

# Filippo Maria Lauria

## INFORMAZIONI PERSONALI

**Nome e cognome:** Filippo Maria Lauria

**Ruolo attuale:** Tecnologo presso l'Istituto di Informatica e Telematica (IIT) del CNR

**Unità tecnologica:** Computer and Communication Networks (CCN)

## ISTRUZIONE E QUALIFICHE

- **dicembre 2013:**  
Laurea Magistrale in Ingegneria Informatica, Università di Pisa
- **febbraio 2014:**  
abilitazione all'esercizio della professione di Ingegnere dell'Informazione

## ESPERIENZA PROFESSIONALE

### Tecnologo (giugno 2016 – presente)

*Istituto di Informatica e Telematica (IIT) del CNR*

- responsabile scientifico per progetti di ricerca nel campo della cybersecurity
- cogestione di infrastrutture di rete complesse
- sviluppo e integrazione di soluzioni software e servizi per la sicurezza informatica

### Assegnista di ricerca (giugno 2014 – maggio 2016)

*Istituto di Informatica e Telematica (IIT) del CNR*

- sviluppo di soluzioni per il monitoraggio di reti geograficamente distribuite
- ricerca nel campo delle reti dual-stack IPv4/IPv6

### Borsista (gennaio 2014 – maggio 2014)

*Dipartimento di Ingegneria dell'Informazione – Università di Pisa*

- sviluppo di interfacce web per l'auto-correzione di esercizi di programmazione
- implementazione di moduli software per la didattica

## RICONOSCIMENTI

- Terzo posto "IIT Innovation Grant 2023" per HCI4IIT
- Certificazione IBM "Quantum Excellence"
- Secondo posto "IIT Innovation Grant 2021" per NetManPy
- Lettera di ringraziamento da Liran Tal (creatore daloRADIUS)
- Interviste su media nazionali (RAI News, PuntoRadioFM)

## LINGUE

- Italiano:  
Madrelingua
- Inglese:  
Livello C1 Advanced

## PROGETTI DI RICERCA PRINCIPALI

### **TRANTOR** / progetto europeo / gennaio 2023 - presente *5G+ evoluTion to mutioRbitAl multibaNd neTwORks*

- contributo alla ricerca sulla qualità di servizio QoS nelle reti satellitari 5G
- supporto tecnico-scientifico per l'integrazione delle tecnologie 5G in ambito satellitare

### **SINTETIC** / progetto europeo / giugno 2023 - presente *ingle item identification for forest production, protection, and management*

- contributo alla progettazione del datacenter per l'operatività del progetto

### **SLICES** / progetto europeo / gennaio 2024 - presente *Scientific Large-scale Infrastructure for Computing/Communication Experimental Studies*

- contributo all'implementazione di una research infrastructure europea in ambito 5G
- research manager infrastructure del datacenter del sito SLICES dell'IIT-CNR

### **QUID** / gennaio 2023 - presente *Quantum Italy Deployment*

- supporto allo sviluppo della rete quantistica italiana presso l'Area della Ricerca di Pisa

### **SIFIS-HOME** / progetto europeo / aprile 2022 - settembre 2023 *Secure Interoperable Full-Stack Internet of Things for Smart Home*

- supporto tecnico-scientifico per l'implementazione di misure di sicurezza su sistemi dedicati al progetto

### **Cybersecurity LAB** / 2017 - 2019 *sottoprogetto RETI*

- responsabile scientifico e referente del sottoprogetto RETI
- presidenza della commissione per conferimento assegno di ricerca
- progettazione, realizzazione e gestione dell'infrastruttura di honeypot
- ricerca sulla diffusione di botnet
- produzione di contributi scientifici e rapporti tecnici

### **6MoN** / 2014-2016

- sviluppo del sistema open-source 6MoNPlus
- monitoraggio delle reti dual-stack geo-distribuite
- risoluzione di problemi specifici delle architetture software

## ALTRE ATTIVITÀ

- consolidamento cibernetico nell'ambito del progetto "cittaeducante" (2022)

## ATTIVITÀ DIDATTICA

### Docenza universitaria / Università di Pisa / 2017 - presente

#### *Master in cybersecurity*

- >100 ore di insegnamento (da settembre 2017 a novembre 2024)
- tematiche: networking e penetration testing

#### *Master in diritto e tecnologia dell'ecosistema digitale*

- tematiche: networking e surface/dark/deep web

### Altri incarichi di docenza

#### *corsi di sicurezza informatica per registrar presso Registro .it (2018-2019)*

- >20 ore di formazione
- tematiche: web application penetration test

#### *corso avanzato di cybersecurity presso ESTAR Toscana (2021)*

- ~10 ore di formazione specialistica
- tematiche: tecniche avanzate di network penetration test

#### *corso sulla "sicurezza del web" presso C3T (2022)*

- ~4 ore di formazione nell'ambito del programma CyberChallenge.IT del Cybersecurity National Lab per il Centro di Competenza Cybersecurity Toscano (C3T)

