

Tests

Created	@Dec 16, 2019 2:10 PM
Tags	Rapport

Test Dump mémoire STM32

Pour ces tests nous utilisons 3 clés différentes pour chaque tests. Afin de vérifier que nous trouvons bien la clé et pas des valeurs similaires trouvées dans la mémoire.

- **Clef 1** : 0x2B, 0x7E, 0x15, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x4F, 0x3C
- **Clef 2** : 0x2B, 0x7E, 0x15, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x5F, 0x3C
- **Clef 3** : 0x2B, 0x7E, 0x15, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x3F, 0x3C

Tests

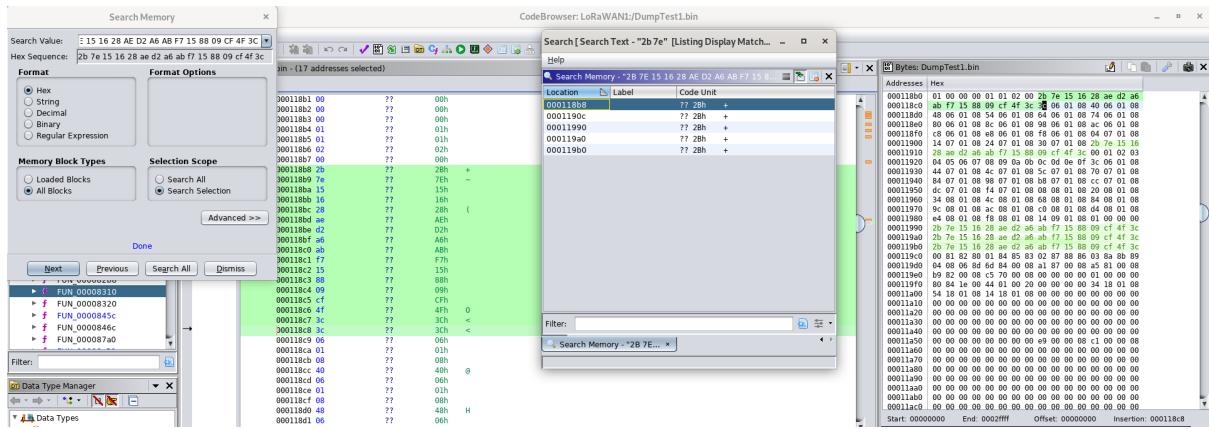
Essais	Tags	Clef	Nombre d'itérations
Validation 1	LoRaMAC	0x2B 0x7E 0x15 0x16 0x28 0xAE 0xD2 0xA6 0xAB 0xF7 0x15 0x88 0x09 0xCF 0x4F 0x3C	5
Validation 2	LoRaMAC	0x2B 0x7E 0x15 0x16 0x28 0xAE 0xD2 0xA6 0xAB 0xF7 0x15 0x88 0x09 0xCF 0x5F 0x3C	3
Validation 3	LoRaMAC	0x2B 0x7E 0x15 0x16 0x28 0xAE 0xD2 0xA6 0xAB 0xF7 0x15 0x88 0x09 0xCF 0x3F 0x3C	3
Validation 4	ProgrammeTest	0x2B 0x7E 0x15 0x16 0x28 0xAE 0xD2 0xA6 0xAB 0xF7 0x15 0x88 0x09 0xCF 0x4F 0x3C	1
Validation 5	ProgrammeTest	0x2B 0x7E 0x15 0x16 0x28 0xAE 0xD2 0xA6 0xAB 0xF7 0x15 0x88 0x09 0xCF 0x5F 0x3C	0
Validation 6	ProgrammeTest	0x2B 0x7E 0x15 0x16 0x28 0xAE 0xD2 0xA6 0xAB 0xF7 0x15 0x88 0x09 0xCF 0x3F 0x3C	0

Conclusions sur les validations

On remarque que à chaque fois nous avons pu retrouver la/les clé(s) dans la mémoire en utilisant le debugger.

Si l'on trouve plusieurs clés pour le programme LoRaMAC c'est car nous avons modifié à chaque fois uniquement les 2 clefs de sessions nécessaires. Le programme LoRaMAC mais en œuvre 5 clefs au total.

Dump Application LoRaMAC



Vous pouvez trouver ci-dessus un dump de la mémoire où l'on a cherché la clé de base du programme LoRaMAC : `0x2B, 0x7E, 0x15, 0x16, 0x28, 0xAE, 0xD2, 0xA6, 0xAB, 0xF7, 0x15, 0x88, 0x09, 0xCF, 0x4F, 0x3C`. Pour préciser le mode de connexion du noeud LoRa était OTAA.

Dump SecApp

Lorsque l'on met en place la sécurité : RDP de niveau 1, il n'est alors plus possible d'utiliser les ports de debugage pour venir lire la mémoire.

Conclusion

On remarque qu'il est assez facile de lire la mémoire d'un micro contrôleur pour un attaquant et qu'il est donc important de verrouiller les ports de debugage.

Il faut aussi noter que pour passer d'un niveau RDP 1 à RDP 0, le procédé est tout aussi facile avec l'utilitaire st-link utility, bien qu'il efface intégralement la mémoire et efface donc le programme qu'elle contient.