Comment déjouer les mesures de sécurité des puces informatiques en privant les ordinateurs de courant

Les informaticiens ont montré qu'il était possible de rendre les unités centrales de traitement (CPU) d'Intel vulnérables aux attaques en manipulant la tension de fonctionnement des processeurs.

ÉCONOMIE NUMÉRIQUE

© metamorworks, Shutterstock

Afin de répondre aux besoins toujours croissants de performance et d'efficacité, il est crucial d'optimiser les processeurs des ordinateurs et d'ajuster leur fréquence et leur tension en fonction des besoins. Plutôt que de consommer de l'énergie sans arrêt, 24 heures sur 24, ce qui produirait trop de chaleur, comme dans un centre de données, et épuiserait rapidement la batterie, comme sur les dispositifs mobiles, les puces sont conçues pour utiliser exactement la quantité appropriée de puissance dont leur processeur a besoin pour accomplir une tâche spécifique. Dans une procédure dite de sous-voltage ou de survoltage, grâce à ce que l'on appelle des interfaces logicielles privilégiées, les systèmes modernes peuvent fonctionner correctement dans des conditions de travail déterminées. De nombreux processeurs, dont la série très répandue Intel Core, reposent sur cette technologie. Mais comment protéger les données lorsqu'un attaquant utilise des moyens physiques pour compromettre la sécurité des puces informatiques?

Partiellement soutenue par les projets FutureTPM et SOPHIA, financés par l'UE, une équipe de scientifiques a montré que ces interfaces logicielles peuvent être

exploitées pour compromettre la sécurité du système. Dans un document de recherche, ils expliquent comment ils ont pu corrompre l'intégrité de l'Intel Software Guard Extensions (SGX): un ensemble de codes d'instruction liés à la sécurité, intégrés dans les processeurs Intel modernes. Le SGX aide à protéger les calculs sensibles à l'intérieur de ce que l'on appelle des enclaves. Leur contenu est protégé et ne peut être consulté ou modifié depuis l'extérieur de l'enclave, même en présence des types de logiciels malveillants les plus avancés.

Manipulation de la tension

Les mêmes scientifiques ont réussi à démontrer la faille de sécurité en contrôlant la tension lors de l'exécution des calculs de l'enclave. «Nous présentons l'attaque Plundervolt, dans laquelle un adversaire logiciel privilégié abuse d'une interface non documentée de mise à l'échelle de la tension de l'Intel Core pour corrompre l'intégrité des calculs de l'enclave Intel SGX.» Ils ajoutent: «Plundervolt contrôle soigneusement la tension d'alimentation du processeur pendant un calcul d'enclave, induisant des défauts prévisibles dans l'ensemble du processeur. Par conséquent, même la technologie de cryptage/authentification de la mémoire d'Intel SGX ne peut pas protéger contre Plundervolt.»

Ils ont conclu que leurs recherches «apportent une preuve supplémentaire que la promesse d'exécution enclavée de l'externalisation de calculs sensibles vers des plates-formes distantes non fiables crée de nouvelles surfaces d'attaque inattendues qui continuent d'être pertinentes et doivent continuer d'être étudiées».

Comme l'indique un communiqué de presse de l'université de Birmingham, partenaire du projet FutureTPM, «Intel a déjà répondu à la menace de sécurité en fournissant une mise à jour du microcode pour atténuer Plundervolt». Cité dans le même communiqué de presse, l'auteur du document de recherche, David Oswald, de l'Université de Birmingham, déclare: «À notre connaissance, la faiblesse que nous avons découverte n'affectera que la sécurité des enclaves SGX. Intel a répondu rapidement à la menace et les utilisateurs peuvent protéger leurs enclaves SGX en téléchargeant la mise à jour d'Intel.»

Le projet FutureTPM (Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module), qui a permis de financer la recherche, se poursuivra jusqu'en décembre 2020. Ses technologies de modules de plate-forme sécurisée (TPM) sont déjà largement utilisées. Les partenaires du projet estiment qu'en plus de l'informatique à sécurité multiniveau, le projet FutureTPM a un impact significatif sur d'autres applications de la cryptographie appliquée en général. Le projet SOPHIA (Securing Software against Physical Attacks), qui a également soutenu le projet de sécurité Plundervolt, se concentre sur l'exécution de logiciels de manière sûre et efficace en présence d'attaques physiques. Il couvre la sécurité matérielle, les

architectures de systèmes sécurisés, les mises en œuvre cryptographiques et les canaux secondaires.

Pour plus d'informations, veuillez consulter:
site web du projet FutureTPM
projet SOPHIA

Pays

Autriche

Projets connexes

FutureTPM

Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module

7 Septembre 2023

PROJET

SOPHIA

Securing Software against Physical Attacks

3 Octobre 2023

PROJET

Articles connexes

PROGRÈS SCIENTIFIQUES

Des failles de sécurité informatique révèlent que la rapidité n’est pas nécessairement un avantage

4 Mai 2018

Dernière mise à jour: 30 Janvier 2020

Permalink: https://cordis.europa.eu/article/id/413290-how-to-breach-computer-chip-security-by-starving-computers-of-voltage/fr