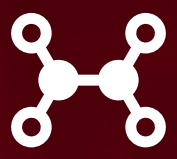

ZENROOM.ORG - DAL MODELLO MATEMATICO ALLA PRODUZIONE CON POCHI SFORZI

DENIS (JAROMIL) ROIO

DYNE.ORG

UNIVERSITÀ ROMA TRE
DIPARTIMENTO DI MATEMATICA E FISICA

MERCOLEDÌ 8 MARZO 2023

ORE 16.00

AULA M1

SEMINARIO DI ORIENTAMENTO

Zenroom.org - dal modello matematico alla produzione con pochi sforzi

Denis (Jaromil) Roio
DYNE.ORG

Abstract: La macchina virtuale "Zenroom" è un ambiente di esecuzione piccolo, sicuro ed estremamente portabile in grado di operare trasformazioni crittografiche avanzate come zero-knowledge proof e calcoli omomorfici in meno di 2MB di RAM. E' possibile integrarlo facilmente in C/C++, Python, Javascript, Golang, Rust e Java e le sue operazioni sui dati possono essere descritte in un linguaggio simile a quello umano chiamato Zencode.

In questo seminario scenderemo in dettaglio per osservare come è fatta all'interno Zenroom ed esploreremo anche le ragioni di alcune scelte: l'adozione di un dialetto di Lua come interprete di sintassi e quella di Milagro per le funzioni crittografiche primitive. Ma soprattutto vedremo come puo' lavorarci un matematico che sviluppa nuovi algoritmi usando uno script simile a Mathematica e mandandoli direttamente in produzione senza bisogno di traduzioni.
Il metodo di lavoro che abbiamo sviluppato in Dyne.org consiste nel rendere indipendente il lavoro dei crittografi matematici da quello degli ingegneri integratori, utilizzando proprio Zenroom in qualsiasi applicazione client e server.

Università Roma Tre
Dipartimento di Matematica e Fisica
Mercoledì 8 Marzo 2023
Aula M1, ore 16.00

Lo speaker: Denis Roio (Ph.D), meglio conosciuto nella comunità hacker come Jaromil, è il direttore tecnico della fondazione Dyne.org e di alcuni progetti faro per la commissione Europea finalizzati allo sviluppo di tecnologie di blockchain e privacy dei dati in città come Amsterdam, Barcellona ed Amburgo. Jaromil è l'autore di Zenroom, l'iniziatore della distribuzione Devuan GNU+Linux e di svariati altri software liberi ed open source.