NETWORK ENGINEERING & SECURITY GROUP - UCYS - DE LA UNIVERSIDAD DE GRANADA

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	**Network Engineering & Security Group – UcyS**
UNIDAD/DEPARTAMENTO DE PERTENENCIA	**Teoría de la Señal, Telemática y Comunicaciones**
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	**Universidad de Granada**

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	**Pedro García Teodoro**	TELÉFONO	958242305
ROL EN EL EQUIPO	Director / Coordinador	MAIL	pgteodor@ugr.es
WEB DEL EQUIPO	www.nesg.ugr.es		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	-	CENTRO	-
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Periodista Daniel Saucedo Aranda
NÚMERO	s/n	CIUDAD	Granada
PROVINCIA	Granada	CÓDIGO POSTAL	18071

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	-		
MAIL	rectora@ugr.es		
TELÉFONO	958243003	WEB	www.ugr.es

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	Hospital Real	CENTRO	-
TIPO DE VÍA	Avenida	NOMBRE DE LA VÍA	Del Hospicio
NÚMERO	s/n	CIUDAD	Granada
PROVINCIA	Granada	CÓDIGO POSTAL	18071

INVESTIGADOR/ES PRINCIPAL/ES

NOMBRE	TITULACIONES
Pedro García Teodoro	Doctor en Ciencias Físicas

TRAYECTORIA PROFESIONAL

- 26 años de experiencia
- Seguridad en redes
- Sistemas y servicios
- Reconocimiento automático del habla
- eLearning...

WEB Y REDES SOCIALES

MIEMBROS DEL EQUIPO

- Gabriel Maciá Fernández
- José Camacho Páez
- Noemí M. Fuentes García
- Rafael A. Rodríguez Gómez
- Roberto Magán Carrión

LÍNEAS Y ÁREAS DE INVESTIGACIÓN

PRINCIPALES LÍNEAS DE INVESTIGACIÓN	ÁREAS DE INVESTIGACIÓN
• Elaboración de mecanismos de respuesta ante ataques • Desarrollo de herramientas de detección de amenazas • Desarrollo de mecanismos de recolección de datos • Detección de anomalías • Detección y monitorizado de ataques • Detección y eliminación de malware • IDS/IPS/firewalls	• Ataques y defensa ante amenazas
• Estudio de patrones • Mecanismos de recolección de datos • Auditoría de sistemas de seguridad	• Evaluación de sistemas y ciberriesgos
• Controles de acceso basados en comportamiento	• Gestión de la identidad
• Monitorizado y seguridad de redes • Sistemas de control industrial en redes (agua, electricidad, alimentación, transporte, finanzas, salud, esalud, ect.) • Mecanismos de recuperación de datos • Detección de software malicioso	• Infraestructuras críticas
• Data mining • Seguridad de redes • Seguridad en big data • Seguridad en dispositivos móviles	• Otras áreas de interés

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES 2016

ADroid: Anomaly-based Detection of Malicious Events in Android Platforms
A. Ruiz-Heras, P. García-Teodoro, L. Sánchez-Casado, 2016

Multivariate Big Data Analysis in the Context of the Internet
J. Camacho, R. Magán-Carrión, P. García-Teodoro, 2016

PCA-based Multivariate Statistical Network Monitoring for Anomaly Detection
J. Camacho, A. Pérez-Villegas, P. García-Teodoro, G. Maciá-Fernández, 2016

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES 2015

Automatic Generation of HTTP Intrusion Signatures by Selective Identification of Anomalies
P. García-Teodoro, J.E. Díaz-Verdejo, J. E. Tapiador, R. Salazar-Hernández, 2015

A Model of Data Forwarding in MANETs for Lightweight Detection of Malicious Packet Dropping
L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, R. Magán-Carrión, 2015

Identification of Contamination Zones for Sinkhole Detection in MANETs
L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, N. Aschenbruck, 2015

Multivariate Statistical Approach for Anomaly Detection and Lost Data Recovery in Wireless Sensor Networks
R. Magán-Carrión, J. Camacho-Páez, P. García-Teodoro, 2015

Analysis and Modeling of Resources Shared in the BitTorrent Network
R.A. Rodríguez-Gómez, G. Maciá-Fernández, P. García-Teodoro, 2015

