

HORIZON
2020

Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures

Resultados resumidos

Un marco de seguridad y privacidad se ocupa de la ciberseguridad

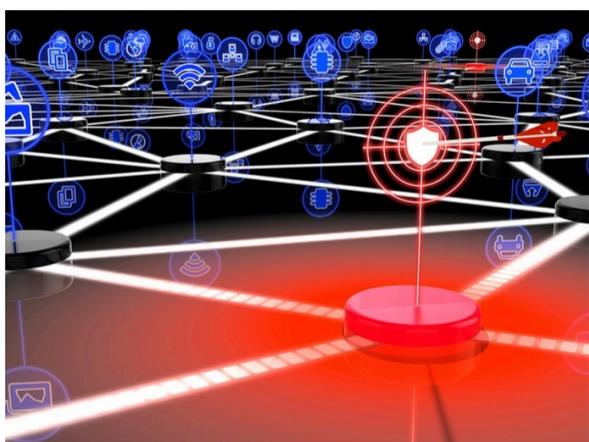
Los sistemas ciberfísicos (SCF) basados en el internet de las cosas (IdC) y las arquitecturas de nube virtualizadas presentan riesgos nuevos e inesperados que no pueden solucionarse plenamente mediante las actuales soluciones de seguridad de última generación. Una iniciativa de la Unión Europea (UE) presentó una solución que aporta una seguridad y confianza máximas.



ECONOMÍA DIGITAL



SEGURIDAD



© BeeBright, Shutterstock

Se necesitan nuevos paradigmas y métodos para incorporar la seguridad desde el primer momento en un sistema TIC, adaptarlo a las condiciones de seguridad cambiantes, reducir la necesidad de corregir fallos tras la implantación y proporcionar garantías de que es seguro y fiable en todo momento. El proyecto [ANASTACIA](#), financiado con fondos europeos, abordó estas preocupaciones a través de la investigación, el desarrollo, la demostración y la validación de una técnica integral que facilita la confianza y seguridad por diseño para SCF heterogéneos, distribuidos y en evolución dinámica.

Solución para la vulnerabilidad creciente de los sistemas TIC actuales

«Con este fin, desarrollamos un marco de seguridad y privacidad que aborda la complejidad de las arquitecturas del IdC y la naturaleza distinta de los posibles ataques», explica el coordinador Stefano Bianchi. El marco permite tomar decisiones autónomas empleando nuevas tecnologías de red como las redes definidas por «software» (SDN, por sus siglas en inglés) y la virtualización de funciones de red (NFV, por sus siglas en inglés), así como metodologías y herramientas dinámicas e inteligentes de aplicación y vigilancia de la seguridad.

El proyecto se basó en funcionalidades de SDN y NFV para integrar los productos de seguridad desarrollados y aportar una forma dinámica de implementarlos cuando sea necesario. Las SDN y la NFV constituyen asimismo una solución de seguridad para SCF e el IdC con elevada conectividad. «Al proponer un marco de seguridad conforme con la privacidad y seguridad para proteger SCF y arquitecturas del IdC complejos, ANASTACIA abarcará muchos sectores de TIC y ámbitos de aplicación distintos», comenta Bianchi.

El marco incluye un paradigma de desarrollo de seguridad basado en el cumplimiento de las mejores prácticas de seguridad y el uso de componentes y facilitadores de seguridad, además de un sello dinámico de seguridad y privacidad global que combina normas de seguridad y privacidad como el Reglamento General de Protección de Datos y las normas ISO con seguimiento en tiempo real y pruebas en línea. Además, incluye un conjunto de componentes distribuidos de confianza y seguridad y facilitadores capaces de orquestar e implementar dinámicamente políticas de seguridad de usuarios y medidas resilientes con evaluación de riesgos dentro de SCF y arquitecturas del IdC complejos y dinámicos.

Estrategias inteligentes de planificación, aplicación y control de seguridad

Las partes interesadas afectadas directamente por aspectos de ciberseguridad y privacidad se verán beneficiadas. Arquitectos de soluciones y «software», analistas y gestores de proyectos aprovecharán el paradigma de desarrollo de seguridad y los desarrolladores e integradores sacarán el máximo provecho de los componentes y facilitadores de seguridad y confianza distribuidos. Responsables principales de información, de seguridad, de seguridad de la información y gestores aprovecharán el sello dinámico de seguridad y privacidad.

Y Bianchi concluye: «ANASTACIA desarrolló metodologías y herramientas para ofrecer garantías adecuadas de que los sistemas TIC desarrollados se mantienen seguros y fiables, y satisfacer la necesidad de niveles certificados de garantía en los que la seguridad se considera la preocupación principal. En última instancia, las soluciones tienen por objeto liberar a los usuarios finales de la carga de tener que comprobar continuamente el estado de seguridad y el respeto de la privacidad del

SCF y la infraestructura del IdC que se controla».

El marco contribuirá asimismo a concienciar sobre las ciberamenazas y las cuestiones de privacidad, y aportará soluciones prácticas para aplicar los enfoques metodológicos e incrementar el nivel de ciberseguridad y privacidad en el [mercado único digital](#) de la UE.

Palabras clave

ANASTACIA, seguridad, privacidad, SCF, IdC, confianza, ciberseguridad, SDN, NFV

Descubra otros artículos del mismo campo de aplicación



[Cuando la tecnología nos cubre las espaldas](#)



[Información y tecnologías médicas combinadas con inteligencia artificial mejoran la clasificación de masas](#)





Autobuses personalizados para la economía compartida



Una plataforma puntera para hacer realidad una red sensible a las aplicaciones



Información del proyecto

ANASTACIA

Identificador del acuerdo de subvención:
731558

[Sitio web del proyecto](#)

DOI
[10.3030/731558](https://doi.org/10.3030/731558)

Proyecto cerrado

Fecha de la firma de la CE
27 Noviembre 2016

Fecha de inicio
1 Enero 2017

Fecha de
finalización
31 Diciembre 2019

Financiado con arreglo a

INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)

Coste total
€ 5 420 208,75

Aportación de la UE
€ 3 999 208,75

Coordinado por
ALGOWATT SPA
 Italy

Última actualización: 7 Agosto 2020

Permalink: <https://cordis.europa.eu/article/id/421747-privacy-and-security-framework-tackles-cybersecurity/es>

European Union, 2025

