

Curriculum Vitæ

UNIVERSITÀ DEGLI STUDI DI MILANO

UNIVERSITÀ DEGLI STUDI DI MILANO Procedura di selezione per la chiamata a professore di I fascia da ricoprire ai sensi dell'art. 18, comma 1, della Legge n. 240/2010 per il settore concorsuale 01/B1 INFORMATICA - , (settore scientifico-disciplinare INF/01 presso il Dipartimento di informatica Giovanni degli Antoni, (avviso bando pubblicato sulla G.U. n. 35 del 30/04/2024) - Codice concorso 5534

INFORMAZIONI PERSONALI

Nome e Cognome: Andrea Lanzi
Data di Nascita: 14 Gennaio 1974
Home Page: lanzi.di.unimi.it
Email Address: andrea.lanzi@unimi.it

FORMAZIONE

Ph.D. degree in computer science **2009**
Ph.D. degree in Computer Science at *Dipartimento di Informatica e Comunicazione (DICO) – Università degli Studi di Milano*.

M.Sc. Degree in Computer Science **2004**
M.Sc. degree in Computer Science from *Dipartimento di Informatica – Università di Bicocca Milano* (final grade of 110/110 *cum laude*). Thesis titled “Analysis, Design and Realization of a Trusted Computing Platform Emulator”.

INCARICHI

Professore Associato (Università degli Studi di Milano) 2020-Now

Sono attualmente Professore Associato presso Il dipartimento di computer science dell'università degli studi di Milano, italia.

Assistant Professor (Università degli Studi di Milano) 2014-2020

Dal Gennaio 2014, sono stato Assistant Professor presso il dipartimento di Computer Science dell'Università degli studi di Milano, italia.

Researcher (Fellowship EURECOM) 2010

Dall'Aprile 2010, sono stato Senior Researcher presso il Computer Security Lab, Gestito dal professore Davide Balzarotti, dell'istituto Eurecom, Sophia Antipolis , France EU.

Post Doctoral Fellow 2009

Dall'Aprile 2009, sono stato Post-Doc presso il Computer Security Lab, Gestito dal professore Engin Kirda, dell'istituto Eurecom, Sophia Antipolis , France EU.

Employed at Georgia Tech, US, (Fellowship Georgia Tech) 2008

Dal febbraio 2008 sono impiegato come Visiting PhD student presso l'Università di Georgia Tech GATech (GA) negli Stati Uniti, nel laboratorio GTISC guidato dal Prof. Wenke Lee

Visiting Ph.D student at Georgia Tech 2007

Dal febbraio 2007 sono impiegato come Visiting PhD student presso l'Università di Georgia Tech GATech (GA) negli Stati Uniti, nel laboratorio GTISC guidato dal Prof. Wenke Lee.

ATTIVITÀ DI RICERCA

Attualmente sono Professore Associato presso il Dipartimento di Informatica dell'Università degli Studi di Milano, in Italia, dove dirigo un laboratorio di sicurezza chiamato LaSER (Laboratorio di sicurezza dei sistemi e delle reti). Sono interessato a diversi aspetti della sicurezza informatica. In particolare, il

mio principale campo di ricerca riguarda i sistemi di rilevamento delle intrusioni host (HIDS), l'exploitation del software contenente degli errori di memoria, il reverse engineering, l'analisi dei malware e forense attraverso tecniche di Machine Learning. Negli ultimi anni ho principalmente studiato l'applicazione di tecniche di emulazione/virtualizzazione e di compilazione per l'analisi e la rilevazione dei malware nel contesto di Android. Inoltre, ho lavorato all'analisi di ampi set di dati di malware per investigare il comportamento delle attuali minacce informatiche e il tema degli attacchi di tipo side-channel.

Più in generale la mia ricerca si concentra principalmente sulla sicurezza dei sistemi. Sono sempre stato attratto dalla ricerca in questo campo poiché richiede generalmente di attraversare i confini di diverse discipline interessanti dell'informatica come i sistemi operativi, le architetture informatiche e le reti, i compilatori e i linguaggi di programmazione e i sistemi distribuiti. Recentemente è diventato ancora più interessante esplorare altri argomenti, come l'analisi dei dati e, più in generale, il machine learning applicato alla cybersecurity. L'obiettivo del mio lavoro è affrontare problemi stimolanti e fornire soluzioni per risolverli. Di seguito sono evidenziati alcuni dei settori in cui ho avuto il piacere di fare ricerca e di delineare alcune delle mie prime idee e direzioni per la ricerca futura.

Bug Finding. La nostra linea di ricerca si concentra sulla protezione del software e la scoperta di bug mediante l'utilizzo di tecniche di analisi dei programmi, come l'analisi statica, il fuzzing e l'analisi dinamica. Lo scopo è quello di identificare i bug nelle applicazioni in modo da poterli correggere prima che vengano sfruttati da hacker o malware. L'analisi statica valuta il codice sorgente o l'eseguibile senza eseguire il programma, mentre il fuzzing testa il software con dati di input casuali. L'analisi dinamica, invece, esegue il programma e monitora il suo comportamento. Con queste tecniche, siamo in grado di identificare vulnerabilità e difetti del software, migliorando la sicurezza delle applicazioni per i nostri utenti. In generale, il problema aperto principale che stiamo affrontando in questa linea di ricerca è quello di sviluppare tecniche che combinino in modo ottimale diverse tecniche di analisi, in modo da migliorare l'efficienza e l'efficacia della protezione del software. Inoltre, l'evoluzione dei linguaggi di programmazione e degli ambienti di esecuzione richiede una costante attenzione e aggiornamento delle tecniche di analisi per garantire la massima sicurezza delle applicazioni.

Neural Program Analysis. La Neural Program Analysis è una tecnica di analisi statica dei programmi che utilizza le reti neurali per migliorare la precisione dell'analisi e l'identificazione di bug. In particolare, questo approccio cerca di superare le limitazioni delle tecniche tradizionali di analisi statica, che spesso non sono in grado di analizzare programmi complessi e non possono rilevare errori di logica. La Neural Program Analysis si basa sull'idea che i modelli di apprendimento automatico possano essere addestrati su grandi quantità di dati per rilevare e correggere gli errori nei programmi. Tuttavia, esistono ancora numerosi problemi aperti in questo campo, tra cui la necessità di raffinare i modelli di apprendimento automatico per adattarsi a programmi più complessi e la difficoltà di interpretare le decisioni prese dalle reti neurali. Inoltre, la Neural Program Analysis richiede un alto grado di expertise sia nell'analisi dei programmi che nell'apprendimento automatico, rendendola ancora una tecnica di nicchia. Tuttavia, i risultati finora ottenuti sono molto promettenti e la Neural Program Analysis potrebbe diventare una tecnica sempre più importante per la sicurezza del software nei prossimi anni.

Side-Channel Attacks. I side-channel attack sono una tecnica utilizzata per violare la sicurezza dei sistemi crittografici. Questa tecnologia sfrutta informazioni che possono essere ottenute da fonti esterne al sistema, come la corrente elettrica, la radiazione elettromagnetica o il suono, per estrarre informazioni sensibili dal dispositivo in questione.

Uno dei principali problemi riguarda la difficoltà di proteggere il dispositivo da tutti i possibili canali di side-channel attack. I dispositivi crittografici devono essere progettati per resistere alle tecniche di side-channel attack, ma non tutti i canali possono essere previsti in anticipo. Ciò significa che anche i dispositivi più sicuri potrebbero essere vulnerabili a nuove tecniche di attacco in futuro. Inoltre, le tecniche di side-channel attack richiedono un alto livello di expertise tecnica e specializzazione, rendendo difficile l'implementazione di contromisure efficaci. Le contromisure sono spesso costose e possono ridurre le prestazioni del sistema, il che limita la loro applicabilità.

