POLITECNICO DI MILANO

PhD in INGEGNERIA DELL'INFORMAZIONE / INFORMATION TECHNOLOGY - 40th cycle

Research Area n. 1 - Computer Science and Engineering

THEMATIC Research Field: ADVANCED BINARY ANALYSIS TECHNIQUES FOR AUTOMATED SECURITY PATCHING AND VULNERABILITY MITIGATIONS

Monthly net income of PhDscholarship (max 36 months)
€ 1400.0 In case of a change of the welfare rates during the three-year period, the amount could be modified.

Context of the research activity	
Motivation and objectives of the research in this field	The candidate will develop and explore advanced techniques for binary rewriting, focusing on methods to manually and automatically patch binary applications with minimal disruption to their functionality and performance, including the addition of security mitigations such as stack canaries and control-flow integrity checks.
Methods and techniques that will be developed and used to carry out the research	Advanced binary analysis techniques, automated binary rewriting frameworks, and security mitigation strategies will be developed and applied to create robust methodologies for manual and automated patching of binary applications. These methods will facilitate precise modification, enhancement, and security hardening of compiled software, ensuring resilience against vulnerabilities and performance integrity.
Educational objectives	After the PhD programme, the student will have developed techniques in binary rewriting and automated patching, with a focus on enhancing software security and resilience. The candidate will gain expertise in advanced binary analysis, automated tool development, and the integration of security mitigations, preparing them to contribute to both academia and industry in the fields of software security, reverse engineering, and cybersecurity research.

Job opportunities	Cybersecurity is an attractive research and professionalarea. Graduates with expertise in this area can easily find jobs both in academia and in private organizations. There is an enormous request for professionals with security assessment skills.
Composition of the research group	1 Full Professors 1 Associated Professors 2 Assistant Professors 6 PhD Students
Name of the research directors	Prof. Stefano Zanero

Contacts
stefano.zanero@polimi.it

Additional support - Financial aid per PhD student per year (gross amount)	
Housing - Foreign Students	--
Housing - Out-of-town residents (more than 80Km out of Milano)	--

Scholarship Increase for a period abroad	
Amount monthly	700.0 €
By number of months	6

Additional information: educational activity, teaching assistantship, computer availability, desk availability, any other information

EDUCATIONAL ACTIVITIES (purchase of study books and material, including computers, funding for participation in courses, summer schools, workshops and conferences): financial aid per PhD student 5.707,20 Euro

TEACHING ASSISTANTSHIP: availability of funding in recognition of supporting teaching activities by the PhD student.
There are various forms of financial aid for activities of support to the teaching practice. The PhD student is encouraged to take part in these activities, within the limits allowed by the regulations.

COMPUTER AVAILABILITY:
1st year: Yes
2nd year: Yes
3rd year: Yes

PRIN PNRR/FARE "Firmware Analysis for vulneRability dEtection" cup D53D23008380006 -

id progetto: 202225BZJC

PRIN PNRR/SETA "Studying thE impact of anti-analysis Techniques in IoT security evAluations" cup D53D23017280001 - id progetto: P202233M9Z