Internship M/F – Building a framework for constant-time analysis of cryptographic SW on embedded systems

life.augmented

Rousset (Fr) / Milano (It)

WHY JOIN US

At ST, we are more than 50,000 creators and manufacturers of microelectronic technologies. We collaborate with over 200,000 customers and thousands of partners. Together, we design and create products and solutions that meet their challenges and the need to contribute to a more sustainable world. Our advanced technologies enable smarter mobility, more energy efficiency and power management, and large-scale deployment of the Internet of Things (IoT) and 5G. ST has received the Top Employer France and HappyTrainees 2023 certifications. They recognize us as a reference employer and demonstrate our commitment to making people a priority.

OUR FUTURE COLLABORATION

Executing cryptographic routines in a constant time, that means their execution time does not depend on input secret data, is a very important countermeasure against timing attacks, a dangerous family of side-channel attacks.
Several tools and frameworks have been developed in order to verify this feature, but it's often difficult to adapt those tools to whole cryptographic libraries for embedded devices.

Within an R&D team specialized in embedded systems security, the objective of this 6-month internship is to evaluate state-of-the art tools (e.g.: DudeCT, CTGrind, FlowTracker, etc.), test them against different cryptographic algorithms on a STM32 microcontroller and, develop a framework to automatically test several cryptographic functionalities running on microcontrollers, trying to integrate in a single solution those tools that have unique desired functionalities.

Our technology starts with you. Come join our team!

YOUR PROFILE

- Last year of a master degree in software engineering / computer science
- Software skills in C.
- Proactivity, autonomy and teamwork.
- Good level of written and spoken English (Resume and cover letter in English).

LOCATION

Rousset (Bouches-du-Rhône, France), close to Aix-en-Provence, or Agrate Brianza (Italy), close to Milan.

HOW TO APPLY

In English, through STCareers portal:

- https://stcareers.talent-soft.com
- Reference: 2023-35642
- Title: STAGE - Outil d'analyse en temps constant de logiciels cryptographiques embarqués M/F".

Stage H/F – Conception d'un framework pour l'analyse en temps constant des logiciels cryptographiques pour systèmes embarqués

Rousset (Fr) / Milan (It)

POURQUOI NOUS REJOINDRE

Chez ST, nous sommes plus de 50 000 créateurs et fabricants de technologies microélectroniques. Nous collaborons avec plus de 200 000 clients et des milliers de partenaires. Avec eux, nous concevons et créons des produits et des solutions qui répondent à leurs défis et à la nécessité de contribuer à un monde plus durable. Nos technologies de pointe permettent une mobilité plus intelligente, une gestion plus efficace de l'énergie, de la puissance et un déploiement à grande échelle de l'Internet des objets (IoT) et de la 5G.
ST a reçu les certifications Top Employer France et HappyTrainees 2023. Elles nous reconnaissent en tant qu'employeur de référence et démontrent notre engagement à faire de l'humain une priorité.

NOTRE FUTURE COLLABORATION

L'exécution de routines cryptographiques en temps constant (ce qui signifie que leur temps d'exécution ne dépend pas des données secrètes), est une contre-mesure très importante contre les attaques par canaux auxiliaires basées sur le temps d'exécution.
Plusieurs outils et frameworks ont été développés afin de vérifier cette propriété, mais il est souvent difficile d'adapter ces outils à des bibliothèques cryptographiques complètes pour systèmes embarqués.

Au sein d'une équipe de R&D spécialisée dans la sécurité des systèmes embarqués, l'objectif de ce stage de 6 mois est d'évaluer des outils de pointe (ex : DudeCT, CTGrind, FlowTracker, etc.), de les tester sur différents algorithmes cryptographiques sur un microcontrôleur STM32 et de développer un cadre pour tester automatiquement plusieurs fonctionnalités cryptographiques sur des microcontrôleurs, en essayant d'intégrer dans une solution unique les outils qui ont des fonctionnalités souhaitées.

Notre technologie commence avec vous. Venez rejoindre notre équipe !

VOTRE PROFIL

- Dernière année de master, école d'ingénieur ou équivalence.
- Compétences en programmation C.
- Proactivité, autonomie et travail d'équipe.
- Anglais écrit et parlé (CV et lettre de motivation en anglais).

VOTRE LIEU DE TRAVAIL

Rousset (Bouches-du-Rhône, France) près d'Aix-en-Provence, ou Agrate (Italie), près de Milan.

COMMENT POSTULER

Via le portail STCareers (en Anglais):

- https://stcareers.talent-soft.com
- Référence: 2023-35642
- Titre: «STAGE - Outil d'analyse en temps constant de logiciels cryptographiques embarqués M/F».