Procesado seguro de la información

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

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	**Procesado seguro de la información**
UNIDAD/DEPARTAMENTO DE PERTENENCIA	**Seguridad y privacidad**
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	**GRADIANT (Centro Tecnológico de Telecomunicaciones de Galicia)**

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	**Juan González Martínez**	TELÉFONO	+34 986120430
ROL EN EL EQUIPO	Director del área de de Seguridad y Privacidad	MAIL	jgonzalez@gradiant.org
WEB DEL EQUIPO	https://www.gradiant.org/tecnologias/seguridad-y-privacidad/		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	Citexvi	CENTRO	Campus Universitario de Vigo
TIPO DE VÍA	Rúa	NOMBRE DE LA VÍA	Fonte das Abelleiras
NÚMERO	s/n	CIUDAD	Vigo
PROVINCIA	Pontevedra	CÓDIGO POSTAL	36310

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	Sara Campos Márquez
MAIL	gradiant@gradiant.org
TELÉFONO	+34 986120430
WEB	www.gradiant.org

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	Citexvi	CENTRO	Campus Universitario de Vigo
TIPO DE VÍA	Rúa	NOMBRE DE LA VÍA	Fonte das Abelleiras
NÚMERO	s/n	CIUDAD	Vigo
PROVINCIA	Pontevedra	CÓDIGO POSTAL	36310

Procesado seguro de la información

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

INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Jaime Loureiro Acuña	Ingeniero de Telecomunicación Máster en procesado de señal en aplicaciones multimedia

TRAYECTORIA PROFESIONAL

Entre el 2010 y 2016 ha trabajado para el Grupo de Tecnologías de la Información de la Universidad de Vigo como investigador contratado. Ha centrado su trabajo en el diseño e implementación de protocolos seguros para la distribución y ejecución eficiente de contenidos multimedia. Durante esa etapa publica el siguiente artículo "Improving the virtualization of rich applications by combining VNC and streaming protocols at the hypervisor layer". Además, ha colaborado en numerosos proyectos de I+D (SMART HOSPITAL y/o SCAPE) relacionados con la seguridad y la privacidad de los datos donde se especializa en técnicas de protección de datos tanto software como hardware. En Noviembre del 2016 se incorpora a Gradiant asumiendo el rol de investigador de seguridad y participando como jefe de proyecto en BlackICE HSM donde se especializa en tecnologías criptográficas avanzadas para el procesado de información en entornos no confiables. Desde el 2018 imparte cursos formativos sobre criptografía en redes distribuidas DLTs y blockchain, capacitando en dicha tecnología a diversas empresas. Desde Enero de 2019 lidera la línea tecnológica de procesado seguro de la información dentro del área de Seguridad y Privacidad. En la actualidad forma parte del comité técnico de la Red de Excelencia Nacional en Tecnologías de Seguridad y Privacidad (ÉGIDA). Es socio fundador de la EBT Infinbox de la Universidad de Vigo que ha obtenido financiación en la aceleradora FINODEX del proyecto Europeo FI-WARE. A través de la spin-off, ha participado activamente en la transferencia al mercado de soluciones como TvTab y SmartHospital.

WEB Y REDES SOCIALES

MIEMBROS DEL EQUIPO

Jiménez Balsa, Gonzalo	Román García-Pardo Rodríguez, Hugo	Rodríguez Silva, Daniel Amós
Álvarez Pérez, David	Martín Ruiz, Carlos	Vázquez Saavedra, Adrián

Procesado seguro de la información		
Características generales	Características del Equipo de Investigación	Características de la Investigación

