Man in the middle pour l'attaque par réplication sur le bus du PCIe

KHELIF Mohamed Amine, MARCUZZI Sylvain, LORANDEL Jordane, ROMAIN Olivier
Laboratoire ETIS - UMR8051 - ENSEA – Université de Cergy-Pontoise
Mohamed.amine.khelif@gmail.com, sylvain.marcuzzi@ensea.fr,
jordane.lorandel@ensea.fr, olivier.romain@ensea.fr.

Résumé :

Le bus PCIe (Peripheral Component Interconnect - Express) est un bus qui permet l'échange de données entre un processeur et des périphériques, comme par exemple une mémoire. D'autres protocoles comme l'USB, l'Ethernet et le WiFi sont aussi très commun et peuvent être attaqué par le rejeu des transactions. Plusieurs attaques ont été démontrées sur le bus USB [1], le WiFi [2] ou encore sur du matériel dédié comme l'Unité de Gestion de Mémoire (MMU) [3]. Un des rares exemples d'attaques Man-In-The-Middle (MITM) sur le bus de PCIe a été réalisé par l'équipe fail0verflow [4] sur la Sony Playstation 4.
Il existe deux types d'attaques MITM: passif ou actif. Le but d'une attaque passive est d'écouter et enregistrer des communications entre deux cibles avec comme principal objectif d'être invisible des autres équipements. Pour l'attaque active le but est d'envoyer des données malveillantes qui peuvent être prédéfinies (attaque par rejeu) à l'hôte, au dispositif ou au deux. Dans notre travail nous avons choisi d'utiliser un FPGA le Stratix V DSP Development Board pour réaliser une attaque de l'homme du milieu passive sur un bus PCIe avec comme principal objectif d'enregistrer toutes les données qui transite entre un processeur et un périphérique (mémoire). L'analyse des transactions sur la mémoire permettra d'identifier des données sensibles, comme un mot-de-passe.
L'architecture proposée pour réaliser cette attaque est présentée sur la Figure 1.

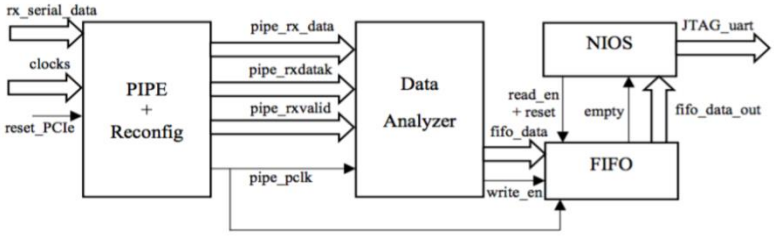

Figure 1:Schéma simplifier de l'architecture sur le FPGA.

Le premier bloc est une IP PHY d'Altera pour le PCIe [5]. Il réalise l'interface avec les chemins physiques du bus et contient les émetteurs-récepteurs PHY, un encodeur/décodeur 8b/10b, un aligneur de mot, etc. Les données sont envoyées et analysées pour garder seulement les données utiles. L'analyse est basée sur les marqueurs SDP et STP qui indiquent le début d'un paquet de données et d'un paquet de transaction respectivement. Les paquets sont alors stockés dans une mémoire FIFO et une interruption est générée au processeur NIOS. Ce dernier lit les données et les affiche en texte pour le nouveau traitement, comme illustré sur la Figure 2. Comme le processeur NIOS est plus lent que le FIFO, une machine à état finis gère le transfert des données entre eux.

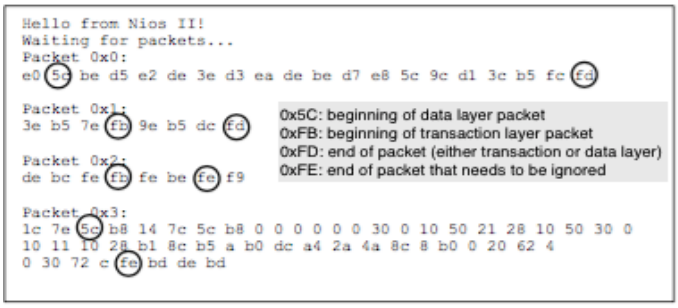

Figure 2: Données obtenu pour l'analyse.

Références :

[1] withdk, «BadUSB2-mitm-poc,» June 2016. [En ligne]. Available: https://github.com/withdk/badusb2-mitm-poc.

[2] WiFi Pineapple, «The WiFi Pineapple wireless auditing platform,» 2017. [En ligne]. Available: https://wifipineapple.com/.

[3] B. Morgan, É. Alata, V. Nicomette et M. Kaâniche, «Bypassing IOMMU Protection against I/O Attacks,» chez Seventh Latin-American Symposium on Dependable Computing (LADC), Cali, 2016.

[4] fail0verflow, «33c3 - team Fail0verflowrunning Linux on PS4,» 2016. [En ligne]. Available: https://www.youtube.com/watch?v=-AoHGJ1g9aM.

[5] Altera, «Altera Transceiver PHY IP Core User Guide,» May 2016. [En ligne]. Available: https://www.altera.com/content/dam/altera-www/global/en_US/pdfs/literature/ug/xcvr_user_guide.pdf.