

CURRICULUM VITAE di

FILIPPO MARIA LAURIA (filippo.lauria@iit.cnr.it)

+ PRINCIPALI ATTIVITÀ LAVORATIVE

LUG 2016 – PRESENTE
TECNOLOGO III LIVELLO
presso l'ISTITUTO
di INFORMATICA
e TELEMATICA
del CNR di PISA

Membro del gruppo che gestisce le reti telematiche del CNR di Pisa, sto continuando a realizzare 6MoNPlus.
Una prima release del software è stata realizzata ed è distribuita attraverso il sito <https://www.6monplus.it>.
Contestualmente, mi occupo di realizzare infrastrutture per monitorare lo spreading attraverso Internet delle botnet (in particolar modo la botnet MIRAI).
In collaborazione con il gruppo di ricerca Trustworthy and Secure Future Internet ho contribuito all'implementazione del framework di autorizzazione, basato su eventi, per lo Usage Control (utilizzando il linguaggio Java).



Partecipazione all'attività di ricerca "DIT.AD006.029.005" del CNR denominato Cybersecurity Lab – in qualità di esperto di sicurezza delle reti.

Partecipazione al gruppo di lavoro per la definizione di una policy di sicurezza riguardante l'utilizzo della rete informatica dell'Istituto IIT, dei servizi informatici e di tutte le apparecchiature connesse in rete al fine di garantirne la conformità al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016.

2016 – PRESENTE
DIPARTIMENTO di
INGEGNERIA
dell'INFORMAZIONE
UNIVERSITÀ di PISA

Codocente dell'insegnamento "Lab of Secure system configuration, device hardening and firewall management" nell'ambito del master universitario di primo livello in cybersecurity (edizioni 16/17, 17/18, 18/19, 19/20, 20/21) organizzato dal Dipartimento di Ingegneria dell'Informazione dell'Università degli Studi di Pisa e dall'Istituto di informatica e Telematica del CNR di Pisa.



+ HIGHLIGHTS CYBERSECURITY

Da oltre 5 anni, ho familiarità con la distribuzione linux per pentester di Offensive Security, Kali Linux, perciò, non sono nuovo all'utilizzo di strumenti come Nmap, Metasploit, Nessus, Nikto, etc.
Ho una buona conoscenza teorica della maggior parte degli attacchi, avendo studiato e messo in pratica attacchi alle applicazioni web, più comuni, come ad esempio: SQL Injection, XSS, LFI, RFI, RCE, etc.

+ FORMAZIONE

MAG 2014 **ABILITAZIONE all'ESERCIZIO della PROFESSIONE di INGEGNERE**

UNIVERSITÀ di PISA **Voto: 221/240**



L'abilitazione all'esercizio della Professione di Ingegnere è stata ottenuta, avendo superato l'esame di stato svoltosi nella II SESSIONE dell'anno 2014.

2010 – 2013 **LAUREA MAGISTRALE IN INGEGNERIA INFORMATICA**

UNIVERSITÀ di PISA **Voto: 109/110**



Tesi:
"progettazione ed implementazione di un'interfaccia web per l'autocorrezione, da parte degli studenti, di esercizi di programmazione"

+ RIEPILOGO COMPETENZE PROFESSIONALI

SISTEMI OPERATIVI **Unix-like, Microsoft Windows Family OSs**

SVILUPPO SOFTWARE **C, C++/STL, Java, sviluppo specifico in ambiente Unix-like (sockets e gestione threads), Bash e Perl (espressioni regolari)**

SVILUPPO WEB **HTML, CSS, PHP, WebObjects Framework, Javascript, jQuery, SQL**


GRAFICA **GIMP, Photoshop**

+ PRODUZIONE SCIENTIFICA

2020 Autore del rapporto tecnico dal titolo:

RAPPORTO TECNICO *"Exploiting an unpatched flaw in daloRADIUS 1.1-2 to obtain a reverse shell", IIT TR-01/2020*


ISTITUTO di INFORMATICA
e TELEMATICA del CNR **Keywords:** cybersecurity, exploit, wast (web application security test)

 Link: <https://www.iit.cnr.it/node/58272>

2018 Autore del rapporto tecnico dal titolo:

RAPPORTO TECNICO *"How long does it take before a new Internet node is contacted for the very first time?", IIT TR-03/2018*

ISTITUTO di INFORMATICA
e TELEMATICA del CNR **Keywords:** cybersecurity, honeypots, malware, network security

 Link: <https://www.iit.cnr.it/node/50970>

2018 Autore del rapporto tecnico dal titolo:

RAPPORTO TECNICO *"Leveraging ROP to redirect the execution flow of flawed binaries", IIT TR-01/2018*


ISTITUTO di INFORMATICA
e TELEMATICA del CNR **Keywords:** buffer overflow, cybersecurity, exploitation, rop (return oriented programming), reverse engineering

 Link: <https://www.iit.cnr.it/node/50785>

DIC 2018 Autore dell'articolo dal titolo:

ARTICOLO *"Sagishi: an undercover software agent for infiltrating IoT botnets, Network Security".*

Network Security Journal
Volume 2019, Issue 1 **DOI:** 10.1016/S1353-4858(19)30009-1


 **Keywords:** cybersecurity, honeypots, IoT (Internet of Things)

Link al journal: <https://www.sciencedirect.com/journal/network-security>

DIC 2017 Autore dell'articolo dal titolo:

ARTICOLO *"How to footprint, report and remotely secure compromised IoT devices".*

Network Security Journal
Volume 2017, Issue 12 **DOI:** 10.1016/S1353-4858(17)30123-x

 **Keywords:** cybersecurity, honeypots, IoT (Internet of Things)

Link al journal: <https://www.sciencedirect.com/journal/network-security>

+ PRODUZIONE SCIENTIFICA

GIU 2016	Coautore dell'articolo dal titolo:
ARTICOLO	"6MoNPlus: Geographically distributed DualStack network monitoring"
32nd edition TERENA Networking Conference TNC16: Building the Internet of People	Link: https://tnc16.geant.org/getfile/2525

2016	Autore del rapporto tecnico dal titolo:
RAPPORTO TECNICO	"A threshold-based caching mechanism for distributed network monitoring tools", IIT TR-04/2016
ISTITUTO di INFORMATICA e TELEMATICA del CNR	Keywords: caching, distributed network, dual-stack network, network monitoring



L'algoritmo descritto è stato implementato utilizzando il linguaggio C++ all'interno del back-end di 6MoNPlus.

Link: <https://www.iit.cnr.it/node/38028>

2016	Autore del rapporto tecnico dal titolo:
RAPPORTO TECNICO	"A distributed architecture for monitoring and controlling geo-distributed computer networks", IIT TR-03/2016
ISTITUTO di INFORMATICA e TELEMATICA del CNR	Keywords: distributed architecture, dual-stack network, geo-distributed network, network monitoring
	L'architettura descritta nel rapporto tecnico è stata utilizzata per l'implementazione (utilizzando il linguaggio C++) del back-end distribuito di 6MoNPlus.
	Link: https://www.iit.cnr.it/node/38022

Il sottoscritto è a conoscenza che, ai sensi dell'art.26 della legge15/68, le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti ai sensi del codice penale e delle leggi speciali. Inoltre, il sottoscritto autorizza il trattamento dei dati personali contenuti in questo curriculum vitae, in conformità alle disposizioni dell'art. 13 del D.lgs 196/2003 e dell'art. 13 GDPR 679/2016.

Ing. Filippo Maria Lauria

(Firma)

Pisa, 20 settembre 2021