LÍNEAS Y ÁREAS DE INVESTIGACIÓN	
ÁREAS DE INVESTIGACIÓN	**PRINCIPALES LÍNEAS DE INVESTIGACIÓN**
ATAQUES Y DEFENSA ANTE AMENAZAS	Nuevos tipos de Malware
GESTIÓN DE LA IDENTIDAD	Autenticación criptográfica Computación segura multiparte Control de Acceso y Autenticación
INTERACCIÓN CON EL USUARIO USABILIDAD	Algoritmos de clave pública usable Usabilidad de los sistemas de autenticación
PROCESADO DE DATOS	Procesamiento seguro de datos Protección de datos (integridad y disponibilidad) Protección de datos (confidencialidad)
PRIVACIDAD	Protocolos criptográficos de preservación de la privacidad Cifrado homomórfico de celosías Sistemas de autenticación anónimos Manejo de la identidad Identidad parcial Privacidad en Cloud Privacidad en IoT
SISTEMAS FIABLES Y ACTUALIZABLES	Computación Segura Seguridad / Privacidad mediante el diseño
ÁREAS DE INTERÉS	Criptografía Criptografía post-cuántica Cloud Computing Internet de las Cosas
OTRAS	Seguridad en sistemas distribuidos y blockchain

Procesado seguro de la información

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

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2016

Rodríguez-Silva, D. A. & Loureiro-Acuña, J. Improving the virtualization of rich applications by combining VNC and streaming protocols at the hypervisor layer. Softw. Pract. Exp. (2016).

PUBLICACIONES AÑO 2015

Rodríguez Silva, D. A., González Castano, F. J., Adkinson Orellana, L., Pedrero López, B. (2015, May). Cloud Spreadsheets supporting Data Processing in Encrypted Domain. Publication presented at Proceedings of 5th International Conference on Cloud Computing and Services Science (CLOSER 2015)

PUBLICACIONES AÑO 2013

Rodríguez Silva, D. A., Adkinson Orellana, L., Nuñez Taboada, D. M., González Castaño, F. J. (2013, May). PaaS Federation Analysis for Seamless Creation and Migration of Cloud Applications. Publication presented at Proceedings of 3rd International Conference on Cloud Computing and Services Science (CLOSER 2013).

Troncoso-Pastoriza, J. R., González-Jiménez, D. & Pérez-González, F. Fully Private Noninteractive Face Verification. IEEE Trans. Inf. Forensics Secur. 8, 1101–1114 (2013).

Rodríguez Silva, D. A., Adkinson Orellana, L., Fernández Díaz, V., González Castaño, F. J. (2013, May). Towards Virtualization of Rich Applications for Distribution under a SaaS Model. Publication presented at Proceedings of 3rd International Conference on Cloud Computing and Services Science (CLOSER 2013).

PUBLICACIONES AÑO 2012

Rodríguez Silva, D. A., Adkinson Orellana, L., González Castano, F. J., Armino Franco, I., González-Martinez, D. (2012, June). Video surveillance based on cloud storage. Publication presented at 2012 IEEE Fifth International Conference on Cloud Computing (CLOUD 2012).

PUBLICACIONES AÑO 2011

Rodríguez Silva, D. A., González Castano, F. J., Adkinson Orellana, L., Fernández Cordeiro, A., Troncoso Pastoriza, J. R., & González Martínez, D. (2011, May). Encrypted domain processing for cloud privacy. Publication presented at Proceedings of 1st International Conference on Cloud Computing and Services Science (CLOSER 2011

Adkinson Orellana, L., Rodríguez Silva, D. A., Gonzalez Castano, F. J., Gonzalez Martinez, D. (2011, May). Sharing Secure Documents in the Cloud-A Secure Layer for Google Docs. Publication presented at Proceedings of 1st International Conference on Cloud Computing and Services Science (CLOSER 2011)

PUBLICACIONES 2010

Adkinson Orellana, L., Rodríguez Silva, D. A., Gil Castiñeira, F., Burguillo Rial, J. C. (2010, May). Privacy for google docs: Implementing a transparent encryption layer. Publication presented at 2nd Cloud Computing International Conference (CloudViews 2010)

