PROJECT IMPACT

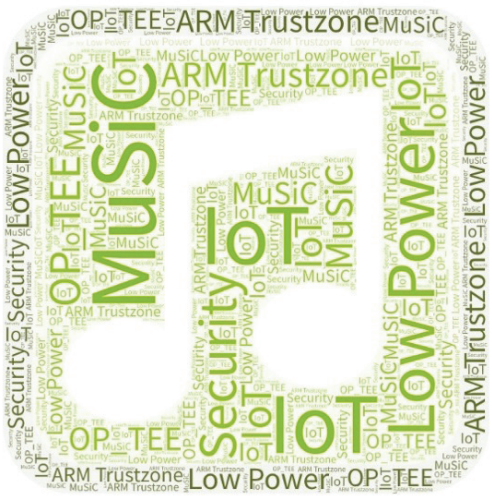
16105

The MuSiC project aims at providing a scalable and certifiable security solution for the mid to high data-rate cost-effective devices in order to secure against application, OS, web, and network based threats and protect critical services on shared networks. [MuSiC]

January 2023

Several billion of connected devices will transform our life brining many benefits. This multitude of connected devices creates backdoors for hackers and cyber criminals. For this reason, it is important that Low data-rate secure devices (e.g. smart cards for payment) and high-end consumer devices (e.g. PCs, mobile phones or tablets) have to become more secure. Today, merchants are flooding the market with untrusted gadgets due to a lack of certification and missing off-the-shelves secured solutions. The threat was highlighted by DDoS attack from thousands of connected devices interrupting digital services. The assailants took advantage of always connected, insufficiently protected devices like IP cameras and routers. The MuSiC project solves lack of security implemented in low-power and cost-efficient connected devices with an **affordable open modular reference platform**, providing a **scalable** and **certifiable solution**.

Background, objectives of the project and challenges

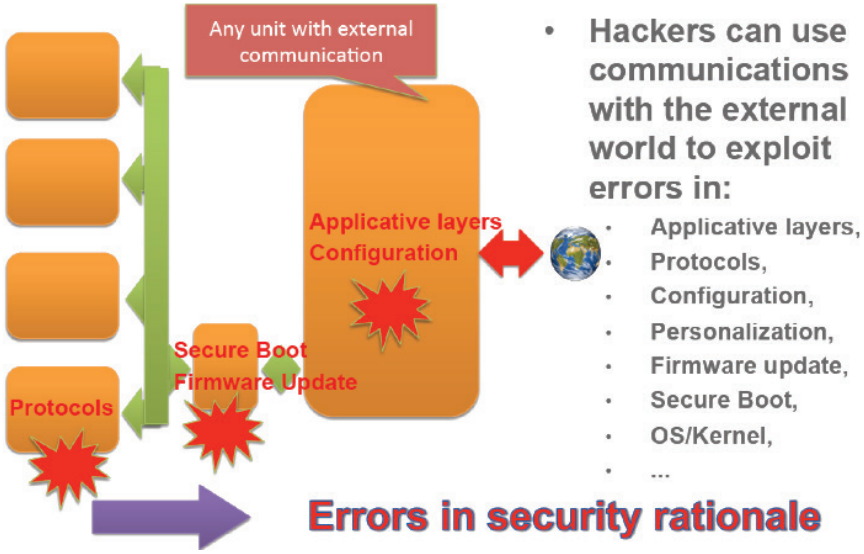


The world is projected to have over many BILLION connected devices in the Internet of Things (IoT). In addition, those devices must connect through the internet to some myriad of other devices like smart phones and cars, applications, websites, and routers. With all its conveniences, the very connectedness of the IoT is potentially a serious concern. As matter of the fact, it provides a pathway for a connected device anywhere in the world to talk to any other device but at the same tile it creates a new set of security challenges.