Nonostante questi problemi aperti, è importante continuare a sviluppare tecniche di protezione contro i side-channel attack per mantenere la sicurezza dei sistemi crittografici. Ci sono diverse soluzioni possibili, tra cui l'uso di tecniche di mascheramento e il miglioramento della progettazione dei circuiti crittografici. Il nostro gruppo è attivo in questa tematica e sta lavorando con

aziende che operano direttamente sulla parte HW dei vari dispositivi.

Participation/Organization as a Program Committee Member of Conferences

Committee Member: Annual Computer Security Applications Conference (ACSAC) anni [2016, 2017, 2018, 2019, 2020, 2021, 2023] (Second-tier Conference)

Committee Member USENIX Security Symposium (USENIX) anno: [2017, 2021, 2022, 2023, 2024] (Top Conference in Security).

Committee Member ACM Conference on Computer and Communications Security (CCS) anni : [2015, 2016, 2017, 2022, 2023] (Top Conference in Security).

Committee Member DFRWS Conference Forensic Conference USA dagli anni [2014-2020, 2022] (Top conference in Forensic).

Committee Member: The International Symposium on Research in Attacks, Intrusions and Defenses (RAID) anni: [2012, 2013, 2015, 2016, 2017, 2019, 2020, 2021] (Second-tier Conference)

Committee Member EUROSEC, European Workshop On System Security anni: [2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019]

Committee Member USENIX WOOT Workshop on Offensive Technologies anno 2015

Committee Member “ARES International Conference on Availability, Reliability and Security”, anni: [2021, 2023]

Committee Member: ”SecureComm 2021 - 17th EAI International Conference on Security and Privacy in Communication Networks”

Committee Member Conference on Detection of Intrusions and Malware Vulnerability Assessment (DIMVA) anni [2012-2017, 2019, 2022] (Second-tier Conference)

Committee Member ACM Asia Conference on Computer and Communications Security (ASIACCS) anni [2017, 2018, 2021, 2022] (Second-tier Conference)

Organizer (Ruolo: co-chair) conference Proceedings of the 13th European on Systems Security, EuroSec@EuroSys 2020, Heraklion, Greece, April 27, 2020. ACM 2020, ISBN 978-1-4503-7523-8. <https://concordia-h2020.eu/eurosec-2020/>

Organizer (Ruolo: program-chair) conference Proceedings of the 14th EuroSec European on Systems Security, EuroSec@EuroSys 26 April , 2021 â Edinburgh, Scotland, UK. ACM 2021. <https://concordia-h2020.eu/eurosec-2021/>

Organizer (Ruolo: co-chair) conference for security track on IEEE International smart cities conference (ICS2), Trento, 2016 Italy. <http://events.unitn.it/en/isc2-2016/isc2-organization>.

Organizer (Program Chair, General Chair) conference CARDS 2019 - 11th EAI International Conference on Cyber Attacks Response and Defense (formerly ICDF2C)
<https://cards-conf.eai-conferences.org/2019/organizing-committee/>

Direzione/Partecipazione a comitati editoriali di Riviste

- Associated Editor: ACM Transactions on Transactions on Privacy and Security (TOPS) is devoted to the study, analysis, and application of information security and privacy. <https://dl.acm.org/journal/tops/editorial-board>.
<https://dl.acm.org/journal/tops>. (2021-Now)
- Guest Editor: ACSAC 2019 special Issue: Autori: “Roberto Perdisci, Martina Lindorfer, Adam Doupè, Andrea Lanzi, Alexandros Kapravelos, Gianluca Stringhini” Journal: Digital Threats: Research and Practice (<https://dl.acm.org/doi/fullHtml/10.1145/3437251>).
- Guest Editor: Advanced Techniques for Memory Forensics Analysis. Mob. Networks Appl. 25(1): 234-235 (2020)
<https://dblp.org/rec/journals/monet/Lanzi20>,
<https://link.springer.com/article/10.1007/s11036-019-01439-9>
- Associated Editor: “Journal of Information Security and Application” Journal of Information Security and Applications (JISA) focuses on the original research and practice-driven applications with relevance to information security and applications. (2014-2016)

- Attività di revisione al journal ACM Transactions on Embedded Computing Systems (TECS)
- Attività di revisione al journal IEEE Transactions on Dependable and Secure Computing (TOPS)
- Attività di revisione al journal ACM Transactions on Internet Technology (TOIT)
- Attività di revisione al journal IEEE Transactions on Information Forensics and Security (TIFS)

Responsabilità Scientifiche in Progetti di Ricerca

- Ruolo: Principal Investigator. Titolo: “ Global Combat Air Programme (GCAP)”, Progetto a livello Nazionale/Militare per la progettazione “C.03 Sviluppo di un Separation Kernel Hypervisor per sistemi avionici di sesta generazione” insieme a Leonardo. Nel Progetto oltre Università degli Studi di Milano sono coinvolte, Università di Sant’Anna di Pisa e Università di Trento, 2023-Now.
- Ruolo: Membro. Titolo: “DATA GOVERNANCE AND DATA PROTECTION” Spoke 10, Progetto PNRR 2023, PE 7.
- Ruolo: Membro. Titolo: “Sovereign Edge-Hub: Un’Architettura cloud-edge per la sovranità digitale nelle scienze della vita” SOV-EDGE-HUB LINEA STRATEGICA DI ATENEO (LSRA): 4 Sicurezza informatica/Cloud (PNRR) finanziato per 175.000 euro (2022)
- Ruolo: Principal Investigator (PI), Progetto finanziato da CISCO US, tipo di bando: Internazionale (Faculty Award), dal titolo “CodeKeeper: Validating Software Integrity on Firmware Images”. definito nell’ambito della sicurezza degli embedded system. Il Consorzio è formato da tre principali professori con Reputation Internazionale tra cui Il Professor Cavallaro di University College of London (UCL), Professor Pierazzi King’s College London (KCL), Professor Long Lu Northeastern University of Boston, US, e due ricercatori attivi nella parte sperimentale e di progettazione. Il progetto è stato finanziato con 100.000\$ e prevede 1 anno e mezzo di attività nel 2021-2022.

- Ruolo: Principal Investigator (PI): Progetto finanziato dalla ditta MBDA Missile System (Partner italiana: <https://www.mbdacareers.it/chi-siamo/>) nel bando internazionale di Open Innovation 2019-2020. Titolo del progetto: “Studio e Analisi dello stato dell’arte degli attacchi Side Channel in ambito HW security”. Il Consorzio è bilaterale: da una parte l’Università degli studi di Milano dall’altra la ditta di security pattern (<https://www.securitypattern.com/>) di Guido Bertoni che opera nella sicurezza degli embedded system.
- Ruolo: Principal Investigator (PI) Progetto finanziato Ministero degli Affari Esteri e Della Cooperazione Internazionale (MAECI) nel bando: Bando di Grande Rivelanza Italia-USA 2019-2021. Titolo del progetto: “Software Execution Environment Protection - acronimo: SEEP” Role: ”Principal Investigator”. Il Consorzio è bilaterale: da una parte l’Università degli studi di Milano dall’altra Northeastern University of Boston, US e in particolare dal Professor Long Lu. Inoltre per il progetto sono stati coinvolti diversi studenti di dottorato sia nell’unità di Milano che nell’unità di Boston Il Finanziamento è annuale dal 2019-2021 e di circa 120.000 euro.
- Ruolo: Principal Investigator (PI) Progetto finanziato dall’università degli studi di Milano (Internal Funding) dal titolo “Sentinel: Situational awareness in critical Infrastructure Environment”. Il Consorzio è formato da sette professori interdipartimentali. In particolare sono coinvolti 3 dipartimenti: Informatica, Matematica, Giurisprudenza e diversi studenti di dottorato. Il progetto è stato finanziato con 30.000 euro e prevede 1 anno e mezzo, attualmente esteso a 2 anni di attività con l’intenzione poi di sottomettere un progetto più ampio EU H2020.
- Ruolo: Membro. Progetto finanziato Ministero degli Affari Esteri per la raccolta di progetti congiunti tra Italia e Israele nell’ambito dell’Accordo di Cooperazione nel campo della Ricerca e dello Sviluppo Industriale, Scientifico e Tecnologico; Programma scientifico e tecnologico Italia - Israele (Track scientifico 2015) - Area di ricerca: Cyber Security. Titolo del progetto: “ PACS Privacy-aware Cyber-security”. Finanziamento totale 100.000 Euro
- Ruolo: Membro. Finanziato da: ANR - France National Research Agency

