GIANLUCA CAPOZZI

Ingegnere Informatico

PROFILO

Studente di Dottorato
Laureato Magistrale in Engineering in Computer Science

PROGETTI

Studio, pianificazione, analisi e valutazione di soluzioni per la generazione di codice binario resistente all'analisi di similarità

PNRM SAFE

Supervisore: Prof. Leonardo Querzoni
Le attività svolte hanno interessato nella prima fase lo studio delle tecniche utilizzate per il confronto tra file in formato binario, focalizzandosi in particolare sulle tecniche basate sull'utilizzo di reti neurali utilizzate per produrre una rappresentazione vettoriale del binario ricevuto in input.
Nella seconda fase dell'attività si sono studiati i principali metodi utilizzati per la produzione di esempi avversari in diversi contesti, dalla classificazione di immagini fino al Natural Language Processing, cercando di capire come adattare soluzioni esistenti al contesto di model utilizzati per l'analisi di codice sorgente e/o binario.
Nella fase conclusiva si sono identificate e valutate delle tecniche, esistenti e non, in grado di produrre codice binario resistente all'analisi di similarità effettuata tramite modelli di reti neurali.
Attività principali:

- Studio di modelli di reti neurali per l'analisi di codice binario
- Studio dei principali metodi per la generazione di esempi avversari contro modelli di reti neurali
- Studio e valutazione dei principali metodi per la generazione di codice binario robusto all'analisi di similarità

Studio dei meccanismi di packing per il firmware di dispositivi di rete

Progetto Industriale

Supervisore: Prof. Leonardo Querzoni
Le attività svolte hanno interessato nella prima fase lo studio dell'operazione di disassembly di codice binario e gli strumenti che possono essere utilizzati per effettuare tale operazione, confrontando i tool che effettuano il disassembly utilizzando la tecnica linear traversal e tool che utilizzano la tecnica recursive traversal. Sono stati inoltre studiati anche alcuni framework in grado di effettuare un'analisi più approfondita.
La seconda fase dell'attività si è concentrata sullo studio delle diverse toolchain di compilazione utilizzate per la produzione di eseguibili.
Attività principali:

- Studio di tool per il disassembly (Radare2, IDApro, Ghidra, angr, BAP, MIASM)
- Studio di toolchain di compilazione per la produzione di eseguibili (GNU, AVR, LLVM) e formati di eseguibile

ESPERIENZE

Contratto di Prestazione Occasionale

Consorzio Interuniversitario nazionale per l'informatica "CINI"

Marzo 2021 - Agosto 2021 — Roma

Supervisore: Prof. Leonardo Querzoni

- Malware Analysis
- Studio delle toolchain di compilazione utilizzate per la produzione di eseguibili
- Studio sui meccanismi e gli strumenti per la compilazione e decompilazione del codice sorgente in ambito embedded systems

Borsista di Ricerca in Cybersecurity

Dipartimento di Ingegneria Informatica, Automatica e Gestionale, Università degli Studi di Roma "La Sapienza"

Settembre 2021 – Ottobre 2021 — Roma

Supervisore: Prof. Leonardo Querzoni

- Malware Analysis
- Analisi di codice sorgente e binario utilizzando modelli di reti neurali
- Adversarial Machine Learning

Ricercatore Visitatore

University College London - Department of Computer Science

Gennaio 2024 – Luglio 2024 | Londra

Supervisore: Prof. Lorenzo Cavallaro
- Analisi di codice sorgente e binario utilizzando modelli di reti neurali
- Adversarial Machine Learning

ISTRUZIONE

National Ph.D. in Artificial Intelligence

Dipartimento di Ingegneria Informatica, Automatica e Gestionale, Università degli Studi di Roma "La Sapienza"

Novembre 2021 – in corso | Roma

Advisor: Prof. Giuseppe Antonio Di Luna
Argomenti:
- Malware Analysis
- Analisi di codice sorgente e binario utilizzando modelli di reti neurali
- Adversarial Machine Learning per testare la robustezza di modelli utilizzati per l'analisi di codice sorgente e/o binario

Laurea Magistrale in Engineering in Computer Science

Dipartimento di Ingegneria Informatica, Automatica e Gestionale, Università degli Studi di Roma "La Sapienza"

Dicembre 2018 – Gennaio 2021 | Roma

Relatore: Prof. Leonardo Querzoni
Titolo della Tesi: *A study on the robustness of the SAFE system for binary similarity against adversarial coding attacks*
Voto: 110/110

Laurea Triennale in Ingegneria Informatica ed Automatica

Dipartimento di Ingegneria Informatica, Automatica e Gestionale, Università degli Studi di Roma "La Sapienza"

Settembre 2015 – Dicembre 2018 | Roma

Relatore: Prof. Leonardo Querzoni
Titolo della Tesi: *"iMedical: un'applicazione progettata per migliorare l'interazione tra medico e paziente"*
Voto: 97/110

ULTERIORI TITOLI

Abilitazione all'esercizio della professione di Ingegnere dell'Informazione

Università degli Studi di Roma "La Sapienza"

Novembre 2021 | Roma

DIDATTICA

Tutor per il corso Sistemi di Calcolo

Università degli Studi di Roma "La Sapienza"

A.A. 2021/2022 - A.A. 2022/2023 | Roma

Corso di Laurea Triennale in Ingegneria Informatica e Automatica

PUBBLICAZIONI

Journal

- **G. Capozzi**, D. C. D'Elia, G. A. D. Luna, and L. Querzoni, "Adversarial attacks against binary similarity systems," *IEEE Access*, vol. 12, pp. 161 247–161 269, 2024.

HARD SKILLS

Python Programming	●●●●●
Assembly x86	●●●●○
C Programming	●●●●○
Java Programming	●●●●○
Javascript	●●●○○
Ruby (Ruby on Rails)	●●●○○
Scala	●●○○○
Node.js	●●○○○
HTML, CSS, XML, jQuery, AJAX	●●●●○
SQL	●●●●○
Malware Analysis: Radare2, IDApro, Ghidra, x32dbg, Scylla, SysInternals	●●●●○
ML libraries: huggingface, numpy, keras, tensorflow, pytorch	●●●●●
PyCharm, Eclipse, NetBeans, IntellijIDEA, Android Studio, Visual Studio Code	●●●●●
Arduino IDE	●●●○○
MySQL, PostgreSQL, Firebase	●●●●○
Data Analysis	●●●○○
Unix OS	●●●●●
Windows OS	●●●○○

LINGUE

Italiano	●●●●●
Inglese	●●●●○
Spagnolo	●●○○○