As a result, without proper security every connected device is a possible target for a cybercriminal's subversion. Devices connected to the internet offer opportunities to cybercriminals ready to exploit flaws and vulnerabilities, whether those flaws are human, hardware, or software based. They can challenge systems via non-invasive, semi-invasive, and invasive or physical attacks. Non-invasive attacks usually involve a stolen password, eavesdropping, or exploiting system bugs to gain access; semi-invasive attacks take advantage of uncontrolled states or injecting faults into a system; and invasive attacks aim to embed software or modify or read internal signals. Fundamentally, security is about protecting assets. These assets can be any kind of Information, capability, feature, or financial or technical resource that may be damaged, lost, or disrupted. Security means assuring data confidentiality, so that information is only made available and disclosed to authorized individuals, entities, or processes and it is fully protected from unauthorized requests. It also requires the integrity of the information is maintained and assured for accuracy and completeness of data over its entire life-cycle. Data cannot be modified in an unauthorized or undetected manner. Finally, security requires the availability of Information so it can be available, only to authorized requestors, whenever needed.

Generally, a system's greater weakness is a failure to properly verify the identity of devices on a network resulting in access and misuse of devices, services, or networks, theft of confidential data or identity, and sometimes counterfeit devices or services being added to the network.

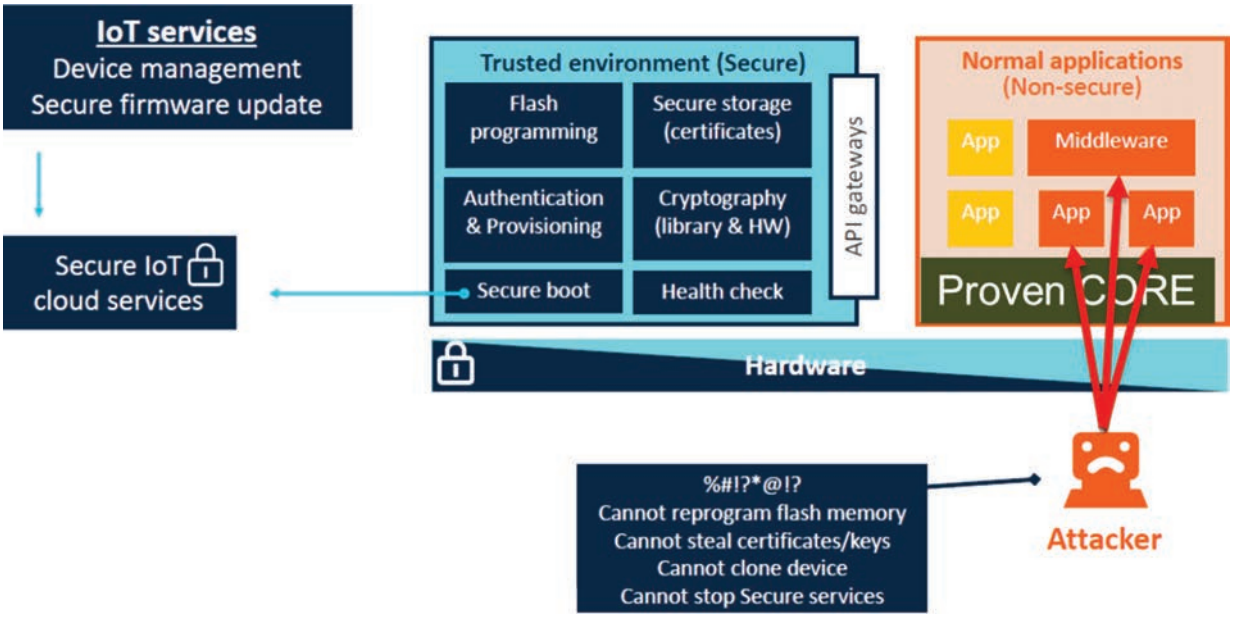
Cybersecurity is a growing concern, and government are investing in new regulations to ensure that security is included at the design stage of the product. Those that do not meet the requirements will not go to the market. Most cyberattacks are non-invasive and misuse network protocols to exploit communication protocol errors and/or flaws in software design or implementation. This is the domain of malware, stack overflows, viruses, and Trojan horses designed to slide unseen past antivirus software, firewalls, and encryption. Recognizing the challenge, MuSiC project proposes a novel and flexible architecture to ensure a solid foundation for robust complete-system protection to keep the device foolproof.



