



SECANT NEWSLETTER

Security and privacy protection in Internet of Things devices

Issue #7

August 2024

Welcome to the 7th SECANT Newsletter!

We are pleased to announce the publication of the final issue of the SECANT newsletter.

SECANT is a 3-year Research and Innovation Action from 2021 to 2024 funded under Horizon 2020.

It kicked off in September 2021 and it gathers a consortium of 19 partners from 10 different countries including large ICT industries, SMEs, research institutes, 1 healthcare organization and 1 EU CERT.

With just a few days away from the end of our project, we have gathered for you all the innovations and the unique advantages of the SECANT solution.

This newsletter edition highlights also the project's recent collaborative efforts and synergies in disseminating the SECANT results. Additionally, it provides a throwback to our last Plenary Meeting in Bucharest, Romania, and extends an open invitation for the upcoming SECANT Final Event!

Table of Contents

p.2	p.3	p.4	p.5
Milestones	SECANT Innovations	SECANT Events	Synergies



Elevating Security and Privacy Protection in IoT devices: Healthcare on the spot

The event will present the innovation advancements of the SECANT project and will provide a platform for discussing challenges and opportunities within IoT and healthcare cybersecurity.

🕒 09:00 AM - 12:00 PM (CET) | **20 SEPTEMBER 2024**

🔗 Join us via Teams

Find more information at www.secant-project.eu

FINAL EVENT

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 101019645.

PROJECT INFORMATION

SECANT: SECurity And privacy protection in IoT devices

Grant Agreement ID: 101019645

Start Date: 1 September 2021

End Date: 31 August 2024

Funded under: H2020-EU.3.7.4, H2020-EU.3.7

Overall budget: 6.567.958,75

EU contribution: 5.202.226,38

Coordinated by: NTT DATA SPAIN

STAY TUNED!

Stay updated on all our latest news, developments, research and general information regarding the SECANT project.

www.secant-project.eu



[@SecantProject](https://twitter.com/SecantProject)



[secant-project](https://www.linkedin.com/company/secant-project)



[secant](https://zenodo.org/communities/secant)



This project has received funding from the European's Union's Horizon 2020 research and innovation program under grant agreement No. 10101964



SECANT Innovations

SECANT enhances digital security, privacy, and personal data protection within complex ICT infrastructures in healthcare sector. SECANT delivers a holistic framework for cybersecurity risk assessment, addresses both human and technical risk factors and bolsters the overall cybersecurity landscape. The effectiveness and versatility of SECANT has been validated through in four realistic pilot use cases within healthcare ecosystem.

Here's a glimpse into the four dedicated press releases published on our website, providing detailed insights into the innovations introduced by SECANT and the added value they bring!

UC1: Protecting the Connected Ambulance of the Future ([Press Release](#))

SECANT secures communication channels and ensures confidentiality, integrity and continuous data exchange of patient information between the ambulance and any external repository.

- User-Friendly Interface
- Increased Trust Levels
- Holistic IT Security Approach

UC2: Cybersecurity for connected Medical Devices & Mobile Applications ([Press Release](#))

SECANT evaluates cybersecurity and privacy within healthcare research infrastructures that rely on interconnected devices, delivering significant innovations in the field.

- Scalability
- Secure Reporting
- Clinical Information Protection

UC3: Health Data Protection in Healthcare Supply Chain ([Press Release](#))

SECANT introduces a system for secure data access between hospitals in the EU.

- Data integrity with complete ownership to the patients
- Decreased overhead expenses in healthcare organisations

UC4: Cyber Security Training ([Press Release](#))

SECANT provides a set of training tools, including a Cyber Range and a mobile application for cybersecurity training, pertaining both cybersecurity as well as healthcare professionals.

- Intuitive and comprehensive acquisition of new knowledge
- Affordable cyber security training solution
- Enhancing cybersecurity awareness of both technical and non-technical staff

Highlight: 7th SECANT Plenary Meeting

Our 7th and final plenary meeting took place in Bucharest, Romania, on 10-11 July 2024, hosted by our project partner, SIMAVI Software Imagination & Vision.

