life.augmented

Press release

P4173S

STM32Trust Ecosystem from STMicroelectronics Consolidates Cyber-Protection Resources for IoT Designers

- ***Comprehensive toolset delivers robust protection for connected devices based on STM32 microcontrollers***

Geneva, July 30, 2019 – STMicroelectronics (NYSE: STM), a global semiconductor leader serving customers across the spectrum of electronics applications, has launched STM32Trust to guide designers' efforts to build strong cyber-protection into new IoT devices leveraging industry best-practices.

STM32Trust combines knowledge, design tools, and ready-to-use original ST software. These help designers take advantage of features built into STM32* microcontrollers to ensure trust among devices, prevent unauthorized access, and resist side-channel attacks. All this averts data theft and code modification.

"Connected devices like smart sensors and remote actuators are intrinsic to our infrastructure and services, so ensuring effective security becomes of paramount importance," explained Ricardo De Sa Earp, General Manager of STMicroelectronics' Microcontroller Division. *"STM32Trust eases developers' understanding and acceptance of the new mandatory security rules, which is a key emerging challenge in the general-purpose microcontroller market today."*

Integrating all available cyber-protection resources for the STM32 family, STM32Trust helps designers implement a robust multi-level strategy leveraging security-focused chip features and software packages.

The STM32 family is the world's leading system-on-chip portfolio based on the Arm® Cortex® CPU architecture and contains almost 1000 variants used in smart appliances, remote sensors, wearables, e-health devices, IoT gateways, access-controlled storage, payments, and many other connected devices. Depending on the model, hardware cyber-protection can include features such as customized secure boot, a random-number generator to prevent hackers observing patterns in signals, dedicated encryption co-processors, and secure storage for encryption keys. ST also builds in tamper detection, firewall code-isolation mechanisms and implements Arm TrustZone® technologies for extra protection of the most sensitive code.

STM32Trust provides product developers with all they need to protect connected objects effectively using these features, including reference material and free software.

Among the reference software packages X-CUBE-SBSFU demonstrates how to protect application code at its most vulnerable when being transferred into boot memory or updated in the field. X-CUBE-SBSFU reference packages are available for the STM32F4, F7, H7, L0, L1, L4, G0, G4, and WB. There is also a reference implementation of ST's secure element STSAFE, which maximizes the security level of the final application.

In addition, Secure Firmware Installation solutions for STM32L4 and STM32H7 microcontrollers provide protection while devices are being programmed for the first time. The solution offers a complete toolset to encrypt OEM binaries with the Trusted Package Creator software, the STM32CUBEProgrammer to flash securely the STM32, and the STM32HSM to transfer OEM credentials to the programming partner.

The STM32Trust resources including tools, evaluated reference material, and source code can be downloaded free of charge from http://www.st.com/stm32trust.

You can also read our blogpost at https://blog.st.com/stm32trust/

* *STM32 is a registered and/or unregistered trademark of STMicroelectronics International NV or its affiliates in the EU and/or elsewhere. In particular, STM32 is registered in the US Patent and Trademark Office.*

About STMicroelectronics

ST is a global semiconductor leader delivering intelligent and energy-efficient products and solutions that power the electronics at the heart of everyday life. ST's products are found everywhere today, and together with our customers, we are enabling smarter driving and smarter factories, cities and homes, along with the next generation of mobile and Internet of Things devices.

By getting more from technology to get more from life, ST stands for life.augmented.

In 2018, the Company's net revenues were $9.66 billion, serving more than 100,000 customers worldwide. Further information can be found at www.st.com.