- 2014 Development of a new malware protection product against exploitation techniques. Questo progetto ha previsto la progettazione di un sistema di protezione contro le varie tecniche di attacco utilizzate dai malware. (2013-2014)
- Ruolo: Membro. Progetto finanziato Dalla Comunità Europea nell'ambito del programma: Seventh Framework Programme (FP7) Titolo del progetto: "Syssec: System Security for Europe" Role: Member. Il Consorzio è composto da diversi gruppi di ricerca europea: Eurecom Institute, VU University Amsterdam, Bochum university in Germany. Il progetto è durato dal 2010-2014.

Formale attribuzione di incarichi di insegnamento o di ricerca (Fellowship)

- Assunto come Senior Research Engineer presso l'istituto di ricerca francese EURECOM, Francia EU, **Fellowship Eurecom: dal 2009-2013.**
<http://www.eurecom.fr/en/people/lanzi-andrea>. EURECOM is considered one of the world's strongest universities in Computer Science Information. In the security field of security Eurecom is considered one of the best EU research places.
- Assunto come research visiting scholar presso l'università Georgia Tech, Atlanta US, nel laboratorio Gtisc diretto dal professor Wenke Lee. Sono stato assunto come researcher dove mi sono occupato di ricerca pubblicando più di 6 paper in differenti top conference, mi sono occupato principalmente della direzione del gruppo di ricerca che faceva capo alla tematica di Malware Analysis. **Fellowship Georgia tech 2008-2009.** Georgia Tech rappresenta una delle top-10 università in US.

Conseguimento di premi e riconoscimenti per l'attività scientifica

- Industry Award: Forensics Tool: Actaeon è uno strumento basato sulla nostra pubblicazione Mariano Graziano, Andrea Lanzi and Davide Balzarotti. "Hypervisor Memory Forensics" 16th Conference Research in Attacks, Intrusions and Defenses, RAID 2013, St. Lucia : Actaeon ha vinto First Prize for volatility Contest. <http://volatility-labs.blogspot.it/2013/08/results-are-in-for-1st-annual.html> (with Actaeon, Intel VT-x introspection)

- Best Paper Award: Babak Rahbarinia, Roberto Perdisci, Andrea Lanzi, Kang Li. “PeerRush: Mining for Unwanted P2P Traffic”. 10th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, DIMVA 2013, Berlin, Germany, <https://www.eurecom.fr/en/research/results-research/awards>
- Best Student Paper Award: Monirul Sharif, Andrea Lanzi, Jonathon Giffin, and Wenke Lee “Automatic Reverse Engineering of Malware Emulators” In Proceedings of The 2009 IEEE Symposium on Security and Privacy (Oakland 09), Oakland, CA, May 2009.
<http://www.ieee-security.org/TC/SP2009/program.html>
- Affiliazione Eurecom Institute, France [2009-2013] EURECOM is considered one of the world’s strongest universities in Computer Science & Information Systems being ranked 551/600 worldwide in 2019 improving to the rank 501/550 in 2021. EURECOM was evaluated by Quacquarelli Symonds (QS) regarding the key pillars, which distinguish a world class university.
- Affiliazione University of Georgia Tech (GATECH), Atlanta, US [2008-2009] Georgia tech è tra le top-10 US university
<https://news.gatech.edu/news/2021/09/13/georgia-tech-ranks-among-top-universities-us-news-world-reports-list-best-colleges>.

Seminari

- Invited Talk “Security of Embedded System”, University of Auckland, New Zealand, February 2017.
- Invited Talk “Detecting exploitation Techniques”, University of Technology and Economics, Budapest, Hungary, November 2015.
- Invited Talk, “Heap Spraying Attacks Survey”, at Georgia Tech University, Atlanta US, August 2015.
- Invited Talk, “Detecting Heap Spraying”, at Stony Brook University, NY, US, August 2015.
- Invited Talk “A Quantitative Study of Accuracy in System Call Based Malware Detection”, at INRIA, Rennes, France, 2014.

- Invited Talk “Hypervisor Memory Forensics”, at Royal Holloway University of London, UK, 2014.
- Invited Talk “Future Malware Research” at the University of Kent UK, April 2012.
- Invited Talk “Future Malware Research” at Eurecom Institute Sophia Antipolis, France, April 2011.
- Presentazione dell’articolo: Autori: Luca Buccioli, Stefano Cristalli, Edoardo Vignati, Lorenzo Nava, Daniele Badagliacca, Danilo Bruschi, Long Lu, and Andrea Lanzi. Titolo: “JChainz: Automatic Detection of Deserialization Attacks in the Java Environment” in SMT workshop collocato con la Conferenza ESORICS 2022, Copenhagen, Denmark.
- Presentazione Articolo: Autori: Stefano Cristalli, Long Lu, Danilo Bruschi, Andrea Lanzi Titolo: “Detecting (absent) app-to-app authentication on cross-device short-distance channels.” ACSAC Conference 2019, Puerto Rico, USA.
- Presentazione dell’articolo Autori: Stefano Cristalli, Edoardo Vignati, Danilo Bruschi, Andrea Lanzi Titolo: “Trusted Execution Path for Protecting Java Applications Against Deserialization of Untrusted Data.” RAID Security Conference 2018, Crete, Greece.
- Presentazione dell’articolo: “Subverting Operating System Properties Through Evolutionary DKOM Attacks” , Autori: Mariano Graziano, Lorenzo Flore, Andrea Lanzi, Davide Balzarotti, conferenza Detection of Intrusions and Malware, and Vulnerability Assessment: 13th International Conference, DIMVA 2016, San Sebastián, Spain, July 7-8, 2016, Proceedings.
- Presentazione dell’articolo: “Improving Mac OS X Security Through Gray Box Fuzzing Technique”, Autori: Stefano Bianchi Mazzone, Mattia Pagnozzi, Aristide Fattori, Alessandro Reina, Andrea Lanzi, Danilo Bruschi, Conferenza: EUROSEC 2014, Amsterdam, NL.
- Presentazione dell’articolo: “Hypervisor memory forensics” Autori: Mariano Graziano, Andrea Lanzi, Davide Balzarotti Conferenza:The 13 th

International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2013).

