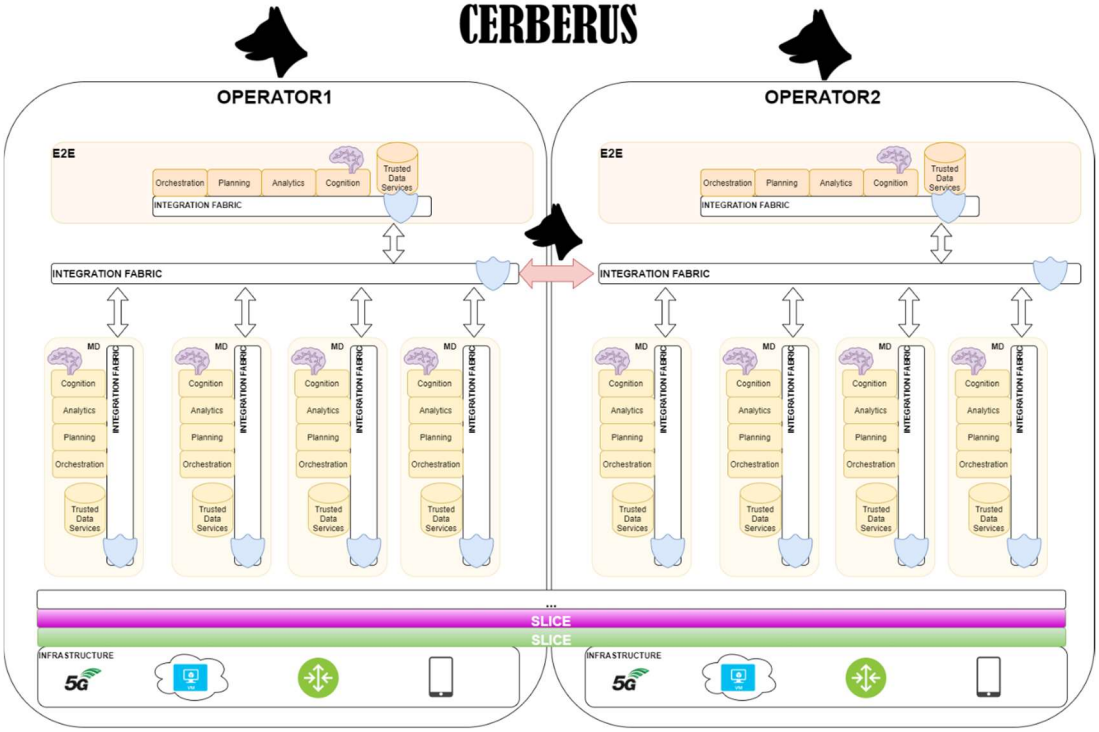
Los proyectos UNICO 5G I+D - UMU

Proyecto UNICO 5G I+D- CERBERUS Seguridad Dinámica y Gestión sobre Redes Virtualizadas Distribuida https://cerberus.inf.um.es/

CERBERUS persigue como principal objetivo proporcionar un framework de administración de seguridad cognitivo, robusto, práctico y adaptable a los eventos futuros. Este framework se basará en técnicas de Inteligencia Artificial (IA) preservando la privacidad para monitorizar, predecir, mitigar y prevenir riesgos y ataques sobre la infraestructura IT. Entre las infraestructuras objetivo se encuentran aquellas que engloban tanto el Internet de las cosas (IoT) y las denominadas SmartCities, así como infraestructuras de comunicaciones 5G, haciendo especial énfasis en las nuevas tendencias orientadas hacia 6G.



Para lograr tan ambicioso objetivo, se ha dividido el proyecto en 4 subroyectos, que se extenderán sobre el transcurso de 3 años y cuyo resultado generará versiones evaluables de los prototipos en entornos relevantes según el ámbito de aplicación (TRL6):

CERBERUS_ZEUS - Gestión de seguridad automatizada en redes 5G/B5G mediante la aplicación del modelo de "closed-loop" basado en arquitecturas ZSM. TSI-063000- 2021-36

La diversidad de servicios a la que se llegará en las redes Beyond 5G (B5G) requiere de una gestión de los recursos acorde con los requisitos que impondrán los usuarios. Está gestión necesitará de una coordinación entre todos los segmentos de la red para poder garantizar un rendimiento y aprovechamiento óptimo de sus capacidades, así como para asegurar un nivel alto de seguridad. Todo esto requiere de una capacidad de control y gestión difícilmente manejable de forma manual, es por ello que los esfuerzos actuales se están enfocando hacia la búsqueda de la automatización de todos estos procesos. Así, la orquestación autónoma tanto de los servicios como de la red y la gestión de la seguridad de ambos permitiría una mejora sustancial con respecto a las soluciones actuales, especialmente teniendo en cuenta que se realiza desde una perspectiva global de la red, siendo capaz de gestionar conexiones extremo a extremo. En esta línea, el Instituto de Estándares de Telecomunicaciones Europeo (ETSI) ha definido una arquitectura basada en un sistema de gestión de bucle cerrado llamada Zero Touch network & Service Management (ZSM). Esta arquitectura contempla funciones de gestión de orquestación, inteligencia, análisis, control y recopilación de datos.

