About the University of Granada

The UGR is the **leading University** in Spain in **ICT research**, and the third one in Europe according to the NTU ranking. The UGR has extensive experience in **EU projects**, with 66 active projects in FP7 (312 presented, 21% success rate, 18M€), and 25 in H2020 (240 presented, 12% success rate, 6M€).

In addition, the *Faculty of Computer Science and Telecommunication Engineering* of the UGR is ranked in the 33rd position in the Shanghai ranking.

UNIVERSIDAD
DE GRANADA

Contact Information:

Pedro García Teodoro

ETS de Ingenierías Informática y de Telecomunicación
Periodista Daniel Saucedo Aranda, s/n
18071-Granada (Spain)
+34 958 24 23 05 | nesg@ugr.es
https://nesg.ugr.es

CITIC-UGR

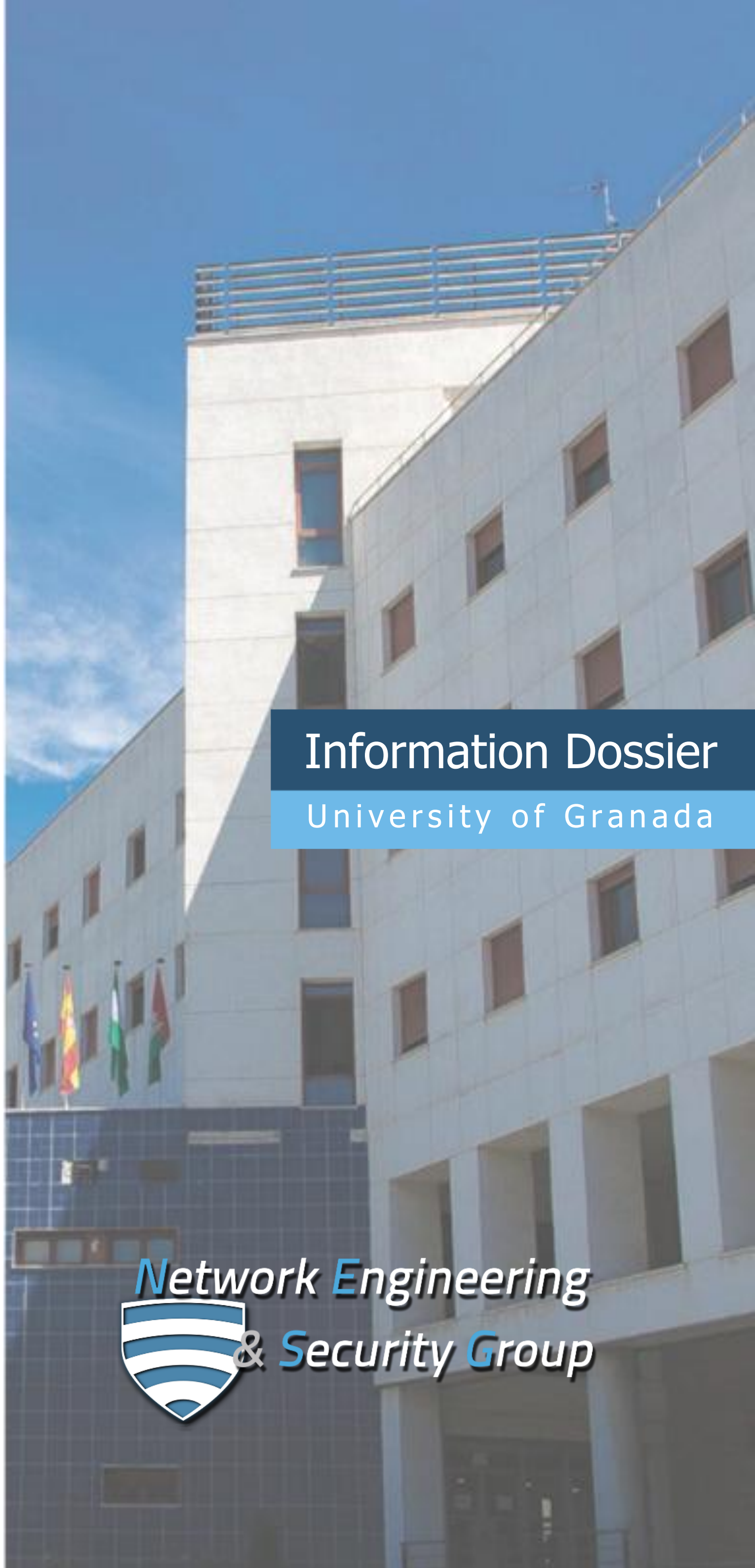
About **NESG**

NESG is a **cybersecurity** research group of the University of Granada (UGR), in Spain. **NESG** is focused on providing and improving security in networks, systems and services, either for wired, wireless and mobile environments.

NESG is member of the **CITIC-UGR** (http://citic.ugr.es) and leads the **UGR CyberSecurity Group** (UCyS - https://ucys.ugr.es), with more than 20 university professors with multidisciplinary expertises in areas such as network and system security, cryptography, secure hardware and software design, cyberlaw, artificial intelligence, machine learning and Big Data.

In addition, through the UGR, **NESG** is founding member of the **Spanish Network in Cybersecurity Research** (RENIC - https://www.renic.es/en), in turn member of the **European Cyber-Security Organisation** (ECSO - https://www.ecs-org.eu/).