## COMPETENZE TECNICHE

### Networking

- progettazione e implementazione infrastrutture di rete dual-stack (IPv4/IPv6)
- gestione switching e routing avanzato
- gestione reti wired e wireless enterprise
- configurazione e manutenzione Next-Generation Firewall (NGFW)
- implementazione e gestione servizi di VPN
- implementazione e gestione servizi AAA (Autenticazione, Autorizzazione, Accounting)

### Cybersecurity

- penetration testing e vulnerability assessment
- threat intelligence e monitoraggio
- progettazione, realizzazione e gestione infrastrutture di monitoraggio basate su honeypot
- analisi malware e botnet
- incident response e gestione emergenze

### Sviluppo software

- linguaggi: Python, C/C++, Java, PHP
- web: HTML, CSS, JavaScript
- framework: Django, Flask
- shell scripting (POSIX, Bash)
- test-Driven Development (TDD)
- sistemi di versioning (Git, SVN)

## Sistemi e infrastrutture

- amministrazione sistemi Linux
- ambienti di virtualizzazione
- cloud computing e servizi distribuiti
- database SQL e NoSQL
- gestione datacenter tradizionali ed iperconvergenti (HCI)
- sistemi di backup e disaster recovery

## RUOLI E RESPONSABILITÀ ATTUALI

### Gestione infrastrutture presso Area della Ricerca di Pisa

#### *APM (Access Port Manager) GARR*

- cogestione del collegamento dell'Area della Ricerca di Pisa con rete GARR
- implementazione sistemi di monitoraggio

#### *Sicurezza perimetrale*

- gestione e implementazione delle policy di firewalling su apparati NGFW di frontiera (IPS/IDS, DoS Protection, ecc.)
- interazione con GARR-CERT per gestione minacce

#### *Servizi di rete*

- supporto alla gestione dell'infrastruttura Wi-Fi
- referente tecnico eduroam per il realm pi.cnr.it
- implementazione e gestione helpdesk di rete
- supporto alla gestione di servizi di switching e routing, nonché DHCP, RADIUS, VPN, ecc.

#### *Responsabilità specifiche per istituti CNR*

- monitoraggio e sicurezza reti per 9 istituti (IPCF, ICCOM, ISTI, IN, ILC, IGG, IRET, IBBA, ITB)
- gestione infrastruttura Wi-Fi e servizi per INO
- gestione completa infrastruttura di rete per IBF
- responsabile degli accessi alla IBM Quantum Network per i ricercatori IIT

## Ruoli istituzionali

#### *RAO (Registration Authority Officer) CNR su piattaforma SCM di Sectigo Ltd*

- implementazione portale web dedicato
- automazione processi di richiesta e rinnovo certificati

#### *Esperto di settore (informatica)*

- iscrizione all'Elenco Regionale Esperti di Settore (ERES) Toscana
- settore: informatica

#### *Commissioni*

- presidente e/o membro in commissioni per la selezione del personale IIT-CNR
- presidente e/o membro in commissioni di valutazione nell'ambito di diverse gare pubbliche per l'acquisizione di beni e/o servizi

## PUBBLICAZIONI E CONTRIBUTI TECNICO-SCIENTIFICI

Sono riportati di seguito solo i contributi più significativi. Per un elenco completo e aggiornato delle pubblicazioni e dei prodotti si rimanda al catalogo della ricerca CNR-IRIS: <https://iris.cnr.it/cris/rp/rp07836>.

### Articoli in rivista

- Lauria, F. M. (2017). How to footprint, report and remotely secure compromised IoT devices. *Network Security*, 2017(6), pp. 14-19.
- Oliveri, A., & Lauria, F. M. (2019). Sagishi: an undercover software agent for infiltrating IoT botnets. *Network Security*, 2019(3), pp. 6-13.

### Rapporti tecnici significativi

- 5G network analysis for dynamic QoS and traffic management. Gebrehiwot, A.; De Vita, A.; Lauria, F. M. (2023).
- A software-based 5G infrastructure for the TRANTOR project. De Vita, A.; Gebrehiwot, A.; Lauria, F. M. (2023).
- Open-source AAA infrastructure deployment with MariaDB, FreeRADIUS and daloRADIUS. Lauria, F. M. (2023).
- Peculiarities of Traffic and QoS management in 5G NTN networks. Gebrehiwot, A.; Lauria, F. M.; A., De Vita (2023).
- Understanding the MIRAI botnet: scanning process, infection method and key features. Lauria, F. M.; A., De Vita (2023).
- Structured cabling system: a methodology for planning and executing works on a complex network infrastructure. Porta, C.; Lauria, F. M.; De Vita, A. (2022).
- Increasing the security level of a Debian-based server. Lauria, F. M.; De Vita, A. (2022).
- Technical and administrative considerations on acquiring a NGFW-based network security solution. Lauria, F. M.; Gebrehiwot, A.; Sannicandro, I. (2021).
- Analysis of CitoDay data leak: a collection of 345 million hacked credentials from 23600 online services. Lauria, F. M.; De Vita, A.; Gebrehiwot, A. (2020).
- A distributed architecture for monitoring and controlling geo-distributed computer networks. Porta, C.; Lauria, F. M.; De Vita, A. (2016).
- A threshold-based caching mechanism for distributed network monitoring tools. Lauria, F. M. (2016).

