Oggetto: Avviso pubblico per la presentazione di Proposte progettuali per la realizzazione di attività di ricerca industriale e sviluppo sperimentale relative al Partenariato Esteso SERICS (PE00000014), nell'ambito dello Spoke 3 "Attacks and Defences" (UNIVERSITA' DEGLI STUDI DI CAGLIARI) ammesso a finanziamento con Avviso Pubblico nr 341 del 15-02-2022 "Partenariati estesi alle università, ai centri di ricerca, alle aziende per il finanziamento di progetti di ricerca di base" – nell'ambito del Piano Nazionale di Ripresa e Resilienza, Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU – CUP: F53C22000740007 – Nomina della Commissione e dell'esperto esterno indipendente.

IL RETTORE

VISTO lo Statuto dell'Ateneo emanato con il DR n. 1396 del 12/06/2012 e ss.mm.ii, da ultimo con il D.R. n. 305 del 28/03/2022;

VISTA la Legge 7 agosto 1990 n. 241 - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

VISTO il Decreto Direttoriale 15 marzo 2022, n. 341 che ha emanato l'Avviso pubblico per la presentazione di Proposte di intervento per la creazione di "Partenariati estesi alle università, ai centri di ricerca, alle aziende per il finanziamento di progetti di ricerca di base" – nell'ambito del Piano Nazionale di Ripresa e Resilienza, Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU";

VISTA l'Iniziativa denominata "Serics - Security and Rights in Cyber Space" per la tematica 7, Cybersecurity, nuove tecnologie e tutela dei diritti, Proponente: SALERNO - Università degli Studi, alla quale l'Università degli Studi di Cagliari ha aderito e nella quale svolge il ruolo di Responsabile dello Spoke 3 "Attacks and Defences";

VISTO il proprio D.R. N. 151/2025 del 7 febbraio 2025, le cui premesse vengono integralmente richiamate in questo provvedimento, che ha emanato la procedura ad evidenza pubblica per il finanziamento, per la presentazione di Proposte progettuali per la realizzazione di attività di ricerca industriale e sviluppo sperimentale relative al Partenariato Esteso SERICS (PE00000014), nell'ambito dello Spoke 3 "Attacks and Defences";

Direzione per la ricerca e il territorio
Dirigente: Dott. Gaetano Melis
Via San Giorgio, 12 – 09124 Cagliari - Tel 070/6752063
pnrr@unica.it - protocollo@pec.unica.it - www.unica.it

VISTO in particolare l'articolo 4.1 dell'avviso – Processo di selezione - che prevede la nomina di una Commissione per la verifica preliminare delle proposte progettuali presentate e di un esperto esterno indipendente per la valutazione di merito;

VALUTATI i tempi per il termine delle attività progettuali;

CONSIDERATA pertanto, la necessità di procedere celermente con le attività di selezione e acquisita la disponibilità di un esperto esterno per la valutazione, in tempi brevi, delle proposte presentate;

SENTITO il Responsabile Scientifico per l'Università degli Studi di Cagliari nell'ambito del Partenariato Esteso SERICS (PE00000014);

PRESO ATTO che i componenti della Commissione e l'Esperto esterno indipendente per la valutazione di merito rilasceranno la prevista dichiarazione di assenza di conflitto di interessi;

VALUTATA la necessità di nominare la Commissione per la verifica preliminare delle proposte progettuali presentate e di un esperto esterno indipendente per la valutazione di merito delle proposte progettuali presentate in risposta all'Avviso emesso con il D.R. n. 151/2025;

DECRETA

ARTICOLO 1

Sono nominati, ai sensi dell'articolo dell'art. 4.1 – Processo di selezione - dell'Avviso pubblico, indicato in oggetto, componenti della Commissione per la verifica preliminare delle proposte progettuali presentate, i soggetti di seguito indicati:

- Prof. Giorgio Giacinto – Professore Ordinario - SSD IINF-05/A Sistemi di elaborazione delle informazioni – afferente alla Dipartimento di Ingegneria Elettrica ed Elettronica;
- Dott. Gaetano Melis – Dirigente – Direzione per la ricerca e il territorio;
- Dott.ssa Silvia Carta – Elevata Professionalità - Direzione per la ricerca e il territorio.