Likewise, **NESG** is also member of the **Big Data Value Association** (BDVA - https://www.bdva.eu/).



Information Dossier

University of Granada

Network Engineering
& Security Group

Data processing and networkmetrics

The networkmetrics research line seeks to take advantage of multivariate analysis and machine learning tools to tackle problems in communication networks, with cybersecurity as main example. An effective detection of cybersecurity incidents requires the combination of several and disparate data sources. This makes cybersec a typical Big Data problem, where the challenge is to handle tons of information from heterogeneous sources at a fast pace. In NESG, we develop new analysis methods to handle Multivariate Big Data, which are also of value in applications like IoT monitoring or Industry 4.0, and in other domains, like chemometrics, bioinformatics and personalized medicine.

Main contributions

- *Camacho, J., Pérez-Villegas, A., García-Teodoro, P., Maciá-Fernández, G. PCA-based Multivariate Statistical Network Monitoring for Anomaly Detection. Computers & Security, 2016, 59: 118-137.*
- *Camacho, J., Rodríguez-Gómez, R., Saccenti, E. Group-wise Principal Component Analysis for Exploratory Data Analysis. Journal of Computational and Graphical Statistics , 2017, 26 (3): 501-512.*
- *Camacho, J., Magán-Carrión, R., García-Teodoro, P., Treinen, J.J. Networkmetrics: Multivariate Big Data Analysis in the Context of the Internet. Journal of Chemometrics, 2016, 30: 487.*
- *UGR'16: A New Dataset for the Evaluation of Cyclostationarity-Based Network IDSs (2018).*

Ethical hacking and digital forensics

Ethical hacking and digital forensics constitute well-known topics aimed at testing and recovering systems and services. Some specific aspects addressed by NESG in this area are:

- Development of new methodologies
- Techniques for fingerprinting
- Exploitation techniques and their countermeasures
- Ethical Hacking capabilities training
- Privacy mechanisms
- Malware analysis and reverse engineering.
- Privacy mechanisms
- Tools and methodologies for digital forensics

NESG leads the *HACKIIT team* participating in CTF competitions.

Main contributions

- *A. Alhazmi, G. Maciá-Fernández, J. Camacho, "Torrent Forensics: Are your Files Being Shared in the BitTorrent Network?", CYBER'2017.*
- *L. Sánchez Casado, G. Maciá Fernández, P. García Teodoro and Nils Aschenbruck, "Identification of Contamination Zones for Sinkhole Detection in MANETs", Journal of Network and Computer Applications (2015).*
- *R.A. Rodríguez-Gómez, G. Maciá-Fernández, P. García-Teodoro, M. Steiner, D. Balzarotti, "Resource Monitoring for the Detection of Parasite P2P Botnets", Computer Networks (2014).*
- *G. Maciá-Fernández, J.E. Díaz-Verdejo, P. García-Teodoro, "Evaluation of a Low-Rate DoS Attack Against Application Servers", Computers & Security (2008).*

Intrusion detection and protection

Systems and users are very vulnerable to attacks of different typology and impact: virus, trojans, ransomware, spyware, data leakage, etc. This way, a principal topic addressed by NESG is that of protecting network environments by means of two subsequent procedures: detection of malicious behaviors, and adoption of countermeasures.

For that, specific research lines are:

- Behavior modeling and classification (multivariate, HMM, clustering, SVM, GA, …)
- Anomaly detection
- Malware detection and classification
- Countermeasures and response mechanisms

Main contributions

- *NESG: "Mobile Device Dynamic Security Management". Spanish TIN2017-83494-T project, 2018-2020.*
- *J.A. Gómez-Hernández, L. Álvarez-González, P. García-Teodoro: "R-Locker: Thwarting Ransomware Action through a Honeyfile-based Approach", Computers & Security, Vol. 73, pp. 389-398, 2018.*
- *Ruiz-Heras, P. García-Teodoro, L. Sánchez-Casado: "ADroid: Anomaly-based Detection of Malicious Events in Android Platforms", International Journal of Information Security, vol. 16, n. 4, pp. 371-384, 2017.*
- *P. García, J.E. Díaz-Verdejo, G. Maciá, E. Vázquez: "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges". Computers & Security, vol. 28; pp. 18-28, 2009.*

Cyberlaw

Cyberlaw is a very extensive field of research that, within the NESG group, focuses on the analysis of International and European regulations and their application in domestic law. The methodological approach is interdisciplinary. The objective is to analyze the state of the regulations, their scope and nature and the problems posed by their application with the purpose of proposing new norms or reforms of existing ones when they are not sufficiently effective. The main areas of study are security of network and information systems, cybersecurity, data protection and Internet governance.

Main contributions

- *Robles Carrillo, M. (2017). El proceso de reforma de la ICANN: objetivos, régimen jurídico y estructura orgánica. Revista de Privacidad y Derecho Digital, año II, Nº 7, pp. 25-65.*
- *Robles Carrillo, M. (2016). Los principios rectores de la cooperación internacional en el ciberespacio. Alcance y contenido del consenso entre los Estados. Revista Iberoamericana de Derecho Internacional y de la Integración, Nº 5.*
- *Robles Carrillo, M. (2016). Amenaza y uso de la fuerza a través del ciberespacio: un cambio de paradigma. Revista Latinoamericana de Derecho Internacionalatin American Journal of International Law, Nº 4.*