- Presentazione dell'articolo: "Thwarting Real-Time Dynamic Unpacking"
Autori: Leyla Bilge, Andrea Lanzi, Davide Balzarotti, Conferenza: at the European Workshop on System Security (EUROSEC) - Salzburg, April 2011.
- Presentazione dell'articolo: "AccessMiner: Using System-Centric Models for Malware Protection", Autori: A Lanzi, D Balzarotti, C Kruegel, M Christodorescu, E Kirda, Conferenza: at the 17th ACM Conference on Computer and Communications Security (CCS 2010) , CCS 2010 Chicago, USA.
- Presentazione dell'articolo: "Secure in-vm monitoring using hardware virtualization" autori: MI Sharif, W Lee, W Cui, A Lanzi Conferenza: Proceedings of the 16th ACM conference on Computer and communication (CCS 2009), USA.
- Presentazione dell'articolo: "Static Analysis on x86 Executable for Preventing Automatic Mimicry Attacks", Autori: Danilo Bruschi, Lorenzo Cavallaro, Andrea Lanzi, alla conferenza International Conference IEEE, (DIMVA 2007) Lucerne Switzerland July 12-13 2007.
- Presentazione dell'articolo: "An Efficient Technique for Preventing Mimicry and Impossible Paths Execution Attacks" autori: Danilo Bruschi, Lorenzo Cavallaro, Andrea Lanzi, conferenza International on Information Assurance IEEE(WIA 2007), April 11-13, 2007, New Orleans, Louisiana, USA.
- Presentazione dell'articolo: "Diversified Process Replicae for Defeating Memory Error Exploits" Autori: Danilo Bruschi, Lorenzo Cavallaro, Andrea Lanzi Conferenza: IEEE International Performance, Computing, and Communications Conference, USA, 2007.
- Presentazione del articolo "Replay attack in TCG specification and solution" Autori: D Bruschi, L Cavallaro, A Lanzi, M Monga Conferenza: 21st Annual Computer Security Applications Conference (ACSAC'05), USA.

- **Cicli di Seminari CyberSecurity.** Ho organizzato cicli di seminari per gli studenti universitari per gestire la squadra di cyberchallenge per le gare di cybersecurity a livello nazionale. In particolare, ho tenuto questi seminari nei tre anni accademici 2017/2018, 2018/2019 e 2019/2020 2021/2022 di 48 ore all'anno, sulla parte di difesa/attacchi.
- **4EU+ online seminars on “Security, Privacy, and Data Protection”** Organized by: 4EU+ Flagship 3 Coordinators: Prof. Vincenzo Piuri & Prof. Giulio Vistoli, University of Milan
<https://iebil.di.unimi.it/4EU+SPDPSeminars/index.html>.

Responsabilità di Studi e Ricerche Scientifiche

- Sono stato commissionato in qualità di review per la valutazione del ERC's Starting Grant 2019 call all'interno del panel PE6 (Computer Sciences and Informatics), gestito dal Prof. Pierre Wolper.
- Sono stato commissionato dalla Commissione Europea come “esperto di sicurezza” nella consulenza definita della mansione di peer reviewer nel progetto H2020 ENUNITY nell'ambito della cybersecurity:
<https://cordis.europa.eu/project/id/740507/it>. Il mio ruolo è stato quello di revisore in tutte le fasi dle progetto. (2018-2019)
- Sono stato commissionato dalla Commissione Europea in qualità di security expert per la valutazione di sicurezza del progetto di passaporto elettronico europeo. Committee di analisi: Prof. Andrea Lanzi, Prof. Lorenzo Cavallaro (Royal Holloway, UK), Prof. Dr. Srdjan Capkun (ETH Zurich), Dr. Claude Castelluccia (INRIA), Prof. Josep Bigun (Halmstad University) (2016-2017)
- Sono stato commissionato dalla Commissione Europea come “esperto di sicurezza nella consulenza del seguente progetto: Access Rights for CISE (Common Information Sharing Environment). European Commission Maritime Affaris and Fisheries”.(2014-2015)
- Sono stato attualmente incaricato dal consorzio del progetto European project H2020 CYRENE (Grant Agreement No. 952690) in qualità di

membro dell' advisor board. Il mio compito principale nel progetto è quello di visionare le varie attività e intervenire in qualità di security expert.

Soggiorno All'Estero & Fellowship presso Università di Prestigio

- Nel corso del 2017 ho avuto l'opportunità di essere ospite presso **l'Università di Auckland, situata in Nuova Zelanda**, in qualità di visiting professor su un progetto di Software Obfuscation. Durante il mio soggiorno, ho avuto modo di lavorare a stretto contatto con la facoltà e i ricercatori dell'ateneo, contribuendo al loro programma di ricerca e condividendo le mie conoscenze e competenze nel campo della Software Obfuscation. Questa esperienza si è rivelata molto gratificante e ha rappresentato un'importante occasione per lo sviluppo della mia carriera accademica e professionale.
- Dal 2009 al 2013 ho avuto l'onore di essere assunto come Senior Research Engineering presso l'istituto francese **EURECOM - Fellowship**, un prestigioso centro di ricerca e istruzione superiore specializzato in tecnologie avanzate della comunicazione. Durante questi anni, ho avuto la possibilità di lavorare a stretto contatto con esperti di spicco nel settore della ricerca scientifica, partecipando attivamente alla conduzione di importanti progetti di ricerca e sviluppo. In particolare, il mio ruolo mi ha permesso di contribuire alla progettazione e implementazione di soluzioni innovative in diversi campi, tra cui sicurezza informatica, intelligenza artificiale e Internet delle cose. Il mio lavoro all'EURECOM ha rappresentato un'esperienza estremamente formativa e stimolante, che ha contribuito in modo significativo alla mia crescita professionale e personale.
- Nel periodo compreso tra il 2007 e il 2009, ho avuto l'opportunità di fare un'esperienza di visiting presso **l'Università Georgia Tech, situata negli Stati Uniti - Fellowship**. In particolare, ho lavorato all'interno del Security Lab Gtisc, un'importante struttura di ricerca gestita dal rinomato professore Wenke Lee. Durante il mio soggiorno, ho avuto modo di collaborare attivamente con i ricercatori dell'università, contribuendo alla conduzione di importanti progetti di ricerca nel campo

della sicurezza informatica. In particolare, ho lavorato sulla progettazione e l'implementazione di soluzioni innovative volte a migliorare la sicurezza dei sistemi informatici. Questa esperienza si è rivelata estremamente formativa e ha rappresentato un'occasione unica per approfondire le mie conoscenze e competenze nel campo della sicurezza informatica, acquisendo al contempo nuove prospettive e punti di vista sulla materia.

Collaborazioni Scientifiche con gruppi Internazionali

Nel corso della mia carriera, ho avuto l'opportunità di coordinare e guidare numerose collaborazioni internazionali, ricoprendo un ruolo di leader e coordinatore in diversi progetti di ricerca. Un esempio significativo è la collaborazione con l'Università di Northeastern a Boston, USA, sotto la guida del Prof. Long Lu, focalizzata sull'analisi dei protocolli di scambio dati utilizzati nelle comunicazioni short-distance come il Bluetooth. Questo progetto, finanziato dal MAECI, aveva l'obiettivo di costruire un sistema automatico di rilevamento dei processi di autenticazione tra le app nei sistemi Android. Il mio ruolo è stato cruciale nel coordinare le attività di ricerca, assicurando una sinergia efficace tra i vari team coinvolti e garantendo il raggiungimento degli obiettivi prefissati. Tutte queste collaborazioni hanno prodotto pubblicazioni scientifiche come riportato nell'elenco delle pubblicazioni presenti in questo CV. Di seguito le collaborazioni con gruppi internazionali:

- Collaborazione con University of California Santa Barbara (UCSB), US Prof. Giovanni Vigna. Nome del progetto: Bootkeeper Obiettivo del progetto: Il principale obiettivo di Bootkeeper è lo studio avanzato delle tecniche di attacco del firmware in particolare del firmware UEFI, e la progettazione di sistemi di difesa basati sugli algoritmi dei compilatori che permettono di verificare proprietà di sicurezza del firmware analizzato
- Collaborazione con University of Berkeley California, US Prof. Dawn Song Nome del progetto: DARPA Cyber Grand Challenge Obiettivo del progetto: Il principale obiettivo del progetto è quello di progettare e sviluppare una piattaforma software che sia in grado di proteggere in automatico le applicazione contro attacchi noti.