PUBLICACIONES 2014

Resource Monitoring for the Detection of Parasite P2P Botnets
R.A. Rodríguez-Gómez, G. Maciá-Fernández, P. García-Teodoro, M. Steiner, D. Balzarotti, 2014

Tackling the Big Data 4 Vs for Anomaly Detection
J. Camacho-Páez, G. Maciá-Fernández, J.E. Díaz-Verdejo, P. García-Teodoro, 2014

A Novel Collaborative Approach for Sinkhole Detection in MANETs
L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, N. Aschenbruck, 2014

A Multiagent Self-healing System against Security Incidents in MANETS
R. Magán-Carrión, J. Camacho-Páez, P. García-Teodoro, 2014

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES 2013

Tampered Data Recovery in WSNs through Dynamic PCA and Variable Routing Strategies
R. Magán-Carrión, J. Camacho-Páez, P. García-Teodoro, 2013

A Generalizable Dynamic Flow Pairing Method for Traffic Classification
J. Camacho, P. Padilla, P. García-Teodoro, J.E. Díaz-Verdejo, 2013

Survey and Taxonomy of Botnets through Life-cycle
R. Rodríguez, G. Maciá, P. García-Teodoro, 2013

Stochastic Traffic Identification for Security Management: eDonkey Protocol as a Case Study
R. Rodríguez Gómez, G. Maciá Fernández. P. García Teodoro, 2013

A Security Response Approach based on the Deployment of Mobile Agents
R. Magán-Carrión, J. Camacho-Páez, P. García-Teodoro, 2013

PUBLICACIONES 2012

A Segmental Parameterisation and Statistical Modelling of E-mail Headers for Spam Detection
F.J. Salcedo-Campos, J.E. Díaz-Verdejo, P. García-Teodoro, 2012

An Efficient Cross-Layer Approach for Malicious Packet Dropping Detection in MANETs
L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, 2012

PUBLICACIONES 2011

New Heuristics for Node and Flow Detection in eDonkey-based Services
R. Rodríguez, G. Maciá, P. García-Teodoro, 2011

PUBLICACIONES 2010

Automatic Signature Generation for Network Services through Selective Extraction of Anomalous Contents
P. García, P. Muñoz, D. Ruete, 2010

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES 2009

Anomaly Detection in P2P Networks Using Markov Modelling
J.E. Díaz, G. Maciá, P. García, J. Nuño, 2009

Fraud in Roaming Scenarios: An Overview
G. Maciá-Fernández, P. García, J.E. Díaz-Verdejo, 2009

Mathematical Model for Low-Rate DoS Attacks Against Applications Servers
G. Maciá-Fernández, J.E. Díaz-Verdejo, P. García, 2009

Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges
P. García, J.E. Díaz-Verdejo, G. Maciá, E. Vázquez, 2009

PROYECTOS RELEVANTES

Sistema información de detección de fugas de información en deep web
Objetivos: Este proyecto persigue construir un sistema de monitorización de información en la deep web. El módulo que NESG desarrolla permite obtener información intercambiada en redes P2P y en redes IRC, con el fin de poder monitorizar eventos de interés, intercambios específicos, etc.

Auditoría de seguridad de la red de Grupo Trevenque
Objetivos: En este proyecto se realiza la auditoría de la seguridad de los sistemas y redes de Grupo Trevenque. Trevenque se ha convertido en el operador Cloud más importante de Andalucía, con su Cloud Center en Andalucía.

MINECO 2014
Objetivos: VERITAS: Visualización De Eventos en Red Inteligente para el Tratamiento y Análisis de la Seguridad (TIN2014-60346-R)

MICIN 2011
Objetivos: SuMA: Supervivencia de redes MANET ante incidentes de seguridad (TEC2011-22579)

Survela (4iq)
Objetivos: Sistema de detección de fugas de información en deep web (CTA 15/795)

ProtectWise Inc
Objetivos: Exploración de datos sobre información de seguridad en red

KPN Mobile International Network Spain S.L.
Objetivos: Investigación sobre fraude en telecomunicaciones. El fraude en roaming

SADESI (Junta de Andalucía)
Objetivos: Mejora de la gestión de red mediante análisis y caracterización del tráfico en redes corporativas de la Junta de Andalucía

Robotiker-Tecnalia
Objetivos: Tele-rehabilitación efectiva en el hogar: investigación y desarrollo de sistemas, técnicas, métodos y mecanismos (TeleREHAB)