PROYECTOS RELEVANTES
IMPULSE (2021-2023): IMPULSE es un proyecto de investigación y desarrollo H2020 orientado al estudio, diseño y desarrollo de soluciones de gestión de identidad basadas en tecnología DLT/Blackchain para el acceso a servicios públicos.
ÉGIDA (2020-2022): ÉGIDA nace como una red formada por 78 investigadores, de los cuales el 27% son doctores, con más de 15 años de experiencia en el ámbito de la seguridad y privacidad de sistemas e información, distribuida en 4 centros de trabajo ubicados en Galicia, Andalucía y País Vasco. Actualmente, los miembros de ÉGIDA facturan más de 9,7 millones de euros de euros en esta tecnología Cervera, lo que supone en promedio el 14% de sus ingresos anuales totales. En el proyecto se trabajará en 4 líneas tecnológicas: criptografía aplicada, protección de la identidad y privacidad, tecnologías para el desarrollo de sistemas de información seguros y seguridad en sistemas distribuidos. Además de estas cuatro actividades técnicas, ÉGIDA cuenta con otras dos actividades transversales, una orientada a la mejora de las capacidades investigadoras y otra relacionada con el impacto de la red.
IRMAS 2.0 (2020-2023): Este proyecto se crea como continuación/consolidación del proyecto IRMAS, con el fin de trabajar en el diagnóstico y en la solución de problemas de seguridad de los sistemas de Seguridad de la Información, a través de la creación de diversos proyectos e iniciativas. En concreto, las actividades de innovación de este proyecto se organizan en tres áreas o líneas de trabajo, protección de la información, protección contra el fraude digital y ciberinteligencia.
IRMAS (2017-2020): Protección de sistemas de información basado en el análisis de datos; Sistemas de control de acceso avanzado y verificación de identidad; Protección y compartición segura de activos digitales basada en el uso de tecnologías criptográficas hardware y software.
BLACK ICE HSM (2016-2019): Este proyecto proporciona una plataforma de gestión de dispositivos criptográficos hardware (HSM) en la nube para que puedan ser ofrecidos como servicio con la posibilidad de programar módulos personalizados para cubrir las necesidades de diferentes verticales. En particular, el proyecto proprociona módulos específicos para un vertical de voto electrónico siguiendo los requisitos definidos por Scytl en base al protocolo utilizado en su solución de e-voting.
SPED-Firma (2018): Desarrollo de una algoritmo para la verificación biométrica de firma en el dominio cifrado.
SCAPE (2012-2017): El objeto de este proyecto es investigar tecnologías que permitan ofrecer mecanismos avanzados de seguridad en la nube. El proyecto se compone de tres subproyectos: SafeGDocs (SP1), que permite cifrar documentos en el SaaS de Google Docs mediante una extensión de Firefox; Criptonube (SP2), que permite gracias al uso de criptoprocesadores ofrecer un entorno seguro de ejecución dentro un proveedor cloud no confiable; y CloudSeep (SP3), que permite procesar datos de forma segura en un cloud utilizando técnicas de procesado de señal en el dominio cifrado.
TACTICA-SPED (2015): El proyecto consta de tres desarrollos: 1) Implementación de un criptosistema en base a la descripción realizada en un paper. El criptosistema debe de funcionar con polinomios de n dimensiones. 2) Desarrollo de operaciones seguras (convolución, diezmado, etc.) que utilicen el criptosistema. 3) Implementación de un prototipo basado en toolbox en Matlab.
HIGEA (2012-2014): Creación de una aplicación orientada a la gestión de información clínica en la nube que almacene de forma segura datos médicos. Para garantizar la seguridad de la información en la nube, se cifrará el contenido de la base de datos asociada a la aplicación clínica, y se desarrollarán los mecanismos de seguridad necesarios para que dicha aplicación pueda realizar consultas eficientes sobre la base de datos como si su contenido estuviese en claro.
SAFECLOUD (2009-2012): Seguridad y privacidad con tecnologías de procesado cifrado en Cloud Computing. Se trata de desarrollar una plataforma segura para el desarrollo de aplicaciones cloud, Estudiar los mecanismos de procesado en el dominio cifrado para adecuarlos a un contexto cloud y optimizar eficiencia de algoritmos y buscar mecanismos de eficiencia desde el punto de vista de la arquitectura cloud.