- Collaborazione con l'università di Northesteran University, Boston, US con il Prof. Long Lu. Nome del progetto: Detecting (absent) app-to-app authentication on cross-device short-distance channel. Obiettivo del progetto: Il principale obiettivo del progetto è stato quello di analizzare i protocolli di scambio dati usati nelle comunicazioni short-distance channel come bluetooth e costruire un sistema automatico di rivelamento di processi di autenticazione che coinvolgono le app all'interno dei sistemi Android.
- Collaborazione con l'università di Ben-Gurion University of Israel Prof. Yuval Elovici. Nome del progetto: Sec-lib: Protecting scholarly digital libraries from infected papers using active machine learning framework. L'obiettivo principale del progetto è quello di rilevare attacchi sofisticati ai documenti pdf etc. attraverso tecniche di machine learning.
- Collaborazione con l'istituto di ricerca EURECOM, Francia, EU Prof. Balzarotti. Nome del progetto: "Micro-Virtualization Memory Tracing to Detect and Prevent Spraying Attacks", Obiettivo del progetto: l'obiettivo del progetto è stata la progettazione di un sistema di difesa che sfruttasse le peculiarità delle tecniche di virtualizzazione.
- Collaborazione con King's College University of London, UK, Prof. Fabio Pierazzi. Nome del progetto è "Cleaner: Generating Adversarial Heap Spraying Payloads in a Problem Space". L'obiettivo del progetto è di analizzare e attaccare tecniche di machine learning utilizzate per mitigare alcuni attacchi memory errors.

PUBBLICAZIONI

- [1] Lanzi Andrea Pagani Elena Bruschi Danilo, Di Pasquale Andrea. Ensuring cybersecurity for industrial networks: A solution for arp-based mitm attacks. *Journal of Computer Security*, vol. Pre-press, no. Pre-press, pp. 1-29, 2024, 2024.
- [2] Edoardo Vignati Lorenzo Nava Daniele Badagliacca Danilo Bruschi Long Lu Luca Buccioli, Stefano Cristalli and Andrea Lanzi. Jchainz:

Automatic detection of deserialization attacks in the java environment. *STM 2022 is the eighteenth workshop in this series and will be held at Copenhagen Denmark*, 2022.

- [3] Antonio Nappa, Aaron Úbeda-Portugués, Panagiotis Papadopoulos, Matteo Varvello, Juan Tapiador, and Andrea LANZI. Scramblesuit: An effective timing side-channels framework for malware sandbox evasion. *J. Comput. Secur.*, 30(6):851–876, 2022.
- [4] Andrea LANZI. Advanced techniques for memory forensics analysis. *Mobile Networks and Applications*, 25:234–235, 2020.
- [5] Danilo Bruschi, Andrea Di Pasquale, Silvio Ghilardi, Andrea LANZI, and Elena Pagani. A formal verification of arpon a tool for avoiding man-in-the-middle attacks in ethernet networks. *IEEE Transactions on Dependable and Secure Computing*, pages 1–1, 2021.
- [6] Fabio Pierazzi, Stefano Cristalli, Danilo Bruschi, Michele Colajanni, Mirco Marchetti, and Andrea LANZI. Glyph: Efficient ml-based detection of heap spraying attacks. *IEEE Trans. Inf. Forensics Secur.*, 16:740–755, 2021.
- [7] Antonio Nappa, Christopher Hobbs, and Andrea LANZI. Deja-vu: A glimpse on radioactive soft-error consequences on classical and quantum computations. *CoRR*, abs/2105.05103, 2021.
- [8] Antonio Nappa, Panagiotis Papadopoulos, Matteo Varvello, Daniel Aceituno Gomez, Juan Tapiador, and Andrea LANZI. Pow-how: An enduring timing side-channel to evade online malware sandboxes. In Elisa Bertino, Haya Shulman, and Michael Waidner, editors, *Computer Security - ESORICS 2021 - 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4-8, 2021, Proceedings, Part I*, volume 12972 of *Lecture Notes in Computer Science*, pages 86–109. Springer, 2021.
- [9] Muhammad Rizwan Asghar, Steven D. Galbraith, Andrea LANZI, Giovanni Russello, and Lukas Zobernig. Towards a theory of special-purpose program obfuscation. In Guojun Wang, Ryan K. L. Ko, Md. Zakirul Alam Bhuiyan, and Yi Pan, editors, *19th IEEE International Conference on*

- Trust, Security and Privacy in Computing and Communications, Trust-Com 2020, Guangzhou, China, December 29, 2020 - January 1, 2021*, pages 394–401. IEEE, 2020.
- [10] Nir Nissim, Aviad Cohen, Jian Wu, Andrea Lanzi, Lior Rokach, Yuval Elovici, and C. Lee Giles. Sec-lib: Protecting scholarly digital libraries from infected papers using active machine learning framework. *IEEE Access*, 7:110050–110073, 2019.
 - [11] Stefano Cristalli, Long Lu, Danilo Bruschi, and Andrea Lanzi. Detecting (absent) app-to-app authentication on cross-device short-distance channels. In David Balenson, editor, *Proceedings of the 35th Annual Computer Security Applications Conference, ACSAC 2019, San Juan, PR, USA, December 09-13, 2019*, pages 328–338. ACM, 2019.
 - [12] Ronny Chevalier, Stefano Cristalli, Christophe Hauser, Yan Shoshitaishvili, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna, Danilo Bruschi, and Andrea Lanzi. Bootkeeper: Validating software integrity properties on boot firmware images. In Gail-Joon Ahn, Bhavani M. Thuraisingham, Murat Kantarcioglu, and Ram Krishnan, editors, *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy, CODASPY 2019, Richardson, TX, USA, March 25-27, 2019*, pages 315–325. ACM, 2019.
 - [13] Andrea Lanzi. Game bot detection on massive multiplayer online role-playing games (mmorpgs) systems. In Newton Lee, editor, *Encyclopedia of Computer Graphics and Games*. Springer, 2019.
 - [14] Ronny Chevalier, Stefano Cristalli, Christophe Hauser, Yan Shoshitaishvili, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna, Danilo Bruschi, and Andrea Lanzi. Bootkeeper: Validating software integrity properties on boot firmware images. *CoRR*, abs/1903.12505, 2019.
 - [15] Eran Toch, Claudio Bettini, Erez Shmueli, Laura Radaelli, Andrea Lanzi, Daniele Riboni, and Bruno Lepri. The privacy implications of cyber security systems: A technological survey. *ACM Comput. Surv.*, 51(2):36:1–36:27, 2018.

- [16] Sergio Mascetti, Nadia Metoui, Andrea Lanzi, and Claudio Bettini. EPIC: a methodology for evaluating privacy violation risk in cybersecurity systems. *Trans. Data Priv.*, 11(3):239–277, 2018.
- [17] Michele Carminati, Mario Polino, Andrea Continella, Andrea Lanzi, Federico Maggi, and Stefano Zanero. Security evaluation of a banking fraud analysis system. *ACM Trans. Priv. Secur.*, 21(3):11:1–11:31, 2018.
- [18] Andrea Possemato, Andrea Lanzi, Simon Pak Ho Chung, Wenke Lee, and Yanick Fratantonio. Clickshield: Are you hiding something? towards eradicating clickjacking on android. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pages 1120–1136. ACM, 2018.
- [19] Stefano Cristalli, Edoardo Vignati, Danilo Bruschi, and Andrea Lanzi. Trusted execution path for protecting java applications against deserialization of untrusted data. In Michael Bailey, Thorsten Holz, Manolis Stamatogiannakis, and Sotiris Ioannidis, editors, *Research in Attacks, Intrusions, and Defenses - 21st International Symposium, RAID 2018, Heraklion, Crete, Greece, September 10-12, 2018, Proceedings*, volume 11050 of *Lecture Notes in Computer Science*, pages 445–464. Springer, 2018.
- [20] Andrea Continella, Michele Carminati, Mario Polino, Andrea Lanzi, Stefano Zanero, and Federico Maggi. Prometheus: Analyzing webinject-based information stealers. *J. Comput. Secur.*, 25(2):117–137, 2017.
- [21] Danilo Bruschi, Andrea Di Pasquale, Silvio Ghilardi, Andrea Lanzi, and Elena Pagani. Formal verification of ARP (address resolution protocol) through smt-based model checking - A case study -. In Nadia Polikarpova and Steve Schneider, editors, *Integrated Formal Methods - 13th International Conference, IFM 2017, Turin, Italy, September 20-22, 2017, Proceedings*, volume 10510 of *Lecture Notes in Computer Science*, pages 391–406. Springer, 2017.
- [22] Nir Nissim, Aviad Cohen, Jian Wu, Andrea Lanzi, Lior Rokach, Yuval Elovici, and C. Lee Giles. Scholarly digital libraries as a platform for malware distribution. In Abhik Roychoudhury and Yang Liu, editors, A