ZEUS propone por tanto una solución capaz de administrar la seguridad de las nuevas infraestructuras B5G mediante orquestación multi-tenant extremo a extremo basada en políticas. De esta manera, se proporcionará a la red de un sistema capaz de reaccionar dinámicamente y en tiempo real ante amenazas a la seguridad, dotándola de capacidades de auto-curación y auto-reparación. En el presente documento se recoge la descripción de la solución propuesta, así como su motivación e innovaciones tecnológicas que se pretenden obtener durante su desarrollo. Igualmente, se fijan los objetivos a alcanzar y la metodología que se usará para cumplirlos.

CERBERUS_HADES - Orquestación automática y reactiva de amenazas y contramedidas de seguridad inter-dominio e intra-dominio mediante la reprogramación del plano de datos. TSI-063000-2021-62

Las arquitecturas B5G cuentan con las redes definidas por software (SDN) y la gestión y orquestación de funciones de red virtuales (NFV-MANO) como pilares fundamentales para su operación y mejoras con respecto a generaciones anteriores. Es gracias a la adopción de estos paradigmas por lo que los sistemas B5G serán capaces de adaptarse dinámicamente a el estado de la red en tiempo real, en función de las necesidades de los usuarios y de forma flexible y escalable. Sin embargo, para poder explotar el máximo potencial de estos paradigmas es necesaria la inclusión de una entidad a cargo de la orquestación y gestión de los recursos de la red, tanto de forma proactiva como reactiva. Esto es especialmente relevante desde el punto de vista de la seguridad de la red, puesto que este sistema podría ser capaz de reaccionar automáticamente ante ataques y mitigar los efectos que estos puedan causar. Estas acciones que se realizan en respuesta a las amenazas pueden ver mejorado su rendimiento mediante la reprogramación dinámica del plano de datos para el procesamiento y monitorización de flujos de datos en tiempo real. Aunque ya hay propuestas en la literatura que consideran este tipo de orquestador, se contemplan escenarios dentro de un único dominio, algo que resulta claramente insuficiente cuando se habla de redes B5G, donde encontramos mayoritariamente escenarios multi-dominio y multi-tenant.

De esta forma, HADES propone una orquestación inteligente y multi-dominio de la seguridad en redes B5G y la aplicación de contramedidas de seguridad inter e intra-dominio mediante la reprogramación del plano de datos. Mediante esta solución, se conseguirá un dominio por parte del orquestador de los planos de control, gestión y monitorización de las redes B5G, con capacidades innovadoras como la automatización de los procesos o el particionado de la red extremo a extremo de forma segura y garantizando un conjunto de recursos para satisfacer los requisitos de los usuarios. En este documento, por tanto, se recoge la descripción de la solución propuesta, así como su motivación e innovaciones tecnológicas que se pretenden obtener durante su desarrollo. Asimismo, se establecen los objetivos a alcanzar y la metodología que se seguirá para llevarlos a cabo.

CERBERUS_HERMES - Soporte a la automatización de la seguridad mediante la gestión inteligente de amenazas y contramedidas de seguridad (CyberThreat Intelligence) y la compartición de conocimiento multi-operador. TSI-063000-2021-44

La variabilidad de servicios que coexistirán en las redes B5G trae de la mano la exigencia de contar con mecanismos de seguridad que no solo contemplen el movimiento de un usuario a través de diferentes dominios, sino también a través de diferentes operadores. Es por ello por lo que surge la necesidad de concebir métodos seguros de colaboración y cooperación entre los mismos, de forma que múltiples operadores sean capaces de compartir información confidencial entre ellos. Este intercambio permitirá mejorar a nivel global la seguridad de los sistemas. Para ello, se podrán compartir acciones de mitigación contra ataques que hayan sido exitosas, o se podrá disponer de un aprendizaje federado para detectar ataques, más rápido y robusto.

