



Les enjeux de la cybersécurité au sein des bâtiments intelligents

Le cas des protocoles BACnet et EtherCAT

Florian Billon – Oualid Koucham

Courte présentation



- ICS Cybervision : Cybersécurité pour l'Internet industriel
 - Analyse de comportements via DPI
 - Visualisation du réseau industriel

Bâtiments intelligents

- Historiquement : GTC/GTB
 - GTC : Gestion Technique Centralisée, supervision d'un lot (électricité, chauffage..)
 - GTB : Gestion Technique des Bâtiments, supervision plus globale de l'ensemble des systèmes
- Aujourd'hui :
 - Plus d'équipements (IoT)
 - Nouveaux standards, plus ouverts
 - Interopérabilité
 - Gestion à distance

Quels enjeux ?



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco IoT

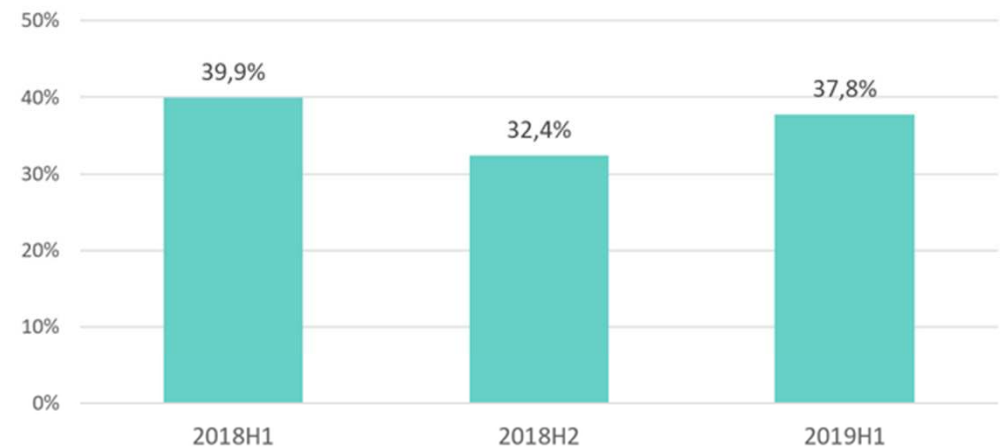
Quels enjeux ?

- Les attaquants s'y intéressent

Hacking Blamed For Late Night
Emergency Sirens In Dallas

**“Mr. Robot” played to our worst
technology fears with a mini horror
movie about a hacked smart home**

**Internet-connected industrial
refrigerators can be remotely
defrosted, thanks to default
passwords**



Smart building systems on which malware was blocked, 2018-2019

Quels enjeux ?

- Les solutions de sécurité aussi

SABOTAGING COMMON IOT DEVICES IN SMART BUILDINGS BY EXPLOITING UNENCRYPTED PROTOCOLS

IBM'S X-Force team nacks into smart building



Siegeware: When criminals take over your smart building

BACnet

- Présentation
- Exemples d'attaques

BACnet

- ASHRAE BACnet, créé en 1987 à l'université Cornell
 - Standardisé par l'ANSI en 1995 puis par l'ISO en 2003
- Protocole dédié au domaine du bâtiment et supporté par des centaines de vendeurs
- Utilisé dans différents lots techniques:
 - Chauffage
 - Ventilation
 - Contrôle d'accès physique
 - ...

BACnet : modèle d'information

- Objets caractérisés par des propriétés
- Peuvent représenter des informations physiques (état des entrées/sorties) ou des informations logiques (applications, calculs, logiques de contrôle,...)
- Exemple : Objet de type *Device*
 - VENDOR_NAME
 - FIRMWARE_REVISION
 - ...

BACnet : services et réseaux

- 5 catégories de services
 - Accès aux objets (lecture, écriture, création, suppression)
 - Gestion d'équipements (découverte, synchronisation d'horloge,...)
 - Alarmes et événements
 - Transfert de fichiers
 - Console virtuelle
- **BACnet/IP**, BACnet MS/TP (RS485), BACnet ISO 8802-3,...
- BACnet Security Services (2009) : AES-CBC, HMAC, fraîcheur des données,...

