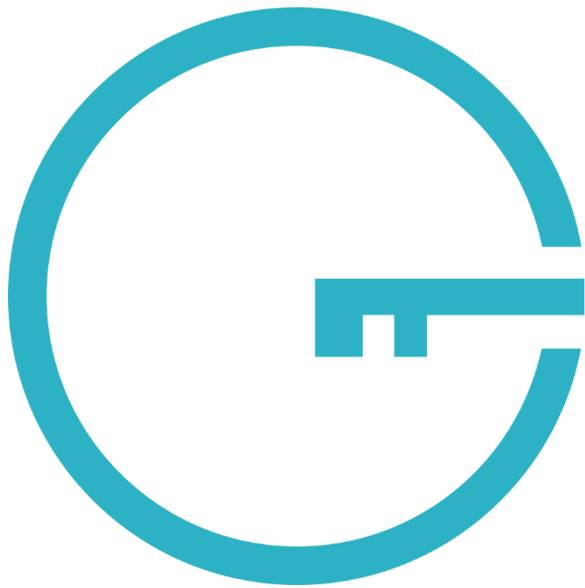# GHOST

Safe-Guarding Home IoT Environments with Personalised
Real-time Risk Control

Article for the EU

Cybersecurity Newsletter

April 2020

Logo of the project

GHOST

Article

Security and privacy in the last mile: GHOST makes your smart home safer

GHOST project is coming to its end with successful results. This project, funded under the EU H2020 programme, has developed a highly-affordable, turn-key, hassle-free solution for securing any home network through the application of the state-of-the-art network monitoring, automated risk assessment and machine learning techniques embedded in a home gateway. The system has been piloted in more than 80 homes in three different countries (Spain, Norway and Romania).

During last years, the explosion of the IoT-enabled services for smart homes has been unstoppable: smart health devices like smartwatches have been used for controlling personal health, home automation solutions has been deployed and integrated with intelligent speakers, etc. It is expected that this trend will continue the same during the next years, as it delivers convenience and efficiency of integrating IoT technologies in our day-to-day activities.

In addition to the explosion of the unstoppable evolution of the IoT-enables market, we are suffering a transformational moment caused by COVID-19 outbreak. The situation has been, undoubtedly, a dramatic and painful experience for humanity. Nevertheless, at least in the developing countries from the European Union (EU), the current situation also triggered a profound and positive change. Suddenly, public institutions, government agencies, universities, schools, discovered that the Internet can help to reduce the spread of diseases (e.g., by eliminating what was previously a normal site - the endless queues) and that public services can be brought to the citizen by existing Information Technology (IT) solutions. Almost by night, what was previously unthinkable, suddenly started to materialize. Regular people were able to access public services, university lectures, etc., all of these being supported by modern IT solutions. Nowadays, a positive and possibly general opinion in these countries seems to be a hope that: "these services will not disappear after COVID-19".

Nevertheless, security and privacy management on this kind of solutions has not evolved at the same pace, especially in terms of user's awareness and cyber knowledge. In addition, most of the security and privacy technologies available nowadays have been developed to protect the assets within the core of the networks (mostly cloud-oriented security solutions and systems for all-IP networks). For this reason, the following question needs to be quickly addressed: Do security solutions raise to the challenge, or do we need to approach the problem differently?

To address this question, the GHOST project somehow anticipated the need to address the requirements of non-IT experts. Accordingly, it developed a security solution that can fit to the needs and the profile of a wide variety of users, including non-security, as well as non-IT experts. The GHOST project addresses these issues by bringing together a team of IT and security experts, alongside non-IT experts that have permanent contact with regular non-IT users. The result of the project is therefore a tool-suite that is adaptable to a wide variety of users. Most importantly, however, the solution has been constantly changed by incorporating the feedback from expert and non-expert users from three different countries in the EU.

GHOST is based on the combination of two main pillars: first, the adaptation of the state-of-the-art technologies like blockchain, machine learning and automated risk assessment for securing home IoT networks (deploying specific tools for constrained and embedded devices); second, as previously commented, the end-user validation and feedback integration (through the execution of the pilots on 87 homes, targeted focus groups and various other end-user related activities). These two pillars have enabled the creation of a usable security and privacy solution for protecting homes being controlled and managed by the inhabitants themselves. The end-user experiments have unveiled two critical findings: a lack of awareness of security and privacy importance for this type of application and a dangerous trust-by-default approach by the end users. GHOST results are, firstly, motivating and engaging the end-user in the management of their home's security and privacy and, secondly, providing the right tools for taking the control over the security and privacy of one of the most precious spaces in our lives: our home. During three years, the GHOST solution was evolving to achieve a higher level of maturity in terms of usability, transparency, robustness, trust, scalability, detection and mitigation capabilities.

Consequently, GHOST can provide the right answer to the above-mentioned question and can help non-IT experts to get familiarized and to accept more easily these sophisticated, but nowadays essential, software solutions.

Website of the project: https://www.ghost-iot.eu/

Project: Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control

Project coordinator: TELEVES S.A.U.

Project acronym: GHOST

Contact: Javier Augusto (jaugusto@televes.com)

Potential images that could be included

GHOST

GHOST Dashboard   A- A+ (🔔) 🌐 👤

- 🔲 Dashboard
- 🧭 Devices
- 📈 Historical Data
- ⚙️ Settings

10:43:20 AM   Live update 🔴 Include External traffic ⚪

🛡 Your home   Network status ❓   Devices Status ❓   Threats ❓
is secure   Last Month ⌄
                         Network   Devices
Total communication events: **12** 0 0 0 0   🐞 **6/12**
                           ⚡   **12**   SecuredLow MediumHigh Critica
77   Threats blocked
                         connected connected
Download report: 📄⬇   Last updated: 10:43:07   Last updated: 10:43:07   Last updated: 10:43:07
Last updated: 10:43:07

Devices Security Status ❓   **Gateway Traffic** ❓

                        ■ Critical 0/12
                        ■ High 0/12
                        ■ Medium 0/12   ■ Packets received
                        ■ Low 0/12   ■ Packets sent
                        ■ Secured 12/12

Last updated: 10:43:07   Last updated: 10:43:07

Live Network Traffic   Flows buffer size   Protocol ❓
                                100   ⌄   All   ⌄

← COLLAPSE SIDEBAR   ▬ Heavy traffic
                        — Light traffic

16:41 ⚠ 🖼   0.45 K/s 🔕 💎 ▧ ◢ 20% 🔋

GHOST - Messages   ☰

‹   ›

✅

Pending action

💬**Problem Description**

We are getting unexpected
communications from door sensor. This
is not a regular behaviour.

🔦**Recommendation**

Check whether the described behaviour
is unexpected. If yes, resolve it.

If you are uncertain, you can check the
device manual or click on More help.

🔑**Solution**

Please indicate how you resolved the
issue:

◯ I removed the device
◯ I fixed the device
◯ I checked and behaviour is fine

More help

Resolved

◁   ◯   ▢