i2CAT Cyber R&I

Características generales | Características del Equipo de Investigación | Características de la Investigación

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	i2CAT Cyber R&I
UNIDAD/DEPARTAMENTO DE PERTENENCIA	Cybersecurity Area
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	i2CAT

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	Jordi Guijarro Olivares	TELÉFONO	638684272
ROL EN EL EQUIPO	Cybersecurity Innovation Manager	MAIL	jordi.guijarro@i2cat.net
WEB DEL EQUIPO	https://i2cat.net/research-topics/cybersecurity/		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	Edificio NEXUS	CENTRO	I2CAT
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Gran Capità
NÚMERO	2	CIUDAD	Barcelona
PROVINCIA	Barcelona	CÓDIGO POSTAL	08034

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	Joan Manel Martin
MAIL	fundacio@i2cat.net
TELÉFONO	34 935 53 25 10
WEB	www.i2cat.net

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	Edificio NEXUS	CENTRO	I2CAT
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Gran Capità
NÚMERO	2	CIUDAD	Barcelona
PROVINCIA	Barcelona	CÓDIGO POSTAL	08034

i2CAT Cyber R&I

Características generales | **Características del Equipo de Investigación** | Características de la Investigación

INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Shuaib Siddiqui	PhD

TRAYECTORIA PROFESIONAL

Dr. Shuaib Siddiqui (shuaib.siddiqui@i2cat.net), has 10+ years of experience working in the academic, research and industry of ICT sector. At present, he is a senior researcher at i2CAT Foundation where he is the Cybersecurity research lead and also the Area Manager for Software Networks research lab. Since he joined i2CAT Foundation in 2015, he has been active in 5G related projects (under H2020) on the topics of control, management, & orchestration platforms based on SDN/NFV, network slicing, and NFV/SDN security. Currently, he is working on the H2020 5GZORRO, as the project coordinator, which targets Zero Touch Automation in a secured and trusted environment for Network and Service Management. He holds a Ph.D. in Computer Science from Technical University of Catalonia (UPC) (Spain), M.Sc. in Communication Systems (2007) from École Polytechnique Fédérale de Lausanne (EPFL), Switzerland, and B.Sc. in Computer Engineering (2004) from King Fahd University of Petroleum & Minerals (KFUPM), Saudi Arabia. He has given several talks at Mobile World Congress, Smart City Expo World Congress, SDN/NFV World Congress and other events. One of his publications titled, “Route Leak Detection Using Real-Time Analytics on local BGP Information”, based on his PhD thesis, received the IEEE Internet Technical Committee (ITC) paper of the year award for 2015.

WEB Y REDES SOCIALES

https://i2cat.net/research-topics/cybersecurity/

MIEMBROS DEL EQUIPO

Compastié, Maxime	Fernández, Carolina	Guijarro Olivares, Jordi
Ortiz Rabella, Nil	Rodriguez Reyes, Daniel	

i2CAT Cyber R&I		
Características generales	Características del Equipo de Investigación	Características de la Investigación

LÍNEAS Y ÁREAS DE INVESTIGACIÓN	
ÁREAS DE INVESTIGACIÓN	**PRINCIPALES LÍNEAS DE INVESTIGACIÓN**
EVALUACIÓN DE SISTEMAS Y CIBERRIESGOS	Detección temprana de ciberriesgos Monitorizado y profiling Cuantificación del riesgo Análisis de riesgos estadísticos y predictivos Recolección de información sobre amenazas
ATAQUES Y DEFENSA ANTE AMENAZAS	Desarrode herramientas de detección de amenazas Phising y Anti-phishing Detección de anomalías Elaboración de mecanismos de respuesta ante ataques
ÁREAS DE INTERÉS	Data mining Cloud Computing Internet de las Cosas Fog Computing Mobile Computing Virtualización y gestión de redes

i2CAT Cyber R&I		
Características generales	Características del Equipo de Investigación	Características de la Investigación

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2019

Jordi Guijarro Olivares, "Devops y Seguridad Cloud" Editorial UOC - Nov/19 - ISBN-13 : 978-8491806233 (https://www.editorialuoc.cat/devops-y-seguridad-cloud)

PUBLICACIONES AÑO 2018

Daniel Guija and Muhammad Shuaib Siddiqui, "Identity and Access Control for micro-services based 5G NFV platforms", 13th International Conference on Availability, Reliability, and Security (AREAS 2018), Hamburg, Germany, Aug 27-30, 2018.