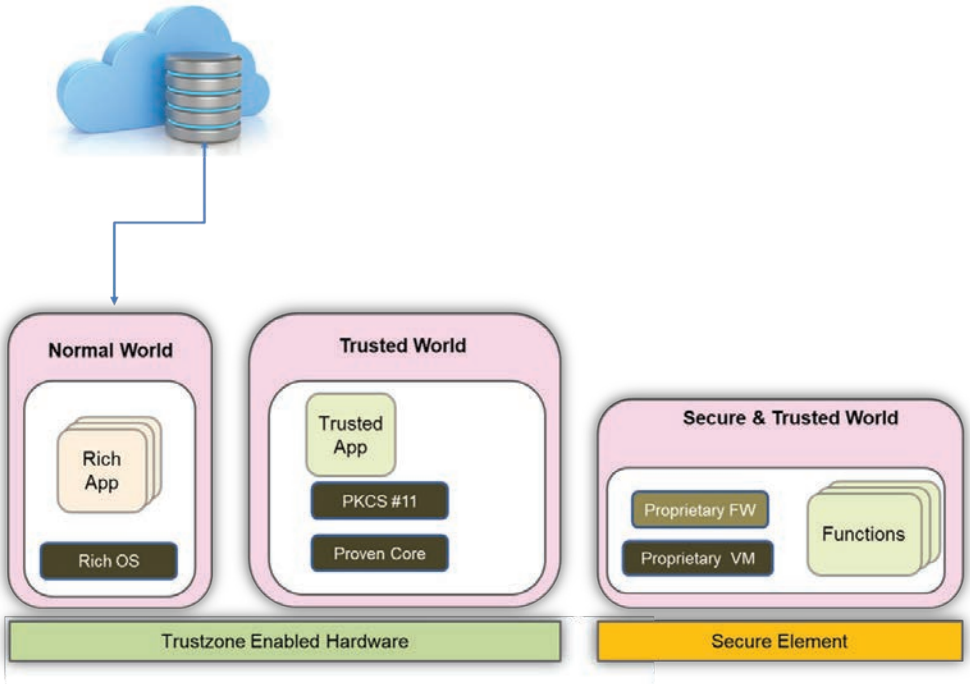
Technological achievements

The major project results is to offer a scalable secure IoT solution for the development of trusted devices offering adequate processing capabilities to support multimedia services, protecting against various kind of attack, covering secure access and sensitive data protection, Cost-effective Common Criteria security certification paths up to the level required by Mission Critical Services in order to give users and manufacturers confidence in these trusted devices,

MusiC is proposing an **affordable open modular reference platform**, providing a **scalable** and **certifiable solution** for any **connected devices** in order to **secure** against application, OS, web, and network based threats and to protect **critical services** on shared networks. One of the **technological innovation** is to develop the proposed **novel architecture** (both hardware and software) optimized for low-power and cost efficient IoT and communication devices supporting the security mechanisms existing today on high-end computing and mobile devices...



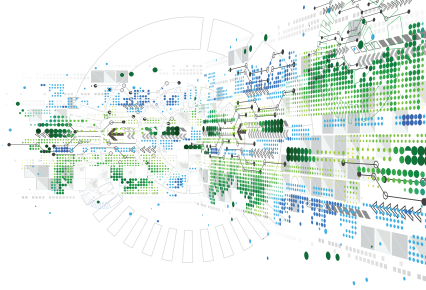
The Technological achievements of MuSiC are the HW/SW implementation a set of dedicated Execution Environment (EEs) managed by Open Portable Trusted Execution Environment (**OP-TEE**) for MPU and **Proven CORE** for MCU. These TEEs will ensure trustworthy (only legitimate devices/objects can connect to services), data protection (both in transit to/from the cloud and inside the edge device) and code and IP protection against theft and devices against Normal Applications OS vulnerabilities. To support the TEE isolation, **OP-TEE and Proven CORE** are strongly linked to the **ARM® TrustZone®**. The ARM Trustzone technology provides all the hardware means to isolate security critical components in a system, by hardware separating a rich operating system, from a secure OS. Thus **OP-TEE and Proven CORE** enable to put the access control at the peripheral or memory creating an isolation barrier that separates assets and code (referred worlds) throughout the overall MPU and MCU.



