Architecture de sécurité distribuée pour réseaux hostile

Contexte

BAG-ERA (http://bag-era.fr) développe des solutions d'intégration et de supervision d'infrastructure numérique dédiées au monde de l'industrie. Nous permettons la modernisation des chaînes de production sans toucher à l'existant, en vue de maîtriser, superviser et optimiser les systèmes de production.

BAG-ERA déploie ses solutions dans des usines ou sur des sites de production énergétique pouvant compter de quelques dizaines de machines à quelques centaines de machines (automates et pc de contrôle inclus). Les composants logiciels sont déployés sur des passerelles industrielles (ex: strato PI https://www.sferalabs.cc/strato/, MyPI http://www.embeddedpi.com/), des serveurs edge mais aussi des PC Windows de différentes générations. De plus un certains nombres de capteurs et actionneurs de type IoT sont déployés pour améliorer la gestion des systèmes de productions. L'ensemble de ces composants se retrouve connectés sur un réseau local, dont une partie peut avoir (temporairement ou en permanence) accès a Internet. Il est donc primordial de garantir la sécurité des échanges de données et des composants.

Sujet

L'objectif de cette thèse est de spécifier et implémenter une infrastructure de sécurité pour vérifier l'intégrité des flux d'un dispositif de contrôle de systèmes industriels. Ce dispositif innovant de contrôle de flux de commande en contexte dynamique sera intrinsèquement sûr et devra fournir des garanties d'intégrité. La sécurité des systèmes reposant principalement sur le chiffrement et l'authentification, les principales menaces portent sur l'établissement des clefs de chiffrement et de signature électronique. La gestion de ces clefs repose généralement sur des algorithmes asymétriques afin de permettre un renouvellement unilatéral et des mécanismes de non-répudiation.

Le principal challenge est le renouvellement des clefs de session pour un process continu, sans interruption notoire du fonctionnement du système industriel et du client intranet, et ceci en anticipant un contexte de longue durée de vie des systèmes (15 à 30 ans). S'il est possible d'utiliser une architecture PKI relativement classique avec autorités de certification et d'enregistrement, il faut définir une gestion des masters-clefs pérenne pour la durée de vie de la plate-forme, un renouvellement réaliste des clefs de sessions sur les dispositifs et des processus de distribution et de pose des clefs devant prendre en compte l'hétérogénéité et la résilience des composants.

En effet, les paramètres de bande passante et les débits de communication des différents acteurs induisent un besoin de personnalisation de l'architecture afin de prendre en compte l'aspect hétérogène des matériels. La fréquence des transferts de certificats, celle du renouvellement des clefs, la prévention des DoS, etc. doivent être adaptés à un passage en production du composant. Le risque est ici dans la définition correcte d'un compromis entre sécurisation, légèreté de l'architecture mise en place et évolutivité des supports.

En particulier, le verrou principal à lever est la mise au point d'une architecture de sécurité réduisant les communications et s'adaptant à un contexte matériel fortement évolutif tout en conservant les propriétés de sécurité. Une première approche consisterait à construire un système de PKI (public-key infrastructure) à révocation hybride entre OCSP (pour limiter les calculs au

niveau du client) et Novomodo (pour limiter les volumes de communications). Cela ne résoudrait toutefois sans doute pas complètement le problème du cloisonnement et de l'évolutivité des supports. Adjoindre une plus grande hiérarchie ou un méta web of trust au-dessus de ces hiérarchies, ou encore une solution utilisant une blockchain de consortium devra très certainement être envisagée.

Enfin une procédure d'analyse dédiée doit également être élaborée et des extensions à la sécurisation des DNS (une approche hybride mixant DNSSec etles techniques évoquées pourrait-elle mieux prendre en compte les problèmes de résilience) ou à l'analyse forensique dynamique des systèmes de contrôle industriel, sont clairement possibles.

Implémentation

Cette thèse s'effectuant dans une startup il est primordial que les résultats obtenus puissent être transférés rapidement. Pour cela l'équipe technique de BAG-ERA apportera un soutien technique. Il sera demandé de qualifier les solutions au regard de leurs implémentations ainsi que de réaliser (avec l'aide d'ingénieur R&D de BAG-ERA) un ou plusieurs démonstrateurs.

Rémunération

selon profile

Dates

Date limite de candidature : 31 août 2019

Date souhaité pour le début de la thèse : Octobre 2019

Contact

E: maxime.louvel@bag-era.fr

A: 16 Boulevard Maréchal Lyautey, 38000 Grenoble

W: http://bag-era.fr

Références:

[1] DPKI: Decentralized Public Key Infrastructure. Allen et al., 2015. https://danubetech.com/download/dpki.pdf

[2] Security Architecture for Point-to-Point Splitting Protocols. Badrignans et al., IEEE World Congress on Industrial Control Systems Security 2017. https://hal.archives-ouvertes.fr/hal-01657605

[3] ARPKI: Attack Resilient Public-Key Infrastructure, Cremers et al. ACM CCS 2014. https://netsec.ethz.ch/publications/papers/ccsfp200s-cremersA.pdf

[4] LocalPKI: An Interoperable and IoT Friendly PKI. Dumas et al., Comm. on Comp. & Information Science 2019. https://hal.archives-ouvertes.fr/hal-01963269

[5] Certificate Transparency, Laurie et al. 2013. https://tools.ietf.org/html/rfc6962

[6] IKP: Turning a PKI around with decentralized automated incentives. Matsumoto & Reischuk, S&P 2017. https://www.ieee-security.org/TC/SP2017/papers/290.pdf

[7] Évaluation de la confiance dans les architectures de sécurité. J-B. Orfila, PhD thesis, U. Grenoble Alpes, France, 2018. https://tel.archives-ouvertes.fr/tel-01985183

[8] Sécurité des systèmes industriels : filtrage applicatif et recherche de scénarios d'attaques. Maxime Puys, PhD thesis, U. Grenoble Alpes, France, 2018. https://tel.archives-ouvertes.fr/tel-01893142

[9] A blockchain-based PKI management framework. Yakubov et al., IEEE/IFIP Network Operations and Management Symposium 2018. http://publications.uni.lu/bitstream/10993/35468/1/blockchain-based-pki.pdf