Injection de faute sur RSA-CRT

Kévin Boyeldieu
Titouan Tanguy
TLS-SEC

Mars 2018

Procédure d'installation

Pour mettre en place le challenge, il faut avoir une carte FPGA Xilinx Nexys2, ainsi qu'un ordinateur sous Linux avec un port COM et un câble permettant la liaison entre notre FPGA et le port COM de l'ordinateur.
En premier lieu il faut programmer la carte FPGA avec *nexys2_rsa_crt.bit*. Le plus simple pour ce faire est de connecter le port micro-usb de la carte à un port USB de l'ordinateur et d'utiliser la commande :

```
djtgcfg -d Nexys2 prog -i 0 -f nexys2_rsa_crt.bit
```

Dans le cas où l'on voudrait que le programme reste sur la carte après avoir éteint cette dernière il faut utiliser le fichier *nexys2_rsa_crt.mcs* et la commande suivante :

```
djtgcfg -d Nexys2 prog -i 1 -f nexys2_rsa_crt.mcs
```

Ces deux commandes nécessitent l'installation de Digilent Adept software.

Une fois la carte prête, la **LED J14** devrait s'allumer. Il faut alors lancer le programme python *start.py* sur la machine Linux. Cela nécessite les droits administrateurs et la librairie python Flask doit être présente (pip install Flask pour l'installer). Ce programme démarre un serveur local à l'adresse suivante: *http://localhost:5000/*. Il suffit alors de se rendre à cette page pour obtenir une console permettant de récupérer les signatures calculées et envoyées par la carte et répondre au challenge proposé.