- Systems Approach to Cyber Security - Proceedings of the 2nd Singapore Cyber-Security R&D Conference (SG-CRC 2017)*, Singapore, February 21-22, 2017, volume 15 of *Cryptology and Information Security Series*, pages 107–128. IOS Press, 2017.
- [23] Nicola Basilico, Andrea Lanzi, and Mattia Monga. A security game model for remote software protection. In *11th International Conference on Availability, Reliability and Security, ARES 2016, Salzburg, Austria, August 31 - September 2, 2016*, pages 437–443. IEEE Computer Society, 2016.
 - [24] Mariano Graziano, Lorenzo Flore, Andrea Lanzi, and Davide Balzarotti. Subverting operating system properties through evolutionary DKOM attacks. In Juan Caballero, Urko Zurutuza, and Ricardo J. Rodríguez, editors, *Detection of Intrusions and Malware, and Vulnerability Assessment - 13th International Conference, DIMVA 2016, San Sebastián, Spain, July 7-8, 2016, Proceedings*, volume 9721 of *Lecture Notes in Computer Science*, pages 3–24. Springer, 2016.
 - [25] Fabio Pagani, Matteo De Astis, Mariano Graziano, Andrea Lanzi, and Davide Balzarotti. Measuring the role of greylisting and nolistings in fighting spam. In *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2016, Toulouse, France, June 28 - July 1, 2016*, pages 562–571. IEEE Computer Society, 2016.
 - [26] Stefano Cristalli, Mattia Pagnozzi, Mariano Graziano, Andrea Lanzi, and Davide Balzarotti. Micro-virtualization memory tracing to detect and prevent spraying attacks. In Thorsten Holz and Stefan Savage, editors, *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016*, pages 431–446. USENIX Association, 2016.
 - [27] Aristide Fattori, Andrea Lanzi, Davide Balzarotti, and Engin Kirda. Hypervisor-based malware protection with accessminer. *Comput. Secur.*, 52:33–50, 2015.
 - [28] Mariano Graziano, Davide Canali, Leyla Bilge, Andrea Lanzi, and Davide Balzarotti. Needles in a haystack: Mining information from public dynamic analysis sandboxes for malware intelligence. In Jaeyeon Jung and

- Thorsten Holz, editors, *24th USENIX Security Symposium, USENIX Security 15, Washington, D.C., USA, August 12-14, 2015*, pages 1057–1072. USENIX Association, 2015.
- [29] Babak Rahbarinia, Roberto Perdisci, Andrea Lanzi, and Kang Li. Peer-rush: Mining for unwanted P2P traffic. *J. Inf. Secur. Appl.*, 19(3):194–208, 2014.
 - [30] Gábor Pék, Andrea Lanzi, Abhinav Srivastava, Davide Balzarotti, Aurélien Francillon, and Christoph Neumann. On the feasibility of software attacks on commodity virtual machine monitors via direct device assignment. In Shiho Moriai, Trent Jaeger, and Kouichi Sakurai, editors, *9th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '14, Kyoto, Japan - June 03 - 06, 2014*, pages 305–316. ACM, 2014.
 - [31] Stefano Bianchi Mazzone, Mattia Pagnozzi, Aristide Fattori, Alessandro Reina, Andrea Lanzi, and Danilo Bruschi. Improving mac OS X security through gray box fuzzing technique. In Davide Balzarotti and Juan Caballero, editors, *Proceedings of the Seventh European Workshop on System Security, EuroSec 2014, April 13, 2014, Amsterdam, The Netherlands*, pages 2:1–2:6. ACM, 2014.
 - [32] Babak Rahbarinia, Roberto Perdisci, Andrea Lanzi, and Kang Li. Peer-rush: Mining for unwanted P2P traffic. In Konrad Rieck, Patrick Stewin, and Jean-Pierre Seifert, editors, *Detection of Intrusions and Malware, and Vulnerability Assessment - 10th International Conference, DIMVA 2013, Berlin, Germany, July 18-19, 2013. Proceedings*, volume 7967 of *Lecture Notes in Computer Science*, pages 62–82. Springer, 2013.
 - [33] Mariano Graziano, Andrea Lanzi, and Davide Balzarotti. Hypervisor memory forensics. In Salvatore J. Stolfo, Angelos Stavrou, and Charles V. Wright, editors, *Research in Attacks, Intrusions, and Defenses - 16th International Symposium, RAID 2013, Rodney Bay, St. Lucia, October 23-25, 2013. Proceedings*, volume 8145 of *Lecture Notes in Computer Science*, pages 21–40. Springer, 2013.
 - [34] Davide Canali, Andrea Lanzi, Davide Balzarotti, Christopher Kruegel, Mihai Christodorescu, and Engin Kirda. A quantitative study of accuracy

- in system call-based malware detection. In Mats Per Erik Heimdahl and Zhendong Su, editors, *International Symposium on Software Testing and Analysis, ISSTA 2012, Minneapolis, MN, USA, July 15-20, 2012*, pages 122–132. ACM, 2012.
- [35] Abhinav Srivastava, Andrea Lanzi, Jonathon T. Giffin, and Davide Balzarotti. Operating system interface obfuscation and the revealing of hidden operations. In Thorsten Holz and Herbert Bos, editors, *Detection of Intrusions and Malware, and Vulnerability Assessment - 8th International Conference; DIMVA 2011, Amsterdam, The Netherlands, July 7-8, 2011. Proceedings*, volume 6739 of *Lecture Notes in Computer Science*, pages 214–233. Springer, 2011.
 - [36] Leyla Bilge, Andrea Lanzi, and Davide Balzarotti. Thwarting real-time dynamic unpacking. In Engin Kirda and Steven Hand, editors, *Proceedings of the Fourth European Workshop on System Security, EUROSEC’11, April 10, 2011, Salzburg, Austria*, page 5. ACM, 2011.
 - [37] Kaan Onarlioglu, Leyla Bilge, Andrea Lanzi, Davide Balzarotti, and Engin Kirda. G-free: defeating return-oriented programming through gadget-less binaries. In Carrie Gates, Michael Franz, and John P. McDermott, editors, *Twenty-Sixth Annual Computer Security Applications Conference, ACSAC 2010, Austin, Texas, USA, 6-10 December 2010*, pages 49–58. ACM, 2010.
 - [38] Andrea Lanzi, Davide Balzarotti, Christopher Kruegel, Mihai Christodorescu, and Engin Kirda. Accessminer: using system-centric models for malware protection. In Ehab Al-Shaer, Angelos D. Keromytis, and Vitaly Shmatikov, editors, *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010*, pages 399–412. ACM, 2010.
 - [39] Monirul I. Sharif, Wenke Lee, Weidong Cui, and Andrea Lanzi. Secure in-vm monitoring using hardware virtualization. In Ehab Al-Shaer, Somesh Jha, and Angelos D. Keromytis, editors, *Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 9-13, 2009*, pages 477–487. ACM, 2009.

