ZEROKIT

Un outil d'investigation pour les experts en cybersécurité

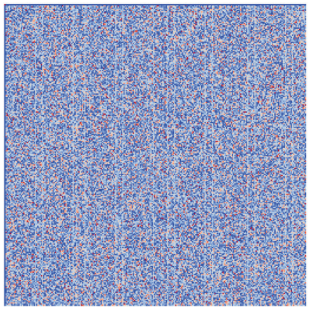
Dans un monde de plus en plus dépendant de l'interconnexion des réseaux et des données, la cybersécurité devient un enjeu essentiel. La sécurisation d'un système d'information repose à la fois sur différents outils proactifs ainsi que sur de bonnes pratiques. Mais lorsqu'un incident de sécurité arrive, il est nécessaire de comprendre, d'explorer et d'analyser le système d'information afin de découvrir, de remédier et de corriger le problème. ZeroKit est un outil collaboratif d'exploration des journaux d'évènements à destination des experts en cybersécurité. En leur permettant de structurer les données, de les explorer à l'aide de visualisations et d'expliquer l'incident sous forme de rapport, ZeroKit permet aux experts d'intervenir plus vite et mieux sur les incidents de sécurité. La collaboration étant au cœur de la plateforme, plusieurs analystes peuvent travailler en même temps sur le même incident et se transmettre point d'intérêts et commentaires directement.

Thèmes :
supervision de sécurité,
analyse d'incident

CONTACT :
Simon Boche, startup Malizen
(issue du centre Inria de Rennes)
https://malizen.com/
simon@malizen.com

SECRET

Vers de nouveaux standards cryptographiques internationaux



La sécurité informatique repose sur des algorithmes cryptographiques sûrs et efficaces. En pratique, les concepteurs de produits choisissent d'intégrer des algorithmes standards qui ont été choisis par les différents organismes de normalisation et standardisation (NIST, ISO/IEC, IETF, etc.) après que ces algorithmes aient été soigneusement analysés et éprouvés longuement par de nombreux spécialistes partout dans le monde. Les menaces nouvelles que font porter les ordinateurs quantiques sur les algorithmes de chiffrements que nous utilisons aujourd'hui rendent nécessaire la conception de nouveaux algorithmes reposant sur des problèmes très difficiles (voire impossibles) à résoudre même pour un ordinateur quantique. Deux concours ont été organisés par le NIST américain : l'un vise à choisir un nouvel algorithme de chiffrement public à sécurité quantique, l'autre porte sur des algorithmes symétriques légers pour l'IoT. L'équipe-projet Cosmiq d'Inria (ex-équipe-projet Secret) a soumis des propositions de chiffres pour ces deux compétitions. Les détails de ces algorithmes seront présentés sur notre stand.

Thèmes :
cryptographie, post-quantique, bas coût, sécurité de l'IoT, concours, normalisation

CONTACT :
Leo Perrin
Équipe-projet Cosmiq
Inria, Paris
leo.perrin@inria.fr

Inria

SCUBA

Audit Automatisé de la sécurité des objets connectés

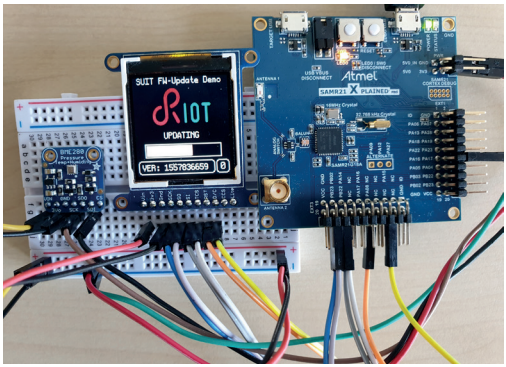
Les objets connectés sont utilisés dans différents domaines d'application, non seulement pour le grand public, mais aussi dans des milieux industriels. La sécurité de ces objets est rarement évaluée d'une manière automatisée à cause du manque d'outils, mais aussi à cause du nombre important et de l'hétérogénéité de ces objets. Les pratiques actuelles sont très artisanales, avec très peu d'aide algorithmique et outils pour construire les scénarios d'évaluation. Celles-ci sont menées principalement par des experts humains. Il est indispensable de développer des outils pour générer les tests de sécurité de ces objets dans des scénarios d'usage assez réalistes. Nous présentons SCUBA Box, un système pour évaluer automatiquement le niveau de sécurité d'un environnement d'un objet connecté en prenant en compte les interactions de l'objet, son environnement, ses profils de sécurité et sa composition logicielle. Une démonstration suivra pour montrer la box et son application associée qui permet de fournir aux usagers les niveaux de sécurité de plusieurs objets vendus dans le commerce, tant pour le grand public que pour l'industrie.