The meeting's agenda was heavily focused on the final developments of the SECANT Use Cases and the integration development, while live demos were presented to the entire consortium.

The two-days meeting aimed towards ensuring that all operational, technical, and strategic aspects were addressed in a cohesive manner towards the project end and the final review preparation. Dedicated workshops on communication, dissemination, and exploitation presented the SECANT results and the strategies of the project.



Synergies

Joint dissemination activities with ENTRUST



With the rise of connected devices and remote delivery in the healthcare sector, the potential impact of cybersecurity breaches has escalated to unprecedented levels. These vulnerabilities could lead to the compromise of clinical data and personal health information, undermine the integrity and accuracy of transmitted data, or even disrupt critical processes and services. There is an urgent need for more robust medical device security and trust management, including strong authentication capabilities, device operational assurance, and automated threat detection. Prioritising situational security awareness is also essential to address these evolving threats.

In response to this challenge, a significant collaboration is underway between two EU projects, SECANT (GA No. 101019645) and ENTRUST (GA No. 101095634), aiming to advance cybersecurity in the healthcare sector. This partnership is focused on joint dissemination activities, sharing results, and collaborative networking to strengthen cybersecurity measures, directly addressing the growing threat of cyberattacks on healthcare systems and devices. Read more [here](#).

Insights from EU Project Coordinators on Advancing Cybersecurity in Healthcare

This article includes insights from Anael Le Bihan, project coordinator for SECANT (NTT DATA) and Lina Giannakandropoulou, project coordinator for ENTRUST (Uni Systems). Explore below the shared approaches of ENTRUST and SECANT in strengthening cybersecurity in healthcare.

- Both projects prioritize cybersecurity in healthcare, by recognizing the critical need to protect sensitive data and ensure the safe operation of medical devices and systems.
- Both projects emphasize the importance of dynamic risk assessment.
- The two projects propose innovative approaches to enhance trust and security.
- Both projects include plans to validate their solutions through four pilot demonstrations.
- Data protection is a central theme in both

For the detailed blog article, visit the SECANT [website](#)

SECANT's is now registered on the Digital Health Uptake (DHU) [Radar](#)!!

DHU Radar

SECANT: a holistic framework for cybersecurity risk assessment addressing both human and technical risk factors in healthcare ecosystem

Keywords: Cybersecurity, Digital Health Data, Provide training content to healthcare provider(s), risk assessment



Synergies

Joint White Paper within the SecureCyber Cluster [Su-ds02-2020]

Ensuring a Secure Future: Comprehensive Insights into 6G IoT Security and Privacy

We are proud to announce our participation at this joint whitepaper, "Ensuring a Secure Future: Comprehensive Insights into 6G IoT Security and Privacy", which comprehensively analyses the security and privacy challenges associated with 6G-enabled Internet of Things (IoT) systems. As 6G technology evolves from previous generations, it promises unprecedented advancements in data transfer speeds, reduced latency, and widespread connectivity. These advancements will significantly impact the IoT ecosystem, which connects myriad devices and enables seamless data exchange. However, this increased connectivity also introduces new cybersecurity threats and privacy concerns.

The whitepaper considers the evolution of 6G IoT cybersecurity, exploring key challenges and potential solutions. It examines research projects, such as **TRUST-AWARE, Arcadian-IoT, ELECTRON, IDUNN, ERATOSTHENES, SENTINEL, SECANT and SPATIAL**, which address specific security and privacy issues in IoT applications, including smart homes, healthcare, and industrial and businesses environments. Additionally, it discusses the role of AI-empowered security techniques in enhancing real-time anomaly detection and response within 6G IoT networks.

This research focuses as well on analyzing advanced encryption mechanisms designed to secure wireless networks and infrastructures against post-quantum security risks, ensuring the safety and privacy of communication networks in an increasingly connected world. The aim of this whitepaper is to guide stakeholders in understanding and addressing the complex security and privacy demands of the 6G IoT era, ensuring a secure and resilient connected world by providing insights into these critical areas.

