life.augmented

Press release

PR N°P4173S

L'écosystème STM32Trust de STMicroelectronics regroupe des moyens de cyberprotection destinés aux concepteurs de produits IoT

Cette panoplie d'outils complète assure une protection robuste aux appareils connectés à base de microcontrôleurs STM32

Genève, le 30 juillet 2019 - STMicroelectronics (NYSE: STM), un leader mondial dont les clients couvrent toute la gamme des applications électroniques, annonce sous l'appellation STM32Trust le lancement d'un écosystème conçu pour permettre aux concepteurs d'intégrer de robustes fonctions de cyberprotection dans leurs nouveaux produits connectés à l'Internet (IoT) en s'appuyant sur les meilleures pratiques en vigueur dans l'industrie.

En regroupant des connaissances, des outils d'aide à la conception et des logiciels ST originaux et prêts à l'emploi, l'écosystème STM32Trust aide les concepteurs à tirer pleinement parti des fonctionnalités intégrées aux microcontrôleurs de la famille STM32* en vue de garantir un haut niveau de confiance entre les appareils, d'empêcher tout accès non autorisé et de résister aux attaques. Cette approche a pour but d'éviter le vol de données et la modification des codes.

« *Les appareils connectés tels que les capteurs intelligents et les actionneurs déportés font partie intégrante de notre infrastructure et de nos services. C'est pourquoi il est absolument essentiel de leur garantir un niveau de sécurité effectif* », explique Ricardo De Sa Earp, directeur général de la division Microcontrôleurs de STMicroelectronics. « *L'écosystème STM32Trust permet aux développeurs de comprendre et d'accepter plus facilement les nouvelles règles de sécurité obligatoires, ce qui représente un nouveau défi majeur pour le marché des microcontrôleurs standards.* »

Intégrant l'ensemble des ressources de cyberprotection mises à la disposition de la famille STM32, l'écosystème STM32Trust aide les concepteurs à appliquer une solide stratégie qui tire parti des outils logiciels et des fonctionnalités des circuits intégrés dédiées à la sécurité.

La famille STM32 est leader mondial sur le marché de systèmes sur puce basés sur l'architecture de processeurs Arm® Cortex®, et contient près de 1 000 variantes utilisées dans les appareils connectés, les capteurs déportés, les produits électroniques portés (*wearables*), les appareils de santé électroniques (*e-health*), les passerelles vers l'Internet des objets, le stockage à accès contrôlé, les systèmes de paiement et autres dispositifs connectés. En fonction du modèle, la cyberprotection matérielle peut inclure des fonctions telles que la personnalisation du démarrage sécurisé (Boot), un générateur de nombres aléatoires, des coprocesseurs de chiffrement dédiés, et une fonction de stockage sécurisée pour les clés de chiffrement. ST intègre par ailleurs des mécanismes de détection de falsifications et d'isolation de code dans les pare-feu, et met en œuvre les technologies Arm TrustZone® pour assurer un niveau de protection supplémentaire pour les codes les plus sensibles.

L'écosystème STM32Trust fournit aux développeurs de produits tout ce dont ils ont besoin pour protéger efficacement les objets connectés, notamment à l'aide de matériels de référence et de logiciels libres.

Parmi les logiciels de référence, le module d'extension X-CUBE-SBSFU montre comment protéger le code d'application en son point le plus vulnérable, c'est-à-dire lorsqu'il est transféré dans la mémoire de démarrage ou mis à jour sur site. Les packages de référence X-CUBE-SBSFU sont disponibles pour les variantes F4, F7, H7, L0, L1, L4, G0, G4 et WB du microcontrôleur STM32. Par ailleurs, une implémentation de référence de l'élément sécurisé STSAFE de ST maximise le niveau de sécurité de l'application finale.

Enfin, des solutions d'installation sécurisée de firmware (SFI) pour microcontrôleurs STM32L4 et STM32H7 apportent un niveau de protection lorsque les appareils sont programmés pour la première fois. La solution propose un ensemble complet d'outils de chiffrement de fichiers binaires pour OEM avec le logiciel Trusted Package Creator, le STM32CUBE Programmer pour flasher le STM32 en toute sécurité et le STM32HSM pour transférer les identifiants OEM au partenaire chargé de la programmation.

Les ressources de l'écosystème STM32Trust, notamment les outils, le matériel de référence évalué et le code source, sont disponibles gratuitement en téléchargement à l'adresse www.st.com/stm32trust.

Vous pouvez également lire notre blogpost à l'adresse suivante : https://blog.st.com/stm32trust/

** STM32 est une marque déposée et/ou non déposée de STMicroelectronics International NV ou de ses filiales dans l'UE et/ou ailleurs. STM32 est enregistré auprès du US Patent and Trademark Office.*

À propos de STMicroelectronics

ST, un leader mondial sur le marché des semiconducteurs, fournit des produits et des solutions intelligents qui consomment peu d'énergie et sont au cœur de l'électronique que chacun utilise au quotidien. Les produits de ST sont présents partout, et avec nos clients, nous contribuons à rendre la conduite automobile, les usines, les villes et les habitations plus intelligentes et à développer les nouvelles générations d'appareils mobiles et de l'Internet des objets.
Par l'utilisation croissante de la technologie qui permet de mieux profiter de la vie, ST est synonyme de « life.augmented ».

En 2018, ST a réalisé un chiffre d'affaires net de 9,66 milliards de dollars auprès de plus 100 000 clients à travers le monde. Des informations complémentaires sont disponibles sur le site : www.st.com.

Contact presse ST :
Nelly Dimey
Tél : 01.58.07.77.85
Mobile : 06. 75.00.73.39
nelly.dimey@st.com