- [40] Andrea Lanzi, Monirul I. Sharif, and Wenke Lee. K-tracer: A system for extracting kernel malware behavior. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2009, San Diego, California, USA, 8th February - 11th February 2009*. The Internet Society, 2009.
- [41] Monirul I. Sharif, Andrea Lanzi, Jonathon T. Giffin, and Wenke Lee. Automatic reverse engineering of malware emulators. In *30th IEEE Symposium on Security and Privacy (S&P 2009), 17-20 May 2009, Oakland, California, USA*, pages 94–109. IEEE Computer Society, 2009.
- [42] Roberto Perdisci, Andrea Lanzi, and Wenke Lee. Classification of packed executables for accurate computer virus detection. *Pattern Recognit. Lett.*, 29(14):1941–1946, 2008.
- [43] Roberto Perdisci, Andrea Lanzi, and Wenke Lee. Mcboost: Boosting scalability in malware collection and analysis using statistical classification of executables. In *Twenty-Fourth Annual Computer Security Applications Conference, ACSAC 2008, Anaheim, California, USA, 8-12 December 2008*, pages 301–310. IEEE Computer Society, 2008.
- [44] Lorenzo Cavallaro, Andrea Lanzi, Luca Mayer, and Mattia Monga. LIS-ABETH: automated content-based signature generator for zero-day polymorphic worms. In Bart De Win, Seok-Won Lee, and Mattia Monga, editors, *Proceedings of the Fourth International Workshop on Software Engineering for Secure Systems, SESS 2008, Leipzig, Germany, May 17-18, 2008*, pages 41–48. ACM, 2008.
- [45] Monirul I. Sharif, Andrea Lanzi, Jonathon T. Giffin, and Wenke Lee. Impeding malware analysis using conditional code obfuscation. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2008, San Diego, California, USA, 10th February - 13th February 2008*. The Internet Society, 2008.
- [46] Abhinav Srivastava, Andrea Lanzi, and Jonathon T. Giffin. System call API obfuscation (extended abstract). In Richard Lippmann, Engin Kirda, and Ari Trachtenberg, editors, *Recent Advances in Intrusion Detection, 11th International Symposium, RAID 2008, Cambridge, MA*,

- USA, September 15-17, 2008. *Proceedings*, volume 5230 of *Lecture Notes in Computer Science*, pages 421–422. Springer, 2008.
- [47] Danilo Bruschi, Lorenzo Cavallaro, and Andrea Lanzi. An efficient technique for preventing mimicry and impossible paths execution attacks. In *Proceedings of the 26th IEEE International Performance Computing and Communications Conference, IPCCC 2007, April 11-13, 2007, New Orleans, Louisiana, USA*, pages 434–441. IEEE Computer Society, 2007.
 - [48] Andrea Lanzi, Lorenzo Martignoni, Mattia Monga, and Roberto Paleari. A smart fuzzer for x86 executables. In *Third International Workshop on Software Engineering for Secure Systems, SESS 2007, Minneapolis, MN, USA, May 20-26, 2007*, page 7. IEEE Computer Society, 2007.
 - [49] Danilo Bruschi, Lorenzo Cavallaro, and Andrea Lanzi. Diversified process replica for defeating memory error exploits. In *Proceedings of the 26th IEEE International Performance Computing and Communications Conference, IPCCC 2007, April 11-13, 2007, New Orleans, Louisiana, USA*, pages 434–441. IEEE Computer Society, 2007.
 - [50] Danilo Bruschi, Lorenzo Cavallaro, Andrea Lanzi, and Mattia Monga. Replay attack in TCG specification and solution. In *21st Annual Computer Security Applications Conference (ACSAC 2005), 5-9 December 2005, Tucson, AZ, USA*, pages 127–137. IEEE Computer Society, 2005.
 - [51] Danilo Bruschi, Igor Nai Fovino, and Andrea Lanzi. A protocol for anonymous and accurate e-polling. In Michael H. Böhlen, Johann Gamper, Wolfgang Polasek, and Maria A. Wimmer, editors, *E-Government: Towards Electronic Democracy, International Conference, TCGOV 2005, Bolzano, Italy, March 2-4, 2005, Proceedings*, volume 3416 of *Lecture Notes in Computer Science*, pages 112–121. Springer, 2005.

In totale 14 pubblicazioni a Rivista e 37 a Conferenza.

DIDATTICA

Il mio obiettivo principale come insegnante è aiutare i miei studenti a diventare pensatori critici. Desidero che giochino con le idee, affrontino problemi impegnativi e condividano ciò che hanno imparato in modo efficace, diventando loro stessi degli insegnanti. Ciò richiede che acquisiscano le competenze necessarie per valutare scientificamente e criticamente un'idea, mantenendo al contempo un atteggiamento costruttivo nello sviluppo di soluzioni nuove e valide. Questo non è un percorso a senso unico, poichè è sorprendente quanto gli studenti possano sfidare se stessi stimolando ancora di più il loro intelletto. Risolvere i problemi è, in definitiva, proprio questo: guardare ai problemi da diverse prospettive, trovare soluzioni eleganti sfruttando la conoscenza e l'esperienza acquisite.

Dal lato pratico, tutti i miei corsi prevedono esercitazioni pratiche per supportare la discussione sui temi descritti nelle lezioni. Ad esempio, le esercitazioni sulle vulnerabilità delle applicazioni e dei siti web sono organizzate in livelli di difficoltà crescente che richiedono agli studenti di sfruttare programmi noti per avere diversi tipi di difetti di sicurezza. Un'altra esercitazione, invece, richiede agli studenti di scrivere un programma in C per raccogliere parole da file con estensioni specifiche. Lo scopo era quello di far loro scrivere un programma capace di raccogliere parole da utilizzare successivamente in un attacco di cracking delle password basato su dizionario. Sebbene queste esercitazioni sembrano essere solo esercizi di programmazione, la loro vera natura viene compresa solo in seguito, quando agli studenti è stato richiesto di analizzare la sicurezza delle soluzioni fornite dai loro compagni di corso: è estremamente interessante osservare la creatività degli studenti e come essi si impegnino al massimo per trovare, sfruttare e risolvere le vulnerabilità che, all'inizio del corso, avevano solo la forma di una pratica di programmazione comune e innocua.

Attività Didattica Insegnamenti e Moduli, Master post-Laurea e Specializzazione

- Titolare dei seguenti insegnamenti in Laurea triennale:
 - Sistemi Operativi I e II (INF01 12 CFU, 72 ore) insegnamento obbligatorio 2020/2021, 2021/2022, 2022/2023, 2023/2024.

- Laboratorio di Programmazione Informatica (INF01 6 CFU), insegnamento obbligatorio 2017/2018.
- Laboratorio di Programmazione Medicina (MED, 6 CFU), insegnamento obbligatorio 2017/2018, 2018/2019.
- Fondamenti di Social Media Digitali (INF01, 6 CFU 48 ore) insegnamento complementare 2018/2019, 2019/2020.
- Laboratorio di Programmazione (MAT01, 6 CFU) insegnamento obbligatorio 2020/2021.
- Sicurezza e Privacy (INF01 6 CFU, 48 ore), insegnamento complementare 2014/2015, 2015/2016, 2016/2017, 2017/2018, 2018/2019.
- Titolare dei seguenti insegnamenti in Laurea Magistrale:
 - Corso di Sicurezza (INF01 6 CFU, 48 ore) 2020/2021, 2021/2022, 2022/2023, 2023/2024.
- Attività Didattiche Post laurea Master, perfezionamento e scuole di dottorato:
 - Insegnamento nell'ambito del Master di CyberSecurity (40 ore) 2019/2020 2020/2021, 2021/2022, 2022/2023.
 - Insegnamento Corsi di formazione Sicurezza per personale tecnico amministrativo unimi (48 ore), 2017/2018, 2018/2019, 2019/2020.
 - Corso Dottorato "Advanced Software Security" (2 CFU, 12 ore) 2016/2017, 2017/2018.
 - Corso Programmazione Python per Avvocati (20 ore) nel corso di specializzazione digitalizzazione del corso di perfezionamento Università degli studi di Milano, "Coding for Lawyers, Legal Tech, Legal Writing and Legal Design" 2019/2020, 2020/2021, 2021/2022, 2023/2024.