Carolina Canales-Valenzuela, Madalina Baltatu, Luciana Costa, Kai Habel, Volker Jungnickel, Geza Koczian, Felix Ngobigha, Michael C. Parker, Muhammad Shuaib Siddiqui, Eleni Trouva and Stuart D. Walker, "Chapter 9: Security in 5G System Design: Architectural and Functional Considerations and Long Term Research", p.207 - p.226, March, 2018, WILEY

PUBLICACIONES AÑO 2017

G. Gardikis; K. Tzoulas; K. Tripolitis; A. Bartzas; S. Costicoglou; B. Gastón; C. Fernández; C. Dávila; L. Jacquin; H. Attak; D. Katsianis; I. Neokosmidis; T. Batista; R. Preto; A. Lioy; A. Litke; N. Papadakis; D. Papadopoulos; A. Pastor; J. Nuñez; N. Davri; G. Xylouris; M. Kafetzakis; M. Terranova; E. Trouva; Y. Angelopoulos; A. Kourtis. "SHIELD: A Novel NFV-based Cybersecurity Framework", 3rd IEEE Conference on Network Softwarization (NetSoft 2017)

M.C. Mont; H. Attak; Y. Beres; C. Fernandez; B.Gaston; J. Ludovic; A. Lioy; J. Nunez; A. Pastor. "SHIELD -Securing against intruders and other threats through a NFV-enabled environment. Guide to Security in SDN and NFV - Challenges, Opportunities, and Applications". Springer, 2017

PUBLICACIONES AÑO 2016

M. S. Siddiqui, E. Escalona, E. Trouva, M.A. Kourtis, D. Kritharidis, K. Katsaros, S. Spirou, C. Canales, M. Lorenzo, "Policy based virtualised security architecture for SDN/NFV enabled 5G access networks," in 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFVSDN), 2016, pp. 44–49.

i2CAT Cyber R&I

Características generales | Características del Equipo de Investigación | **Características de la Investigación**

PROYECTOS RELEVANTES

H2020-DS04-2015 SHIELD proposed a universal solution for dynamically establishing and deploying virtual security infrastructures into ISP and corporate networks. SHIELD builds on the Network Functions Virtualisation (NFV) concept, considering virtual Network Security Functions (vNSFs), to be instantiated within the network infrastructure, effectively monitoring and filtering network traffic in an adaptive and distributed manner. TID was focused on business-oriented use cases and market needs, leading the innovation management activities, and contributed to the development of the vNSF environment and the smart security orchestration mechanisms.

H2020-SU-ICT-01-2018 CARAMEL (Artificial Intelligence based cybersecurity for connected and automated vehicles) CARAMEL's goal is to proactively address modern vehicle cybersecurity challenges applying advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques, and also to continuously seek methods to mitigate associated safety risks. Although past initiatives and cybersecurity projects related to the automotive industry have reached to security assurance frameworks for networked vehicles, several newly introduced technological dimensions like 5G, autopilots, and smart charging of Electric Vehicles (EVs) introduce cybersecurity gaps, not addressed satisfactorily yet. Considering the entire supply chain of automotive operations, CARAMEL targets to reach to commercial anti-hacking IDS/IPS products for the European automotive cybersecurity and to demonstrate their value through extensive attack and penetration scenarios. https://www.h2020caramel.eu/

H2020-SU-DS03-2019 PALANTIR aims at bridging the gap between large enterprises and SMEs/MEs, by providing multi-layered, infrastructure-wide threat monitoring, cyber-resiliency and knowledge sharing in a heterogeneous ecosystem, while at the same time being able to market these services to third parties in the form of Security-as-a-service (SECaaS). PALANTIR will implement a coherent privacy assurance, data protection, incident detection and recovery framework, focusing on the case of highly dynamic service-oriented systems and networks, taking advantage of their inherent programmability features and abstractions. https://cordis.europa.eu/project/id/883335

H2020-ICT-2014 CHARISMA (Converged heterogeneous advanced 5G cloud-RAN architecture for intelligent and secure media access): CHARISMA proposes an intelligent hierarchical routing and paravirtualised architecture that unites two important concepts: devolved offload with shortest path nearest to end-users and an end-to-end security service chain via virtualized open access physical layer security (PLS). The CHARISMA architecture meets the goals of low-latency and security required for future converged wireless/wireline advanced 5G networking. http://www.charisma5g.eu/

TDA in Cybersecurity: Users' exposition to a cyberthreat is a big challenge to solve, according to the Cybersecurity Agency of Catalonia. This project intends to develop solutions to solve that. It is framed in the Research & Innovation in Digital Advanced Technologies (TDA) of Smartcatalonia. The Agency wishes to strengthen and update its technological capacities on: Predicting cyberthreats' impact on the information systems of the Government of Catalonia. - Determining which users are more susceptible of being cyberthreats' victims. - Adopting users' protection actions. https://i2cat.net/projects/tda-ciberseguretat/