RAINBOW NEWSLETTER

ISSUE 4, MAY 2021

RAINBOW is a Research and Innovation Action funder under the EU Horizon 2020 framework programme, focusing on producing an open, trusted **fog computing platform** facilitating the deployment, orchestration and management of scalable, heterogeneous and secure IoT services and cross-cloud apps.

SECURITY & TRUST FOR FOG SERVICES

Transforming cloud applications into **scalable and elastic micro-services** with inter-communication and data analysis over the network raises significant security risks.

Authentication, **access control**, **intrusion detection**, and **revocation** are identified as the main security challenges, that require careful design due to the distributed nature of fog computing and the limited resources of IoT devices.

RAINBOW ensures security and privacy primitives across the device-fog-cloud-application stack by its **trust and remote attestation mechanisms** and the provision of a **secure "*zero-conf*" overlay mesh network**.

Horizon 2020
European Union Funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871403

PROJECT INFORMATION

TITLE: RAINBOW - *A fog platform for secured IoT services*
GRANT AGREEMENT NO: 871403
CALL ID: ICT-15-2019-2020
CALL TOPIC: Cloud Computing
START DATE: January 1st, 2020
END DATE: December 31st, 2022
COORDINATOR: UBITECH Ubiquitous Solutions

Follow us in social media:

Facebook
@RainbowProjectH2020

Twitter
@RainbowH2020

LinkedIn
rainbow-project-h2020

Look for our hashtags!

#RAINBOW_H2020
#FogComputing
#EdgeComputing
#Industry4
#secureIoT

https://rainbow-h2020.eu

RAINBOW ATTESTATION MODEL & SPECIFICATION

RAINBOW model for Security, Privacy & Trust Establishment

In RAINBOW each fog ecosystem achieves security by adding a Trusted Platform Module (TPM) component acting as a decentralized Root-of-Trust for enhancing the security posture of the entire environment. TPMs also offer Direct Anonymous Attestation functionality to enable anonymous authentication.

Trust Models

Trust models, able to capture the complex relationships between all involved entities and components, are defined for delivering the high-level functionalities related to secure (edge and mesh) device identification and integrity, data integrity and confidentiality, anonymity and resource integrity in the context of RAINBOW.

Trust Assumptions, Security & Safety Requirements

RAINBOW defines a set of assumptions and requirements in order to establish and maintain strong guarantees of trust in a fog-based environment, that will enable the management of trust-aware service graph chains. A fog-based system is at a trusted state if and only if all of the following requirements are successfully met:

- Hardware or software support for remote attestation
- Data confidentiality, integrity and availability
- Memory-Safety
- Type-Safety
- Control-Flow Safety
- Operational-Correctness
- Cryptography
- Physical Security

Horizon 2020
European Union Funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871403

RAINBOW COLLECTIVE ATTESTATION POLICY ENABLERS

Hardening the Fog/Edge IoT Stack

The need to devise open and standardized mechanisms for IoT services requires trusted attestation schemes for efficient, secure fog node identification and management. RAINBOW aims to achieve high security and privacy guarantees by using a TPM, acting as the underlying Root-of-Trust (RoT). A RoT is a crucial element in a computer-system and even more so in a distributed environment such as the ones studied in RAINBOW. RoT enables other components in a system to come to a trust decision for a given situation.

RAINBOW Zero-Touch Configuration

RAINBOW aims at the creation of privacy- and trust-aware service graph chains through the provision of Zero-Touch Configuration (ZTC) functionalities: fog nodes, wishing to join a fog cluster, adhere to the compiled attestation policies by providing verifiable evidence on their configuration integrity and correctness. In other words, the ZTC should provide guarantees that a node will be able to join a network if and only if it can prove that it is at a "correct state" - without, however, needing prior communication of its own state beforehand.

RAINBOW Direct Anonymous Attestation

Direct Anonymous Attestation (DAA) is an anonymous digital signature mechanism that allows secure platform authentication and privacy-preserving communication. In RAINBOW, DAA is offered through a trusted component such as the TPM acting as a decentralized Root-of-Trust for enhancing the security posture of the entire environment.

Secure & Privacy-Preserving Overlay Mesh Networking

The deployment of wireless fog nodes raises many functional requirements. As far as connectivity is concerned wireless nodes formulate temporal connections with their neighbours and must route packets to each other without relying on static routing tables and fixed network subnets. In other words, the networking environment per se is dynamic and uncontrolled. Each node that enters a wireless fog network must be addressable. RAINBOW will adopt open-source software CJDNS (https://github.com/cjdelisle/cjdns), which allows the implementation of an encrypted IPv6 peer-to-peer network using public-key cryptography for address allocation and a Distributed Hash Table for high level routing and dynamic load balancing.

