CetraC, une approche nouvelle de la cybersécurité des réseaux embarqués

La cybersécurité, ou plus particulièrement le risque cyber, s'est imposée aujourd'hui comme un risque majeur, qu'il s'agisse des états, des administrations, des entreprises, ou même des personnes physiques. Le hacker a remplacé Mandrin. À la veille de l'ouverture du FIC, le Forum international de la Cybersécurité à Lille, il nous a semblé intéressant de vous présenter l'approche que CetraC avait de la cybersécurité des réseaux embarqués.

En effet, à l'heure où l'on parle d'autonomie, de haut débit embarqué, de cyber défense, le risque d'attaque à l'endroit des réseaux de données embarqué dans les véhicules est considérable. Il est considérable certes, mais surtout en augmentation forte. Pour ne citer que deux exemples, on peut évoquer la tentation de prendre le contrôle, voire de voler, des véhicules autonomes. On peut également envisager le risque terroriste : pourquoi tenter de détourner un avion en envahissant le cockpit si l'on peut faire dérailler un train à l'aide de la wifi du bord ?

Toutefois, nous voyons 3 différences majeures dans la défense cyber des réseaux embarqués par rapport à celle des réseaux communs.

La première est d'ordre organisationnel : il est difficile d'embarquer en permanence dans un train, un avion ou une automobile un RSSI. Les stratégies de défense qui consistent à monitorer le réseau se heurtent donc à une question d'ordre philosophique : qui pour monitorer le monitoring ?

La deuxième différence est topologique : la plupart des véhicules, qu'il s'agisse de navires de commerce, de train ou d'avions de transport, embarquent des passagers. Ceux-ci doivent avoir accès au réseau, ou du moins un réseau qui leur est dédié. Or, par définition, il n'est pas possible d'empêcher un hacker de monter dans un train ou dans un paquebot.

La troisième dernière différence est d'ordre architectural. Une défense habituelle, c'est d'ailleurs la plus forte, consiste à ségréguer les réseaux Or, en embarqué on veut justement les mutualiser. On veut les mutualiser pour un gain de place, pour un gain de temps, et, tout simplement parce que cela coûte cher de les installer.

Nous nous trouvons donc face à une menace, non plus de l'extérieur, mais également de l'intérieur ; menace à laquelle il n'est pas possible d'interdire l'accès au réseau. Il est donc fondamental de contraindre chaque utilisateur dudit réseau à rester dans la partie de ce dernier qui lui est réservée (réseau invités ou passagers par exemple). Malheureusement l'absence de RSSI interdit de vérifier que cela se passe comme on le souhaite et la mutualisation nécessaire des réseaux rend l'existence de passerelles, d'un domaine à un autre, incontournable.

C'est ici qu'intervient CetraC. Nous fournissons les nœuds du réseau - en français les commutateurs. Notre technologie est 100% hardware – nos produits ne contiennent pas, contrairement à ce qui se fait quasi-systématiquement, de logiciel, le firmware, cible favorite des assaillants. Ainsi le risque de modification du comportement du commutateur par un processus malin - un virus – se trouve réduit à zéro. Nous garantissons donc ces commutateurs afin qu'ils soient utilisés comme des nœuds de confiance. Par ailleurs, nous ségrégons réellement les données qui passent sur un même câble Ethernet ou une même fibre optique. Pour faire simple, elles sont transportées par les mêmes routes mais ne se croisent jamais. CetraC interdit ainsi à l'intrus de se promener où il le souhaite sur le réseau et d'accéder aux parties sensibles.

CetraC permettant également de chiffrer les données, et assurant de nombreuses fonctions de sûreté de fonctionnement (redondance, déterminisme...) nous proposons la technologie qui accompagne la révolution Ethernet des réseaux embarqués de données.

CetraC, par l'architecture, ferme donc les vulnérabilités que l'on avait été contraint, par cette même architecture, d'ouvrir.