HERMES propone por tanto la automatización de esta compartición de conocimiento entre operadores para la gestión inteligente de amenazas y contramedidas de seguridad. Los datos que se intercambiarán para facilitar esta gestión incluirán indicadores de compromiso, acciones y políticas de mitigación, así como modelos de IA para detectar ataques. Los operadores tendrán un control detallado de todos estos datos intercambiados, manteniendo la privacidad y reduciendo al mínimo las posibilidades de revelación de datos sensibles. Se investigarán también nuevos mecanismos de encriptación de datos a través de políticas y nuevos modelos de datos para desarrollar avanzados planes de orquestación de seguridad. En este documento se recoge, por tanto, los principales objetivos científicos y tecnológicos, así como la descripción técnica de la solución propuesta, la motivación del proyecto y las innovaciones tecnológicas que se pretenden alcanzar. Finalmente, se fijan los objetivos que se quieren alcanzar y la metodología para lograrlo.

CERBERUS_HEFESTO - Despliegue y evaluación de la solución en el ámbito de Smart Campus. TSI-063000-2021-45

Los campus universitarios están sufriendo una transformación hacia espacios más inteligentes y seguros. Estos espacios se caracterizan por una gran variedad de tipos de usuarios, con diferentes requerimientos y que usan un amplio abanico de servicios. Es por ello por lo que se está apostando por el despliegue de arquitecturas basadas en B5G, de forma que se pueda maximizar el aprovechamiento de los recursos sin que los usuarios vean degradada su experiencia de usuario ni vean vulnerada su privacidad. De esta manera, se pretende desplegar y evaluar el framework propuesto de gestión de seguridad automatizada en el ámbito de SmartCampus. Para ello, se propone como escenario de pruebas la infraestructura Gaia-5G, localizada en el Campus de Espinardo de la Universidad de Murcia. Aquí se llevará a cabo la integración de la solución propuesta y se definirán una serie de casos de uso que sirvan para demostrar la adecuación y el rendimiento del framework. Los bancos de pruebas contarán con diferentes tecnologías, dominios y operadores B5G. Destacan entre estas tecnologías las capacidades dinámicas que proporcionan NFV y SDN, la reprogramación dinámica del plano de datos y la integración de modelos de IA para la toma de decisiones basadas en políticas. En este documento se describe técnicamente la infraestructura donde se harán las pruebas y las innovaciones que se pretenden alcanzar con la integración del novedoso sistema diseñado dentro de dicha infraestructura B5G. También se fijan los objetivos a alcanzar y la metodología que se seguirá para alcanzarlos.

Información práctica de la Universidad de Murcia

La Universidad de Murcia cuenta con **GAIA-6G**, un testbed de nuevas tecnologías de comunicaciones, IoT y movilidad inteligente situado en el campus de Espinardo y que forma parte del laboratorio de investigación de Sistemas Inteligentes y Telemática GSIT de la Facultad de informática de la UMU, Figure 1. Siguiendo la idea de "Smart Campus", se ha desplegado una infraestructura de sensores IoT, habilitados por redes de acceso, transporte y sistemas de cómputo distribuido que nos permiten experimentar en un entorno único donde se mezclan tecnologías punteras a todos los niveles del despliegue y otras veteranas y asentadas en el campo de las telecomunicaciones.

Figure 1 - Infraestructura Campus Espinardo UMU.

Además de disponer de puntos de despliegue en diversos edificios del campus, el testbed consta de dos nodos principales donde se albergan la mayoría de los recursos de cómputo. GAIA-6G además cumple un doble rol: producción para tareas de cómputo científico, incluyendo el alojamiento de servicios relacionados con nuestras tareas de investigación, y a su vez, parte de la red es totalmente mutable para poder desplegar diferentes escenarios y explorar otras posibilidades.

Esta mutabilidad además está coordinada siguiendo los paradigmas de orquestación cloud y NFV. De esta manera podemos desplegar servicios dinámicamente, reconfigurando de forma automática toda la infraestructura necesaria, tanto sistemas de cómputo, como la RAN y la red de transporte intermedia. Para ello contamos con despliegues de arquitecturas cloud como Openstack o Kubernetes y orquestadores independientes como OSM. Además, hemos desarrollado un módulo de interconexión de la API de nuestro core 5G Amarisoft para que OSM sea capaz de modificar los parámetros de la red 5G dinámicamente y, actualmente, nos encontramos desarrollando el mismo componente para los cores 5G Free5GC y Open5GS siguiendo las APIs estándares definidas por la

3GPP para arquitecturas 5G. Estos componentes son la pieza final para permitir la reconfiguración dinámica de toda la infraestructura llegando hasta la capa de acceso radio. Estas capacidades han sido puestas a prueba con proyectos de gemelo digital de edificios y sistemas a bordo de automóviles, así como demostradores de segmentación (slicing) de red para garantizar el caudal apropiado a aplicaciones críticas y orquestadores de red de próxima generación habilitados por tecnologías de aprendizaje automático capaces de responder autónomamente ante ataques y variaciones de las condiciones de la red.