ARTICOLO 2

Direzione per la ricerca e il territorio
Dirigente: Dott. Gaetano Melis
Via San Giorgio, 12 – 09124 Cagliari - Tel 070/6752063
pnrr@unica.it - protocollo@pec.unica.it - www.unica.it

E' nominato, ai sensi dell'articolo dell'art. 4.1 – Processo di selezione - dell'Avviso pubblico, indicato in oggetto, Esperto esterno indipendente per la valutazione di merito delle proposte progettuali il Dott. Marco Balduzzi, di cui si allega il CV.

ARTICOLO 3

La Commissione e l'Esperto esterno sono autorizzati a utilizzare modalità telematiche per lo svolgimento dei lavori.

ARTICOLO 4

All'Esperto esterno sarà corrisposto un compenso di Euro 600,00. L'incarico dei componenti della Commissione è svolto a titolo gratuito.

Visto del Direttore Generale

Il Rettore
Prof. Francesco Mola
Sottoscritto con firma digitale

Marco Balduzzi, Ph.D.

Greater Bergamo Metropolitan Area

Summary

I am a team leader and principal researcher in computer and network security. I hold Ph.D. in system security from Télécom ParisTech and an M.Sc. in computer engineering from the University of Bergamo. My interests encompass all aspects of IT security, with a particular emphasis on real-world problems that affect systems and networks. Some topics that I specialize in are web security, code analysis, malware detection, cybercrime, online privacy, and ICS threats.

I have been involved in the security domain since 2002, with international experience in both industry and academia. With previous experience as a security engineer and a proven record of successful R&D projects, I am currently a technical research lead at Trend Micro.

With over 50 talks at major cybersecurity events such as RSA, Black Hat and Hack In The Box, I am considered a veteran speaker. I regularly engage with the research community and serve on the program committees of conferences and workshops. My work has been published in the proceedings of top peer-reviewed conferences such as NDSS, RAID, and ACSAC, and has been featured by distinguished media outlets such as BBC, CNN, Forbes, The Register, Slashdot, InfoWorld, and DarkReading.

As a free software sympathizer, I am involved in open-source projects and underground hacking communities. In my free time, I enjoy rock climbing, alpinism, and traveling.

My personal website is https://www.madlab.it

In a summary:
- Principal Researcher and Team Leader
- Researcher with 20+ peer-reviewed publications (papers and books)
- Veteran Speaker with 50+ conference talks (14 at Black Hat, 8 at HITB)
- Program Committee Member of conferences, journals and patent programs

Experience

Technical Research Lead

Trend Micro

Jan 2023 - Present (11 months)

I am a long-term member of Trend Micro's Forward Looking-Threat Research (FTR) team. This team consists of a top-notch, selected group of senior researchers that investigate problems affecting modern technologies and their use, with the goal of understanding the current threat landscape and anticipating future attacks. We regularly conduct both offensive and defensive research, and present our work in major conferences.

Within this group, I act as security expert, leading innovative research to success and contributing to better protect our users.

President and Co-founder

Berghem-in-the-Middle & No Hat

Jun 2017 - Present (6 years 6 months)

As a founding member and president in charge, I lead BITM in its mission of sharing knowledge, engagement with the security community, and organization the No Hat yearly conference.

Senior Security Researcher

Trend Micro

Apr 2012 - Dec 2022 (10 years 9 months)

I am halfway between academic and industrial research: On one side, I conduct scientific research aimed at publishing in peer-reviewed conferences; on the other side, I address the needs of an industrial environment, for example by conducting practical research, advising on internal R&D projects, acting as subject-matter expert, and contributing to the company's public outreach.

