CYBER

hackAtech

Shake science. Shape innovation.

#cybersécurité

#hacking

#incidents

CYBERSÉCURITÉ
Se défendre contre les menaces numériques

Inria

CARACTÉRISTIQUES

La digitalisation de notre société change radicalement la manière dont les systèmes informatiques sont utilisés. Nous sommes nombreux à être connectés continuellement sur Internet, nous sommes ainsi exposés en permanence à des attaques : les données sensibles peuvent être volées, modifiées ou détruites.

La **cybersécurité** est la protection des systèmes informatiques par rapport aux vols et dommages sur leur matériel (*hardware*), logiciel (*software*) ou architecture. Plus précisément, la cybersécurité permet à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité, la confidentialité, ou les preuves associées (*identité, authenticité, traçabilité*) des données stockées, traitées ou transmises.

Habituellement, les attaques contre des systèmes d'informations n'impliquent pas de hardware mais exploitent la vulnérabilité des softwares. Cependant des attaques récentes, telles que Rowhammer, CLKSCREW, Spectre ou Meltdown ont montré qu'une attaque implémentée dans un logiciel peut utiliser les spécificités du matériel pour arriver à leurs fins. Ces nouvelles attaques sont dangereuses puisqu'elles rendent possibles les attaques du matériel à distance.

QUELS ENJEUX ?

- Protection des données sensibles et privées
- Sécurité des systèmes informatiques des collectivités et entreprises
- Continuité de service des administrations


© Jirsi/ Fotolia

USE CASES

- **Identification et neutralisation de fichiers malveillants :** virus, rançongiciel
- **Détection d'intrusion dans des systèmes**
- **Protection des systèmes,** y compris IoT (maisons connectées, industrie automobile.

Exemples

- **Startup Malizen :** commercialise ZeroKit, une plateforme collaborative pour fluidifier le travail des équipes cyber. Elle leur permet de centraliser les données, de les explorer intuitivement grâce à des datavis automatiques et un suivi par machine learning, de collecter et partager les points d'intérêt et les pistes, puis d'exporter des rapports interactifs.
- **Startup Daspren :** a développé PARAD, une solution de protection des données face aux nouveaux rançongiciels (ransomware) inconnus. Parmi les technologies qu'utilise PARAD se trouve DaD (Data Aware Defense), une technologie Inria développée au sein de l'EPI Tamis et du LHS (Laboratoire Haute Sécurité)..

FICHE IDENTITÉ

- Équipes projet : Cidre, Emsec, Pacap, Cairn et Diverse

FONCTIONNALITÉS GÉNÉRIQUES

Focus sur deux domaines de recherche à Inria

PROCESSEURS DURCIS : un enjeu sécuritaire majeur de la décennie

Caractéristiques

Le durcissement des processeurs est l'ensemble des techniques permettant de renforcer les propriétés de sécurité en leur sein. Confidentialité: l'attaquant ne doit pas pouvoir extraire d'information non autorisées. Intégrité: il ne doit pas pouvoir altérer le système. Disponibilité: il ne doit pas pouvoir l'empêcher de fonctionner ni même le ralentir significativement.

Le durcissement est devenu un enjeu majeur depuis 2018 et la médiatisation des attaques Spectre et Meltdown montrant qu'il est possible d'utiliser le comportement spécifique du processeur, le matériel, pour induire des vulnérabilités logicielles. Régler cette nouvelle classe de vulnérabilité s'est montré très ardue, et n'a toujours pas de solution faisant consensus.

Cas d'usages

- **Infrastructures critiques:** sécurisation des processeurs assurant les services critiques: énergie, transport, communications, ...
- **Médical :** éviter les perturbations des services de soin à cause de menaces logicielles.
- **Défense :** protéger les équipements militaires des attaques informatiques.

SUPERVISION DE LA SÉCURITÉ : détection d'intrusions et de fuite d'informations sensibles

Blare, un moniteur de flux d'information

Blare est un moniteur de flux d'information opérant au niveau du système d'exploitation. Grace à un mécanisme de propagation de teinte, Blare surveille les flux d'information entre les fichiers, processus, sockets et pages mémoires. Blare permet d'identifier la contamination de l'OS par un programme éventuellement malveillant.

Blare est implanté sous Linux et Android en tant que Patches du noyau permettant de suivre les flux d'informations entre les objets du systèmes (*processus, fichiers, sockets, etc*) et d'en évaluer la légalité vis-à-vis d'une politique de sécurité (*politique de flux*). En outre, une implémentation dans la JVM existe, ainsi qu'une implémentation pour surveiller les flux entre machine sur le réseau.

Aspects innovants

- Pas besoin d'une connaissance préalable des attaques.
- L'outil permet de vérifier le respect de politiques qui ne se restreignent pas au control des accès mais portent sur la circulation de l'information.
- Les versions Linux et Android sont implémentées dans le noyau en tant que Linux Security Module (LSM) : overhead réduit.
- L'ensemble des hôtes surveillés peut collaborer afin de suivre les flux d'information inter-hôtes.

CONNAISSANCES MINIMUM REQUISES

- **Connaissances des systèmes (Windows, Linux, Android)**
- **Connaissances informatiques (pare-feu, réseau, IA)**
- **Langages de programmation (C et python)**

READ ME : https://www.slideshare.net/INRIA/inria-cybersecurity-current-challenges-and-inrias-research-directions-131352245

Référents :

Belkacem Teibi (DASPREN)

belkacem.teibi@inria.fr

Christopher Humphries (MALIZEN)

christopher.humphries@inria.fr

INSTITUT CARNOT Inria

UNION EUROPÉENNE

l'Europe s'engage en France

Inria