CONTACT :
Jerôme François, Thomas Lacour et Abdelkader Lahmadi (Équipe-projet Resist, Inria Nancy), Frédérick Beck (LHS, Inria Nancy)
jerome.francois@inria.fr
thomas.latour@inria.fr
abdelkader.lahmadi@loria.fr
frederic.beck@inria.fr

Thèmes :
sécurité IoT,
évaluation de la sécurité

Inria

Mises à jour logicielles sécurisées sur microcontrôleurs à basse consommation avec RIOT



Lorsqu'une faille de sécurité est découverte dans un ensemble d'équipements IoT sans fil déjà déployés, il n'est possible de la corriger à distance et d'assurer le maintien de la sécurité de l'ensemble du déploiement que si le système de gestion des équipements fournit un mécanisme de mise à jour fiable et robuste. Ces mises à jour sécurisées sont difficiles, car certains des dispositifs fonctionnent sur du matériel contraint (tel que des microcontrôleurs), disposant de très peu de mémoire (des dizaines de kilo-octets), de CPU lents (des dizaines de MHz), fonctionnant sur batterie et utilisant un réseau sans fil à faible bande passante (quelques kbit/s).

RIOT- **https://riot-os.org** - est un système d'exploitation conçu pour les dispositifs IoT basés sur des microcontrôleurs. Ce système d'exploitation fournit tous les éléments de base pour effectuer des mises à jour de micrologiciels avec des protocoles standard et une sécurité de bout en bout. Une large gamme de protocoles de communication IoT sont gérés (tels que 802.15.4, BLE ou LoRa). Des bibliothèques cryptographiques de pointe, optimisées pour des dispositifs très contraints, sont utilisées pour vérifier l'authenticité des mises à jour. Une implémentation du futur protocole standard de mise à jour de firmware de l'IETF (Internet Engineering Task Force) appelé SUIT (Software Updates for the Internet of Things) est aussi disponible. La démonstration montrera comment tous ces éléments de base sont réunis en conjonction avec une véritable application IoT (un moniteur de qualité de l'air) pour effectuer des mises à jour tout en envoyant les données des capteurs de gaz à un tableau de bord public sur le Web.

CONTACTS :
Alexandre Abadie et Francisco Molina
(ingénieurs Inria, Saclay),
Emmanuel Baccelli
(Équipe-projet Infine / TRiBE, Inria, Saclay)
alexandre.abadie@inria.fr
francois-xavier.molina@inria.fr
emmanuel.baccelli@inria.fr

Thèmes :
sécurité IoT,
mise à jour sécurisée

Inria

HARDBLARE

Un co-processeur dédié au suivi des flux d'information

HardBlare propose une solution à la fois matérielle et logicielle permettant de détecter des attaques logicielles contre la confidentialité et l'intégrité.

HardBlare implante un suivi dynamique des flux d'information (DIFT). Le DIFT consiste à (1) attacher des étiquettes à des conteneurs d'information (par exemple des fichiers, des variables de pro- gramme ou des registres), à spécifier une politique de flux d'information (par exemple définissant si les contenus de deux fichiers peuvent se mêler dans un troisième) et (2) à propager les étiquettes lors de l'exécution des applications pour refléter les flux d'information qui se produisent et détecter ceux qui violent la politique définie.

HardBlare combine un DIFT à grain fin (au niveau hardware) avec un marquage (étiquetage) au niveau du système d'exploitation ou l'utilisateur peut plus naturellement spécifier une politique de sécurité.

Nous avons conçu un co-processeur DIFT multi-cœur dédié sur FPGA, isolé du CPU principal et qui ne nécessite aucune modification de ce CPU principal. L'isolation de ce co-processeur DIFT le protège des attaques logicielles visant les applications exécutées sur le CPU principal. Le co-processeur isolé doit obtenir cependant des informations du CPU principal sur les flux d'information engendrés par les exécutions d'applications. Ces informations requises par le DIFT sont obtenues à la fois grâce à un précalcul pendant l'étape de compilation des applications et à des mécanismes d'instrumentation et de traces matérielles au moment de l'exécution.

Nous avons implémenté notre approche sur la Digilent ZedBoard en utilisant le SoC Xilinx ZYNQ qui combine deux hardcores (ARM Cortex-A9) avec un FPGA Xilinx. Nous avons modifié le noyau Linux pour gérer l'étiquetage des fichiers. Nous avons également développé un pass LLVM pour implémenter les étapes de précalcul et d'instrumentation.

Dans cette démonstration, organisée dans le cadre du semestre thématique du SILM sur la sécurité des interfaces logiciels/matériels (https://semestres-cyber.inria.fr/en/silm/), nous allons illustrer comment cette approche peut être utilisée pour détecter des attaques classiques sur un système Linux.

CONTACTS :
Guillaume Hiet
Équipe-projet Cidre Inria, Rennes
guillaume.hiet@centralesupelec.fr
Pascal Cotret, ENSTA Bretagne
pascal.cotret@ensta-bretagne.fr
Mounir Nasr Allah, CentraleSupélec
mounir.nasrallah@centralesupelec.fr

Thèmes :
détection d'intrusions,
support matériel

Inria