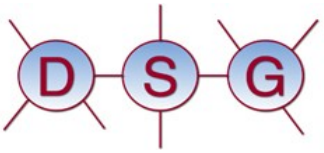

Proposta di Tesi

TITOLO:

Reverse Engineering Assistito e Verificabile con Ghidra MCP per l'Analisi di Binari IoT/Open-Source

DESCRIZIONE:

Il tema della tesi è progettare e sviluppare un sistema di Reverse Engineering automatico basato su Ghidra (https://github.com/nationalsecurityagency/ghidra) e su LLM. In particolare il sistema deve essere in grado di utilizzare un server MCP (Model Context Protocol), come ad esempio https://github.com/bethington/ghidra-mcp, consentendo all'LLM di interrogare in modo controllato i servizi esposti da Ghidra. In tal modo, il sistema è automaticamente in grado di raccogliere evidenze dal binario e produrre ricostruzioni strutturate di funzioni, componenti e possibili comportamenti di interesse.

Il sistema dovrà essere evidence-driven, cioè ogni conclusione dovrà essere supportata da interrogazioni esplicite a Ghidra, e dovrà lavorare su un task mirato e realistico, ad esempio: ricostruzione automatica di capability di binari IoT o utility di sistema, individuazione di entry points, uso di funzioni sensibili (rete, file system, parsing input, cifratura), e generazione di una scheda tecnica di sicurezza del binario.

I benchmark sul binary analysis con LLM, con task concreti e misurabili come code summarization, decompilation understanding e capability inference: BinMetric (https://www.ijcai.org/proceedings/2025/0858.pdf).

I. **0. Definizione del task**

   Studiare e costruire un mini-benchmark interno di task di reverse engineering assistito. Il task dovrà essere ristretto e chiaro, ad esempio: Function capability reconstruction (data una funzione, il sistema deve inferire se implementa parsing input, accesso a file, comunicazione di rete, cifratura/hash, autenticazione, gestione processi, ecc…), Entry-point to sink tracing semplificato, Binary security card generation (produrre una scheda strutturata del binario con componenti rilevanti per analisi security) ecc.. Volendo qualcosa di ispirazione da BinMetric…

II. **Progettazione dell'architettura del sistema**

Il compito è studiare e progettare un sistema basato su una pipeline come ad esempio:

a. MCP Client / Orchestrator
b. Planner (decide quali query fare a Ghidra in sequenza)
c. Evidence Ledger: archivio strutturato delle evidenze raccolte (funzione, tool usato, output sintetizzato, confidenza, ipotesi supportata) → ogni risposta finale del sistema deve essere tracciabile a evidenze esplicite, non solo a testo generato dal modello.
d. Hypothesis Builder: modulo che formula ipotesi intermedie sul comportamento di una funzione/binario.
e. Verifier: modulo che prova a confermare o smentire un'ipotesi richiamando altri tool Ghidra
f. Report Generator: produce output finale strutturato.

III. Sviluppo del prototipo

Lo studente dovrà realizzare un prototipo funzionante, implementando il client MCP e integrazione con un server Ghidra MCP open-source, sviluppando una libreria di azioni elementari, come ad esempio: get function list, decompile function, inspect xrefs, ecc. La logica di business deve definire una strategia di interrogazione, fino alla produzione di output strutturato (JSON o MD), adatto a essere letto da un analista umano o da altri moduli software.

IV. Esperimenti e Valutazione

Creare un prompt che chieda alle AI di analizzare una funzione di codice, usando il Context Pack. Chiedere di produrre una lista di potenziali vulnerabilità, ognuna con descrizione del problema, tracciamento (da dove arriva il dato pericoloso fino a dove causa danno), eventuale proposta di fixing.

V. Verifica e Confronto

L'obbiettivo finale è una valutazione ben progettata su un insieme limitato ma curato di binari/funzioni. È possibile realizzare il confronto tra modalità di analisi (ablativo di alcune parti), con diverse metriche da individuare sulla base del task.

Il sistema sarà basato su modelli LLM open source o ad accesso gratuito.

Referente universitario:

dott. Ing. **Gabriele Penzotti** (gabriele.penzotti@unipr.it)
Prof. Luca Veltri (luca.veltri@unipr.it)

Distributed Systems Group, Dipartimento di Ingegneria e Architettura