Attività di tesi di Laurea

In qualità di relatore o correlatore, ho supervisionato più di 45 tesi triennali e oltre 35 tesi magistrali incentrate principalmente sulla sicurezza dei sistemi, con particolare attenzione alla progettazione e allo studio di sistemi di difesa

per le diverse tecnologie, come ad esempio il web, gli smartphone e i sistemi embedded. Grazie a questa esperienza, ho approfondito le mie conoscenze in questo ambito, lavorando a stretto contatto con studenti di talento e supportandoli nella loro formazione accademica e professionale.

Attività di tesi di Dottorato

Nel corso del mio lavoro di ricerca, ho avuto l'opportunità di supervisionare Stefano Cristalli, che ha conseguito il dottorato nell'anno accademico 2018/2019 presentando una tesi dal titolo "Analisi statiche e dinamiche per la protezione dell'ambiente di esecuzione del software Java". Attualmente, sono il supervisore di 4 studenti di dottorato: Davide Rusconi (dal 2022) e Matteo Zoia (dal 2022), Davide Parata (dal 2023) e Andrea Monzani (dal 2023). Riassumendo una tesi conclusa e 4 tesi attive.

Attività Dipartimentali

- **Gestione del laboratorio di Sicurezza Laser.** Durante la mia esperienza presso il Dipartimento di Informatica e il laboratorio di Sicurezza, ho maturato competenze di leadership e coordinamento. Nel 2015, sono stato scelto come Vice Direttore del team di sicurezza Laser, ruolo che mi ha permesso di guidare le attività del gruppo. In questa posizione, mi sono occupato della preparazione e dell'esecuzione di progetti, della valutazione delle prestazioni dei ricercatori del team e del supporto alla selezione di nuovi ricercatori e dottorandi.

Nel corso degli anni, ho dimostrato una notevole abilità nella gestione finanziaria, essenziale per la sostenibilità del gruppo. In particolare, ho coordinato la realizzazione di tre progetti scientifici internazionali: il progetto PACS finanziato dal Ministero degli Affari Esteri, il progetto CISCO sulla protezione del software e il progetto MAECI sulla sicurezza dei sistemi embedded. Ho anche gestito progetti più piccoli come Sentinel e lo studio degli attacchi Side-Channel in collaborazione con MBDA Missile System.

In qualità di leader del team, ho avuto l'opportunità di interagire con altre istituzioni dell'UE e degli Stati Uniti, tra cui Northeastern University of Boston, US and USCB, University of California, US, EURECOM (Francia), King's College of London (UK), Tel Aviv University, Israel. Il

mio ruolo prevedeva anche compiti amministrativi e di interazione con altri gruppi.

Grazie alla mia esperienza, il nostro gruppo di ricerca è cresciuto e attualmente comprende 4 dottorandi, 1 ricercatore (post-doc) e 5 studenti di master, tutti sotto la mia supervisione. Insieme, abbiamo partecipato a varie gare di sicurezza informatica come CyberChallenge.it.

- **Gestione della CyberChallenge Unimi.** Dal 2019 al 2024 ho coordinato l'iniziativa italiana di Cyberchallenge, durante la quale abbiamo formato più di 100 persone per partecipare a gare di sicurezza informatica. Il mio ruolo principale è stato quello di coordinare e preparare la parte di laboratorio. Grazie al nostro impegno, la nostra università ha ottenuto ottimi risultati, classificandosi al sesto posto su 62 posizioni.
- **Commissione Erasmus.** Come membro della commissione Erasmus, il mio ruolo prevede la selezione e la gestione degli studenti che partecipano al programma di borse Erasmus e degli studenti stranieri che studiano presso la nostra università. In particolare, mi occupo della valutazione delle candidature, dell'organizzazione delle attività di orientamento, dell'assistenza agli studenti durante il loro soggiorno e del monitoraggio dei loro progressi accademici. Il mio lavoro all'interno della commissione mi ha permesso di acquisire competenze in diversi ambiti, tra cui la gestione delle relazioni interpersonali, l'organizzazione di attività e l'elaborazione di dati.
- **Commissione Giudicatrice per la Selezione Dottorandi** nel 2023. Sono onorato/a di far parte della commissione di selezione dei potenziali dottorandi per il bando del 2023. Il mio ruolo all'interno della commissione prevede la valutazione delle candidature pervenute, la selezione dei candidati più idonei e la raccomandazione dei migliori per la concessione di borse di studio. Partecipare a una commissione di selezione di questo tipo mi offre l'opportunità di approfondire le mie conoscenze nel campo della ricerca accademica e di contribuire alla formazione di una nuova generazione di studiosi.
- **Commissione Giudicatrice per Selezione Master In CyberSecurity** Sono orgoglioso di far parte della commissione e dell'organizzazione del Master in Cybersecurity presso l'Università degli Studi di Milano a

partire dal 2022. Il mio ruolo principale all'interno del progetto prevede la pianificazione e la coordinazione delle attività didattiche, la progettazione dei programmi di insegnamento e la supervisione del corpo docente. Come coordinatore del progetto master, ho la responsabilità di garantire l'alta qualità del programma e di assicurarmi che gli studenti acquisiscano le competenze necessarie per diventare esperti nel campo della cybersecurity.

- **Collegio di Dottorato** Essere membro attivo del Collegio di Dottorato dal 2015-Now mi ha permesso di partecipare attivamente alle attività accademiche e di ricerca all'interno del mio dipartimento universitario. Il mio ruolo prevede la partecipazione a riunioni la revisione dei programmi di dottorato e la valutazione dei progetti di ricerca degli studenti di dottorato. Essere parte attiva del Collegio di Dottorato mi ha permesso di lavorare a stretto contatto con colleghi di diverse aree disciplinari, di approfondire le mie conoscenze e di contribuire alla crescita del mio dipartimento universitario. Inoltre, ho avuto l'opportunità di interagire con studenti di dottorato e di condividere la mia esperienza con loro.
- **Commissioni Di Dottorato.** Ho fatto parte della commissione di Dottorato nel 2023 del candidato Andrea Oliveri dal titolo della tesi: "A Zero-Knowledge Approach to Memory Forensics" presso l'istituto di Ricerca Eurecom nel sud della Francia. (Ottobre 2023). Inoltre, ho fatto parte della commissione di dottorato per la tesi dal titolo "Tecniche attive per rivelare e analizzare la sicurezza dei server nascosti", presentata dal candidato al dottorato Srdjan Matic presso l'Università di Milano nel 2018.
- **Tutoraggio Studenti.** Una delle attività di cui mi occupo attivamente è il tutoraggio per l'orientamento degli studenti iscritti alla Laurea in sicurezza dei sistemi e delle reti informatiche. In particolare, ho partecipato come tutor nei tre anni accademici 2020/2021, 2021/2022 e 2022/2023, 2023/2024. Questo ruolo di supporto ha comportato diverse responsabilità, tra cui la gestione di sessioni di tutoraggio, la correzione e la valutazione degli elaborati degli studenti e la partecipazione attiva a riunioni e incontri di coordinamento.
- **AQ sicurezza informatica magistrale (2024).** Nel ruolo di coor-

dinatore del corso di laurea magistrale in Sicurezza Informatica presso l'Università degli studi di Milano, mi occupo di pianificare e supervisionare l'intero programma didattico, assicurando che i contenuti siano aggiornati e rilevanti rispetto alle più recenti evoluzioni tecnologiche e alle esigenze del mercato.

Milano, 27 Maggio 2024