BACnet : exemples d'attaques

■ Reconnaissance

- Utilisation de messages Who-Is afin de récupérer des informations sur les adresses et identifiants des composants BACnet
- Utilisation de messages Who-Has afin d'identifier les composants BACnet détenant un objet (tel qu'un capteur de température)
- Utilisation de messages Read-Property afin de collecter des informations sur l'identifiant du vendeur, le nom du modèle, ainsi que les objets et services implémentés

■ Usurpation de messages BACnet

- Usurpation d'identité via des réponses I-Am suite à des requêtes Who-Is
- Redirection de trafic en usurpant l'adresse source des messages de type I-Am-Router-To-Network

BACnet : exemples d'attaques

- **Attaques exploitant le modèle d'abonnement de BACnet**
 - Possibilité pour les clients de s'abonner à certaines variables sur un serveur BACnet
 - Notification à chaque changement de valeur des variables
 - Ces notifications peuvent nécessiter un acquittement de la part des abonnés (Confirmed notifications)
 - `APDU_Timeout` : paramètre fixant le temps d'attente avant retransmission d'une notification non acquittée
 - `Number_Of_APDU_Retries` : paramètre fixant le nombre maximal de tentatives
 - Attaque : abonnement à tous les équipements BACnet sur le réseau, en exigeant l'acquittement des notifications et avec un paramètre `APDU_Timeout` bas
 - Renouvellement de l'abonnement et/ou multiples abonnements

BACnet : exemples d'attaques

■ Attaques par canaux cachés

- Flux d'information violant la politique de sécurité du système
- Exfiltration d'information, communication serveur C&C et bots dans un botnet
- Utilisation de messages BACnet légitimes afin d'établir un canal caché
- Paramètres : identifiant du réseau pour les NPDU, identifiant du composant pour les requêtes Who-Has
- Encodage : Who-Has → 00, Who-Is → 01, Who-Is-Router-To-Network → 10, I-Am-Router-To-Network → 11

■ Ecriture de variables

- Utilisation de messages Write-Property afin d'interférer avec le comportement nominal du processus physique

EtherCAT

- Présentation
- Exemples d'attaques
- Vecteurs potentiels

EtherCAT

- Ethernet for Control Automation Technology
- Publié en 2003
- Systèmes temps réel, temps de réponses déterministes
- Lecture/Ecriture à la volée

EtherCAT : point de vue réseau

- Topologies flexibles : En étoile, en bus, en anneau
- Paquets Ethernet (0x88a4) ou au dessus d'UDP
- Un “maître” et des “esclaves”
- Utilisation presque optimale de la bande passante
 - Une ou plusieurs commandes par paquets
 - Système de mapping mémoire : même commande pour plusieurs équipements

Exemples d'attaques

- Pas d'authentification, pas de confidentialité
- Injection de paquets et usurpation d'adresse MAC
 - Lancement d'actions sur les équipements
- Attaque Man In The Middle
 - Interception de commandes
 - Modification de valeurs de capteurs

Autres vecteurs potentiels

- Désynchronisation d'horloges
- Changement de mapping mémoire
- Altération/perturbation des communications entre “maîtres”
- Saut dans les compteurs
- Paquets invalides
- ...

Quelles mesures prendre ?

- Segmenter le réseau et en restreindre l'accès
- Appliquer les mises à jour/être conscient des vulnérabilités
- Mettre en place des systèmes de surveillance
 - IDS, avec des règles spécifiques
 - Outil spécialisé pour un suivi plus fin

Sources

<https://www.welivesecurity.com/2019/02/20/siegeware-when-criminals-take-over-your-smart-building/>

<https://www.forescout.com/company/blog/sabotaging-smart-building-iot-devices-using-unencrypted-protocols/>

<https://ics-cert.kaspersky.com/reports/2019/09/19/threat-landscape-for-smart-buildings-h1-2019-in-brief/>

<https://techcrunch.com/2019/02/08/industrial-refrigerators-defrost-flaw>

<https://www.npr.org/sections/thetwo-way/2017/04/08/523147464/hacking-blamed-for-late-night-emergency-sirens-in-dallas>

http://www.ethercat.org/pdf/ethercat_e.pdf

https://www.ethercat.org/pdf/english/EtherCAT_Introduction_0905.pdf

<https://infosys.beckhoff.com/english.php?content=../content/1033/ethercatsystem/2469135243.html&id=>

J. Kaur, J. Tonejc, S. Wendzel, and M. Meier, “Securing BACnet’s Pitfalls,” in IFIP Sec’15

P. Ciholas, A. Lennie, P. Sadigova, and J. M. Such, “The security of smart buildings : a systematic literature review,” CoRR, vol. abs/1901.05837, 2019

D. G. Holmberg, N. I. of Standards, and T. (U.S.), “BACnet wide area network security threat assessment,” U.S. Dept. of Commerce, National Institute of Standards and Technology [Gaithersburg, Md.], 2003