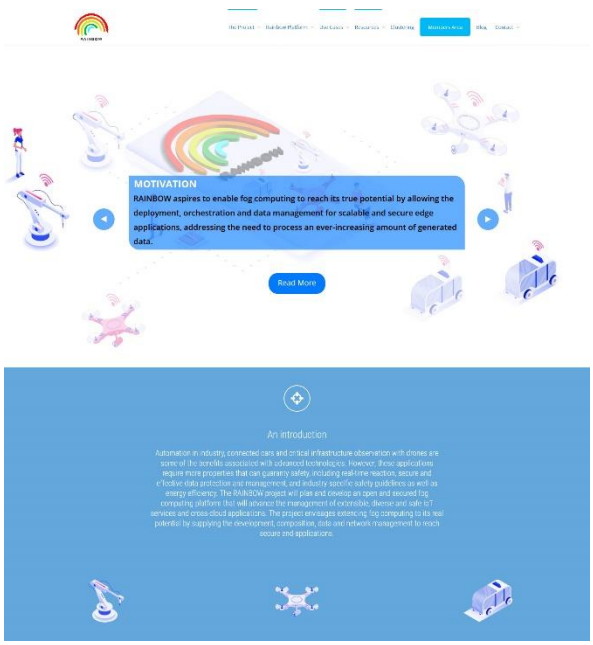
Horizon 2020
European Union Funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871403

REVAMPED RAINBOW WEBSITE

The RAINBOW project website undergone a facelift in April 2021. Changes occurred in the landing page along with new content providing more details about the **RAINBOW Platform** related to the project's Motivation, Open Challenges, Mission & Vision as well as its Impact.

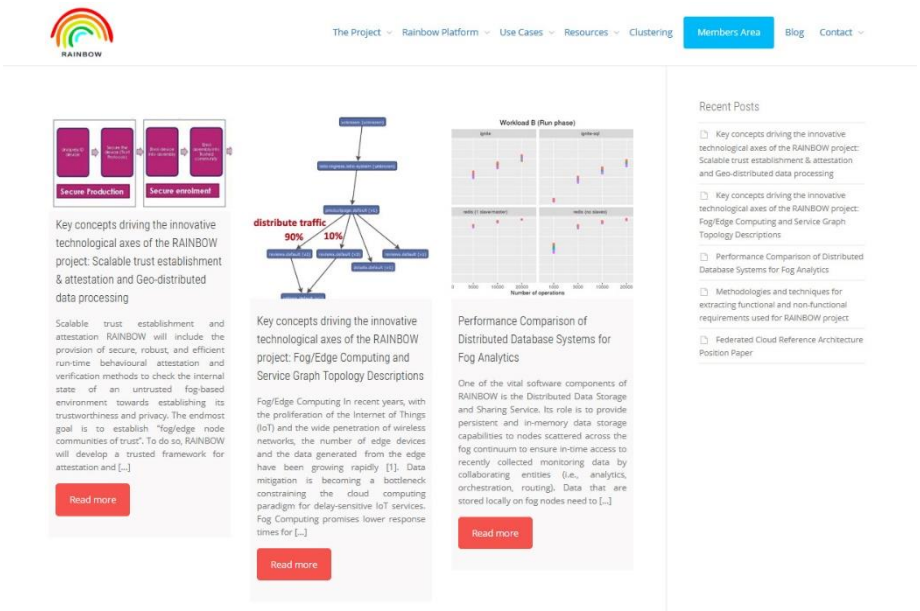
Check out our revamped website at https://rainbow-h2020.eu



RAINBOW BLOG

New interesting content is added regularly in the RAINBOW blog. Our partners are providing short technical articles and sharing news with regards to the Fog/Edge Computing and research advancements in the European Cloud ecosystem.

Have a look at https://rainbow-h2020.eu/blog/



Horizon 2020
European Union Funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871403

RAINBOW SUPPORTED EVENTS

REGAIN Workshop

Aiming to explore big data as a key driver for circular digital transformation REGAIN will present collaborating networks and projects and foster the exchange of experience and novel ideas from Big Data/AI and Green Technologies/Circular Economy communities. The workshop is hosted under the BDVA/DAIRO Data Week online event on May 27, 2021.

For more information, please visit the website: https://datalab.csd.auth.gr/regain/

SecSoft International Workshop

Aiming to integrate Security, Safety, Trust and Privacy support in virtualized environments SecSoft is co-hosted at the 7th IEEE International Conference on Network Softwarization (NetSoft2021) that will be held from June 28 to July 2, 2021 in Tokyo, Japan. The SecSoft workshop is a joint initiative by the following EU projects: **ASTRID**, **CYBER-TRUST**, **GUARD**, **SIMARGL**, **DATAVAULTS**, **RAINBOW**, **PALANTIR** and **SPEAR**.

For more information, please visit the website: https://www.astrid-project.eu/secsoft/

3rd Workshop on Cyber-Security Arms Race (CYSARM)

The CYSARM workshop, which aims to foster collaboration among cyber-security researchers and practitioners to better understand the various facets and trade-offs of cybersecurity and the impact of new security technologies and algorithms, is co-hosted at the annual ACM Conference on Computer and Communications Security (CCS2021) that will be held from November 14 to 19, 2021 in Seoul, South Korea. The CYSARM workshop is a joint initiative by the following EU projects: **ASSURED**, **PUZZLE**, **RAINBOW** and **C4IIoT**.

For more information, please visit the website: https://cysarm.org/

Horizon 2020 European Union Funding for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871403