The team is responsible for investigating future threats, including the security of emerging technologies and user privacy, and for designing proof-of-concept solutions to detect and mitigate potential risks.

We actively collaborated in joint projects with major research groups in universities and LEA/CERT organizations, and we regularly presented at both academic and industrial conferences.

Senior Security Researcher

Nov 2008 - Nov 2016 (8 years 1 month)

I worked (as PhD first and Senior Research later) in iSecLab (https://iseclab.org/) by conducting research in the wide domain of privacy and security. Our goal consisted of investigating current and future threads and propose cutting-edge countermeasures to be published in conference papers (proceedings) and presented in conferences.

Senior Security Engineer

BMC Software

Jan 2008 - Oct 2008 (10 months)

As security expert, I was responsible of researching, implementing and supporting the development of the Precision Vulnerability Management solution. I held the research and development of the security scanner and its vulnerability tests. During my stay, I replaced a strong portion of the existing code with the NMap Security Scanner solution that we licensed and adopted.

Network Security Researcher

SAP

Sep 2007 - Dec 2007 (4 months)

I worked in the Security & Trust group of SAP Labs France by taking part in the WASP European Project. The goal consisted of integrating Wireless Sensor Networks in Enterprise Applications by satisfying tight availability and security requirements.

Security Researcher and Developer

secunet Security Networks AG

Aug 2006 - Jul 2007 (1 year)

As R&D engineer, I researched and implemented an antivirus prototype which was integrated within a hypervisor. More information are included in a book that I published on the topic and is available on Amazon (titled "Security by virtualization: A novel antivirus for personal computers").

Briefly: We modified the QEMU virtual machine to intercept any disk I/Os so to build a consistent cache used to scan for malware. The prototype was implemented in C and Bash under Linux.

Security Consultant

Mar 2006 - Aug 2006 (6 months)
As part of Emaze's staff I conducted security consulting services such as penetration testing, vulnerability assessment, computer forensics, system hardening, architecture designing, compliance and training.

Security Consultant

Secure Network
Jan 2004 - Dec 2005 (2 years)
As part of Secure Network's staff I conducted security consulting services such as penetration testing, vulnerability assessment, computer forensics, system hardening, architecture designing, compliance and training.

Network Security Researcher

ICT Consulting
Jun 2004 - Nov 2004 (6 months)
During this internship I designed a router-based intrusion detection system (IDS) that I implemented on a Cisco 2600 device. The idea was to integrate a network sensor into existing device nodes to detect distributed security issues such as DoS attacks, portscans, SPAM activities and botnets.

Education

EURECOM

Doctor of Philosophy - PhD, Computer and Information Systems Security/Information Assurance
2008 - 2011
Title of the Thesis: Automated Measurements of Novel Internet Threats.

In this thesis, we advance the state-of-art in large scale testing and measurement of Internet threats. We research into three novel classes of security problems that affect Internet systems that experienced a fast surge in popularity (i.e., ClickJacking, HTTP Parameter Pollution, and commercial cloud computing services that allow the outsourcing of server infrastructures). We introduce the first, large scale attempt to estimate the prevalence and relevance of these problems on the Internet.

Università degli Studi di Bergamo

Master of Science in Computer Engineering - MSc, Computer Engineering
2001 - 2007

In July 2004, I earned my B.Sc. with a thesis titled "A new model of Intrusion Detection System: The Router-IDS". In this work, I introduced a context-based IDS, which correlates host-based and network-based information to reduce the number of FPs.

In March 2007, I earned my M.Sc. with a thesis titled "Security by Virtualization: a novel antivirus for personal computers". In this work, I proposed a novel AV that sits in a hypervisor and intercepts raw I/O disk-sector to scan for malware.

Skills

Cyber Threat Intelligence (CTI) • Security Research • Team Leadership • People Management