IOMMU et attaques DMA

Jean-Christophe Delaunay
Jérémie Boutoille

SYNACKTIV
jean-cristophe.delaunay@synacktiv.com
jeremie.boutoille@synacktiv.com

Avec l'utilisation généralisée des technologies de virtualisation, de Cloud et des besoins toujours plus importants en matière de performances, des techniques visant à accélérer le traitement des données ont été créées et intégrées. Parmi ces technologies, le Direct Memory Access (DMA) permet, sous certaines conditions, de contourner des mécanismes de sécurité implémentés par les composants logiciels et matériels. Afin de limiter les risques de sécurité relatifs au partage de ressources entre composants virtualisés et leur hôte, un nouveau composant appelé Input Output Memory Management Unit (IOMMU) a été intégré. Cette IOMMU détermine notamment les accès mémoire pouvant être réalisés par les composants situés sur le bus PCI.
Ce document a pour but d'exposer le fonctionnement et l'intégration de l'IOMMU par les principaux systèmes d'exploitation utilisés de nos jours (Windows, macOS et Linux). A partir de cet état de l'art, une revue des attaques existantes par DMA est présentée.
Ces travaux proviennent de l'état de l'art réalisé en prévision d'un nouveau projet RAPID 1 par Synacktiv : DMArvest.

1. https ://www.defense.gouv.fr/aid/soutenir-vos-projets/subventions/rapid

Mots clé |
DMA, IOMMU, ACLs, PCI Express, attaques logicielles, attaques matérielles, Windows, Linux, macOS, pcileech, Thunderclap