STM32 MP1

ST33

The Secure world, hosting OP-TEE or Proven CORE, runs Trusted Applications and protect confidential cryptographic data (e.g. keys, certificates) using a **SE** (Secure Element) that is a tamper-resistant processor. Using SEs applications can use security services like authentication, encryption, signature to protect application data. MuSiC has optimized these TEEs from mobile communication to IoT devices bringing a path toward the Common Criteria certification of the highest security levels, through the optional integrations of a SE protecting connected devices, up to the highest level of security while keeping the cost and time-to-market in line with the constraints of the target industry. Music technology has been successfully used in several demonstrators representing use cases within **Smart City** and **PPDR** (Public Protection and Disaster Relief) applications integrating these trusted devices and validating the ability to answer to different security and performance requirements.



KEY APPLICATION AREAS

- Transport & Smart Mobility
- Health & Well-Being
- Energy
- Digital Industry
- Digital Life Health & Well-Being

ESSENTIAL CAPABILITIES

- Systems and Components Architecture, Design & Integration
- Connectivity & Interoperability
- Safety, Security & Reliability
- Computing & Storage
- ECS Process Technology, Equipment,Materials & Manufacturing

PARTNERS

STMicroelectronics / ADWAVE / AIRBUS Defense and Space / CAMEA / CEA / FIT of Brno University of Technology / HI-Iberia Ingeniería y Proyectos / Prove & Run / Quobis Networks SL / Tecnologías Servicios Telemáticos y Sistemas SA

COUNTRIES INVOLVED

- Czech Republic
- France
- Spain

PROJECT LEADER

Marcello Coppola
STMicroelectronics Grenoble2 SA

KEY PROJECT DATES

01 June 2018 to 31 December 2021

Market Potential

The partners in the MuSiC project are active in the global IoT in market, and to Smart City and PPDR markets. According to Fortune Business Insights, the global IoT market is estimated to rise to USD 2465.26 billion by 2029 at a CAGR of 26.4%. According to the analysis, the penetration of smart cities and deployment of vehicle solutions will push well for the global outlook. As matter of the fact the smart city market will grow, accordingly MarketsandMarkets from USD 156.1 Bn in 2021 to USD 258.2 Bn in 2026 at CAGR 10.6% during 2021-2026. During the project, the technological innovations were investigated in the STM32U5 and STM32MP1 supporting Trust zone. These STM32U5 and STM32MP1 will create new market opportunities in the global IoT market enabling ST to enter in the MPU market which reached US$ 3.4 Bn in the year 2021 and it is expected to grow with a CAGR of 8% between 2021 and 2031. High-tech project partners will obviously benefit from these market opportunities for their hardware or software building blocks based on STM32.

Societal & Economic Impact

The major project results will be:

- A scalable secure solution for the development of trusted devices offering adequate processing capabilities to support multimedia services, protecting against various kind of attack, covering secure access and sensitive data protection,
- Cost-effective Common Criteria security certification paths up to the level required by Mission Critical Services in order to give users and manufacturers confidence in these trusted devices.

Demonstrators for representative use cases within **Smart City** and **PPDR** (Public Protection and Disaster Relief) applications integrating these trusted devices are projected to grow at a CAGR of 90%-95% to reach $54 billion in 2026, according to findings from a market study by Everest Group.

Future Developments

MuSic target the fast growing IoT/MtoM security market offering platforms and technologies that enable to bring products to market faster removing the today trap of a “sell now and we’ll patch it later” mentality. MuSiC raises the levels of efficiency and security and will contribute to the digital transformation in Smart City and PPDR as well as the necessity to introduceTEE as part of the Cloud infrastructure offerings.

Aeneas Office
44 rue Cambronne
F-75015 Paris - France
Tel. +33 1 40 64 45 80
Fax +33 1 40 64 45 89
penta@aeneas-office.org
www.penta-eureka.eu

Penta (E! 9911), is a EUREKA Cluster whose purpose is to catalyse research, development and innovation in areas of micro and nanoelectronics enabled systems and applications.