### Altri contributi

- coautore della policy di sicurezza informatica dell'IIT-CNR
- sviluppo procedure specifiche per la sicurezza del sito web dell'IIT-CNR
- documentazione analitica sul servizio di emissione dei certificati digitali CNR
- svolgimento di attività di penetration testing nell'ambito della protezione dalle cyber-minacce delle risorse informatiche connesse alle reti dell'IIT-CNR
- identificazione e segnalazione di molteplici vulnerabilità critiche in sistemi software, tra cui due CVE (Common Vulnerabilities and Exposures) ufficialmente riconosciuti:
  - CVE-2022-4366: Esposizione di informazioni sensibili di sistema in daloRADIUS
  - CVE-2022-4630: Cookie di sessione senza flag HttpOnly in daloRADIUS

## SOFTWARE E SERVIZI SVILUPPATI

### 6MoNPlus

- sistema open-source per il monitoraggio di reti dual-stack (IPv4/IPv6)
- diffusione internazionale su >70 organizzazioni

### Globethreatd

- sistema web per la visualizzazione 3D di minacce botnet che integra i dati provenienti dall'infrastruttura di honeypot menzionata precedente
- diffusione internazionale, ~20.000 visite dal 2018

### DNSRecon

- strumento per l'esecuzione di security testing dei sistemi DNS
- diffusione internazionale, >120.000 utilizzatori/anno

### daloRADIUS

- sistema web per la gestione di implementazioni AAA basate sul protocollo RADIUS
- diffusione internazionale, >10.000 utilizzatori/anno

### Altri software/servizi

#### *WoG (Wordlist Generator) e CHO (Crack Hashes Online)*

- strumenti per test di sicurezza password a diffusione internazionale

#### *Cybertrain*

- piattaforma per la distribuzione di macchine virtuali appositamente vulnerabili per il training virtuale in cybersecurity di studenti e/o professionisti di tutto il mondo

#### *Servizi web sviluppati*

- portale dedicato al servizio di emissione dei certificati SSL/TLS per gli utenti del CNR
- portale dedicato al supporto di rete per gli utenti dell'Area della Ricerca di Pisa
- portale per la gestione in autonomia degli account eduroam da parte degli utenti dell'Area della Ricerca di Pisa
- DALP strumento per la protezione degli apparati di rete

## CERTIFICAZIONI e CORSI SPECIALISTICI

### IBM Quantum

- Qiskit Global Summer School 2022 con conseguimento della certificazione "Quantum Excellence"

### Cybersecurity

- corso "OWASP Top 10 - 2021" (Cybrary)
- corso "Identifying Web Attacks Through Logs" (Cybrary)
- corso "Creating a World Class Security Operations Center (SOC)" (Cybrary)
- corso "Windows Privilege Escalation for OSCP & Beyond" (Hackers Academy)
- corso "Linux Privilege Escalation for OSCP & Beyond" (Hackers Academy)

### Networking

- Leviton Network Solutions Certification Course
  - Copper and Optical Fiber Communications Cabling Systems
  - Smooth Sailing Best Practices for Planning a Smart Building

### Infrastructure

- corso di formazione all'utilizzo di Proxmox VE e CEPH in ambienti iperconvergenti (Rackone SRL)
- Linux: Introduction to Shell Scripting for DevOps (Coursera Project Network)

### Formazione GARR

- corso "Zero Trust - Fidarsi è bene, ma zero fiducia è meglio"
- corso di aggiornamento professionale per APM costituito dai seguenti moduli:
  - La struttura della rete GARR
  - Le attività dei Network Operations Center (NOC)
  - Le Policy della Rete GARR
  - L'evoluzione della rete nei data center
  - Configurazione di base dell'accesso
  - LIR, NIC e DNS (IPv4 e IPv6)
  - GARR-CERT - Gestione della sicurezza della rete
  - SCARR: Più prevenzione per maggiore sicurezza
  - Il monitoring della Rete GARR
  - Infrastrutture di Autenticazione e Autorizzazione: la Federazione IDEM
  - GARR Cloud, servizi di Calcolo e storage
  - GARRLab: infrastruttura, tecnologie e risultati
  - Sistemi di videoconferenza
  - Eduroam: installazione di base
- corso "IDEM MDX: Query dinamiche per non annegare in un mare di metadata"
- corso "pfSense (livello base)"
- corso "reti programmabili software defined (SDN)"

Pisa, 5 dicembre 2024