Offre de stage embarqué/sécurité: améliorer le support des TPM v2.0 du chargeur de démarrage U-Boot

Bootlin

Offre à retrouver sur `https://bootlin.com/fr/blog/stages-2020/`

Présentation de la société

La société Bootlin propose des services de développement et de formation autour de Linux embarqué et son noyau. Créée en 2004 et composée aujourd'hui de 12 personnes, elle dispose d'une expertise reconnue en développement noyau Linux et intégration Linux embarqué. Avec une majorité de clients à l'Étranger, Bootlin compte parmi ses clients de grands fabricants de processeurs et de nombreux producteurs de systèmes embarqués.

Fortement ancrée dans l'Open Source, Bootlin publie tous ses supports de formation gratuitement sous licence libre, et réalise un très grand nombre de contributions au noyau Linux et à d'autres projets de la communauté. Bootlin est régulièrement dans les 20 entreprises contribuant le plus au noyau Linux, à l'échelle mondiale.

Bootlin investit également beaucoup dans l'implication de ses ingénieurs dans la communauté technique, ce qui leur donne une visibilité et une notoriété au delà des murs de la société qui les emploie, qu'on retrouve assez rarement dans d'autres sociétés en France et même ailleurs dans le monde.

Sujet du stage

Le bootloader U-Boot est le chargeur de démarrage de loin le plus utilisé pour démarrer Linux sur la plupart des plateformes embarquées à base de processeur non-x86 (ARM, MIPS, PowerPC, RISC-V, etc.).

L'an dernier, Bootlin a contribué à U-Boot un premier travail sur le support des TPM v2.0 (Trusted Platform Modules), assurant un support minimaliste des fonctionnalités premières. Cela fait quelques années que les TPMs sont utilisés dans le monde des ordinateurs personnels et ils font petit à petit leur arrivée dans le monde de l'embarqué, d'où le besoin d'approfondir ce support initial.

Parmi les nombreuses utilisations que peut avoir un TPM, celle qui nous intéresse serait la délivrance d'un secret à condition que le matériel/logiciel de la plateforme corresponde à un état attendu par le TPM. Cette fonctionnalité est appelée *measured boot* et nécessite une participation de la part du chargeur de démarrage. La fonctionnalité existe déjà mais ne remplit qu'à moitié son rôle puisqu'il n'existe aujourd'hui aucune manière de prévenir une attaque par rejeu (*replay attack*).

La spécification TPM v2.0 prévoit pourtant des mécanismes d'authentification pour se prémunir contre ce type d'attaque et l'enjeu du stage serait de les implémenter et de les contribuer au projet U-Boot officiel.

Dans le cas où l'avancée serait plus rapide que prévue et toujours dans le cadre d'améliorer le chargeur de démarrage U-Boot, il sera possible de contribuer à U-Boot sur d'autres thématiques, tant le nombre de travaux engagés est grand (*refactoring*, passage vers *kconfig*, généralisation du *device model*, etc.

Ce stage s'articulera de la manière suivante :

— Découverte des TPMs et de leur spécifications, rapide état de l'art
— Développement au niveau du code d'U-Boot et tests sur une plateforme matérielle commune (type Beagle Bone Black ou Raspberry Pi + TPM sur SPI)
— Contribution à la communauté et interaction avec les mainteneurs du code que vous aurez modifié

Il vous familiarisera avec des cartes matérielles populaires. Vous découvrirez également les pratiques des développeurs et des mainteneurs d'U-Boot, qui sont proches de celles pratiquées dans la communauté du noyau Linux. Ces connaissances seront sans aucun doute utiles dans votre future carrière dans le domaine du logiciel embarqué et du logiciel libre en général.

Encadrement du stage

Le stage sera encadré par Miquèl Raynal, ingénieur à Bootlin depuis 2017 et contributeur à U-Boot et Linux.

Le stagiaire évoluera dans une équipe d'ingénieurs noyau Linux et Linux embarqué, avec un très fort niveau d'expertise.

Compétences recherchées

— Bonne connaissance du langage C
— Connaissance de Linux embarqué et du noyau (par exemple au travers d'expérimentations sur Raspberry Pi ou équivalent)
— Connaissance minimale de Git
— Compréhension du fonctionnement des communautés open-source, et capacité à communiquer en anglais (IRC, e-mail, etc.)

Informations pratiques

- Lieu:
  - Colomiers, à proximité de Toulouse (accessible en train).
- Dates: entre février et septembre 2020
- Rémunération brute mensuelle: entre 500 et 1000 EUR selon profil (stage de fin d'étude ou milieu d'étude, expérience, etc.)
- Durée de stage: minimum 4 mois
- Candidature: envoyez votre CV et e-mail de motivation à `jobs@bootlin.com`