COMMUNIQUER

LA CYBERSÉCURITÉ DES RÉSEAUX TSN

Le Time Sensitive Networking introduit la notion de temps-réel dans l'Ethernet standard. Sans entraîner une profonde révision technologique, la sécurité des réseaux TSN nécessite de tenir compte du déterminisme qui régit l'acheminement des données. René Hummen et Oliver Kleineberg de la société Belden nous apportent leur expertise sur ce point.

En introduisant des propriétés de communication en temps réel et une garantie de service, la technologie TSN pose de nouveaux défis en matière de sécurité informatique. Ils peuvent heureusement être gérés par les mécanismes et les procédures de protection existants et éprouvés, à condition de s'appuyer sur les bonnes pratiques mises en œuvre pour la sécurité du réseau industriel.

Le Time-Sensitive Networking s'appuie sur un ensemble de normes spécifiées par les groupes de travail IEEE 802.1 et 802.3 ; certaines récemment publiées récemment et d'autres, encore en préparation. Elles stipulent la nécessité de disposer d'une base de temps partagée par tous les appareils reliés à un réseau TSN. Cette compréhension communément admise du temps est indispensable pour transmettre des données de façon déterministe le long d'une trajectoire planifiée à l'avance, en respectant un délai connu (latence) avec une variation faible (jitter).

Pour cela, les réseaux TSN s'appuient sur une méthode appelée : accès multiple à répartition dans le temps (Time Division Multiple Access ou TDMA). Les intervalles de temps de ces cycles sont réservés aux flux de données prioritaires afin qu'ils soient protégés des autres types de transmissions. En d'autres termes, une réservation crée un circuit virtuel entre deux ou plusieurs terminaux via l'infrastructure TSN. Pour s'assurer que chaque périphérique respecte les intervalles de temps attendus, les horloges internes de tous les périphériques doivent être synchronisées en s'appuyant sur le protocole normalisé IEEE 1588, appelé Precision Time Protocol (PTP).

DE NOUVEAUX POINTS D'ENTRÉE POUR LES CYBER-AGRESSIONS

Bien connues, les attaques par déni de service (DoS) consistent à inonder un réseau avec de grandes quantités de requêtes jusqu'à ce qu'il soit incapable de remplir sa fonction. La technologie TSN s'appuyant sur des horloges synchrones, le protocole PTP ainsi que le mécanisme TDMA deviennent de nouveaux vecteurs d'agression. Il suffit par exemple, de cibler un seul et même intervalle de temps réservé, pour perturber un flux de communication critique.

En plus de la surcharge de certains créneaux horaires, le protocole PTP peut lui-même devenir une cible. Par exemple, il est possible de détourner la fonction du serveur-

Dr. Oliver Kleineberg, Manager Advance Development

maître délivrant les données de synchronisation, en utilisant des paquets PTP falsifiés. Un faux serveur pourrait ainsi envoyer des spécifications de latence suffisamment élevées pour qu'elles sabotent la synchronisation des intervalles de cycles sur les terminaux soumis au TSN.

LES MÉCANISMES DE LA SÉCURITÉ

Pour l'essentiel, les solutions de sécurité habituelles comme les pare-feux, restent des dispositifs incontournables pour sécuriser une infrastructure TSN. Les propriétés temps réel ont cependant, une influence sur l'approche de certaines mesures de sécurité. Par exemple, les paquets de données traversant un pare-feu DPI (Deep Packet Inspection) ne peuvent être inspectés en temps réel puisque son logiciel doit vérifier la charge utile transmise. Si ce délai n'est pas pris en compte lorsque des cycles sont réservés, les paquets risquent d'être retardés jusqu'à dépasser leur temps de latence maximal. Une première solution consiste à utiliser des pare-feux supportant un mécanisme déterministe compatible avec les exigences de la technologie TSN. Une autre possibilité passe par la prise en compte du retard d'acheminement afin que la planification TDMA soit ajustée lors de la réservation d'un cycle.

Cette transparence au niveau des délais s'applique également aux commutateurs (switchs) qui assurent les mécanismes de sécurité au niveau matériel, comme les listes de contrôle d'accès (Access Control List ou ACL) et le filtrage des paquets sans état. Même si ces mécanismes fonctionnent habituellement à vitesse filaire, le faible retard qui est introduit dans l'acheminement des flux déterministes, peut perturber les réseaux TSN, où les transmissions reposent sur une précision de l'ordre de la microseconde, voire moins. Si de tels mécanismes sont nécessaires à la sécurité, Il est indispensable que leur influence soit prise en compte dans les calculs de latence et d'ordonnancement du TSN.

Dr. René Hummen, Senior Researcher, Future Technologies

Dans tous les cas, il faut tenir compte des exigences en termes de latence et de temps de cycles des applications. Si certains types d'inspection induisent un retard acceptable à l'intérieur même du réseau TSN, d'autres ne pourront être déployés qu'à ses extrémités de contact avec les autres zones de communication, avec lesquelles les retards de délivrance des paquets seront tolérables. Il est donc nécessaire d'identifier les zones au sein desquelles des performances déterministes sont primordiales par l'importante dépendance qu'entretiennent les équipements connectés entre eux.

On peut en conclure que la sécurité peut être assurée par des pare-feux DPI aux interconnexions entre les différentes zones de communication, tandis que des filtres de paquets ACL peuvent assurer la sécurité à l'intérieur des zones régies par le TSN.

LA SÉCURITÉ JUSQU'À LA COUCHE 2 DU MODÈLE OSI

L'un de ces mécanismes, encore en cours d'élaboration dans le cadre la normalisation de la technologie TSN, est appelé Ingress Filtering and Policing (IEEE 802.1Qci). Il permet de vérifier si les trames de données ainsi que leur temps de réception correspondent à un flux de données réservé. Dans la négative, le paquet est rejeté avant qu'il n'impacte négativement le fonctionnement du réseau. De plus, des mécanismes tels que MACsec (Media Access Control Security) peuvent être utilisés pour authentifier, chiffrer et protéger l'intégrité des différents flux entre les équipements du réseau.

Là encore, la latence introduite par l'accomplissement de ces opérations de contrôle doit être prise en compte mais c'est un très faible prix à consentir pour disposer d'une infrastructure de communication déterministe ayant l'avantage d'être totalement indépendante de tel ou tel constructeur ou éditeur de logiciel.

Informations issues d'un document publié par le Dr. René Hummen et le Dr. Oliver Kleineberg de la société Belden. ▬