FULL WHITEPAPER: [SecureCyber-Cluster-White-Paper](#)



SECANT Final Event

We are pleased to invite you to the SECANT Final Event, which will take place online on September 20th, from 09:00 AM to 12:00 PM CET. This event will demonstrate the innovation advancements of the SECANT project, aimed at enhancing cybersecurity in the healthcare sector. Furthermore, it will also provide a platform for discussing about the challenges and opportunities within IoT and healthcare cybersecurity.

The event, titled "Elevating Security and Privacy Protection in IoT devices: Healthcare on the spot" will commence with an opening session, followed by a high-level presentation from the Project Coordinator and the Scientific and Technical Coordinator of SECANT. This will be followed by a keynote address by Juuso Stenfors, Program Manager at the European Commission. The next session: "Challenges and opportunities in IoT and Healthcare Cybersecurity and Data Privacy: Insights from R&D projects," will feature insights from experts involved in European projects specialised in these areas.

Following this, the SECANT project will present its four Use Cases within the healthcare ecosystem: 1) Protecting the Connected Ambulance of the Future, 2) Cybersecurity for Connected Medical Devices & Mobile App, 3) Health Data Protection in Healthcare Supply Chain and 4) Cyber Security Training. Additionally, towards enhancing the dynamic nature of the event, apart from the speeches the event will include selected live demonstrations which will be presented to all attendees. The event will conclude with an open discussion, offering participants the opportunity to share their views and ask questions.

The event is addressed to cybersecurity and eHealth experts, the SECANT end-users, as well as industrial stakeholders.

[Website announcement.](#)

LinkedIn event:



The banner features a dark grey diagonal section on the left with the SECANT logo (a padlock with a DNA helix) and the text "SECANT" in orange, and "FINAL EVENT" in white below it. The main white area contains the event title "Elevating Security and Privacy Protection in IoT devices: Healthcare on the spot" in orange, a brief description, the time "09:00 AM - 12:00 PM (CET)", the date "20 SEPTEMBER 2024", and the instruction "Join us via Teams". At the bottom, it includes the European Union logo and funding information, and the website "www.secant-project.eu".

SECANT

**FINAL
EVENT**

**Elevating Security and Privacy
Protection in IoT devices:
Healthcare on the spot**

The event will present the innovation advancements of the SECANT project and will provide a platform for discussing challenges and opportunities within IoT and healthcare cybersecurity.

🕒 09:00 AM - 12:00 PM (CET) | **20
SEPTEMBER
2024**

📍 Join us via Teams

Find more information at www.secant-project.eu/

 This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 101019645.



The SECANT consortium



3 Large ICT industries

NTT DATA

THALES
Building a future we can all trust

SIMAVI
Software Imagination & Vision

9 SMEs
EIGHTBELLS
Independent Research & Consultancy

UBITECH
ubiquitous solutions

axon logic

**INFO
LYSIS**

**IANUS
TECHNOLOGIES**

EXALENS®

**Security Labs
Consulting**

adrestia
Equipment & Research & Development

bi²S Ltd
Business and IoT
Integrated Solutions

5 research institutes and universities

**Karolinska
Institutet**

i2cat

iti
Information
Technologies
Institute

**TIC
Salut Social**

**UNIVERSITY OF
SURREY**

1 healthcare organization

**POLARIS
Medical**

1 European CERT

**CENTRUL NATIONAL DE RĂSPUNS LA INCIDENTE
DE SECURITATE CIBERNETICĂ - CERT-RO**

twitter

@SecantProject

Visit our website:
www.secant-project.eu

Download SECANT material:

zenodo

secant-project

linkedin

secant-project

[Click here to subscribe to the SECANT newsletter](#)



This project has received funding from the European's Union's Horizon 2020 research and innovation program under grant agreement No. 101019645

