Systèmes de contrôle industriel embarqués : le point sur la sécurité

David Kleidermacher
Responsable Technologies de Green Hills Software

Stuxnet, probablement le logiciel malveillant (malware) le plus perfectionné qu'ait connu le monde informatique – et sans nul doute le plus sophistiqué qui se soit jamais attaqué directement à des systèmes de contrôle industriel embarqués – a sensibilisé considérablement les concepteurs de systèmes embarqués aux problèmes de sécurité. La question est : que faut-il faire ? Partagés entre la nécessité d'améliorer la sécurité et les pressions du marché visant à augmenter la productivité, les développeurs ont tendance à faire l'impasse sur la sécurité, exception faite des contrôles rendus obligatoires par les réglementations. Il faut inverser cette situation si l'on veut faire obstacle aux malware de type Stuxnet ou à pire. Il faut appliquer une surveillance réglementaire ciblée aux systèmes de contrôle embarqués stratégiques et à leur chaîne logistique. Il faut former les développeurs à la sécurité embarquée sous mandat de leur direction. Enfin, nous devons adopter un tout nouveau système d'assurance de sécurité pour protéger les composants les plus essentiels des systèmes de sûreté industriels.

Le MP944, considéré par beaucoup comme le premier microprocesseur du monde, a dirigé le système de commandes de vol de l'avion de combat à réaction du F-14 Tomcat de la Marine américaine ; il se situe à l'origine de plus de quarante années de progrès accomplis par les technologies des systèmes embarqués. Selon l'analyste pressenti, les ordinateurs embarqués représentent entre 94 et 98 % des ordinateurs mondiaux. Pratiquement toutes les grandes multinationales – des sociétés comme EADS, Exxon, Tata, Hewlett Packard et Johnson & Johnson – intègrent et misent tout sur les systèmes embarqués au cœur de leurs principaux produits. Et, bien entendu, le consommateur ne pourrait se passer des robustes applications embarquées équipant les avions, automobiles, équipements médicaux et systèmes de contrôle industriel.

Parallèlement, la complexité des logiciels, la connectivité réseau et les menaces d'attaques malveillantes continuent de croître dans ces systèmes embarqués essentiels. Le réseau électrique intelligent (smart grid) – avec ses terminaux et capteurs intelligents, ses compteurs intelligents et ses passerelles de réseaux (tous étant des systèmes embarqués) – en est un bon exemple, mais ce n'est qu'un parmi d'autres.

La complexité des systèmes embarqués

L'un des premiers systèmes embarqués à avoir équipé une automobile a été l'ordinateur de bord de la Cadillac Séville 1978, commandé par un microprocesseur Motorola 6802 à 128 octets de RAM et deux kilo-octets de ROM. Le code source imprimé ne dépasse pas quelques pages.

En comparaison, même l'automobile la plus bas de gamme contient aujourd'hui dix processeurs ou plus et on compte jusqu'à 200 microprocesseurs dans les modèles haut de gamme. Si on ajoute à cela les systèmes d'infoloisirs tournant sous des systèmes d'exploitation tels Microsoft Windows et Linux, le contenu total d'un logiciel embarqué peut facilement dépasser 100 millions de lignes de code. L'avionique de l'avion de combat F-35 Joint Strike Fighter est estimée contenir à peu près six millions de lignes de code, utilisées par les commandes électriques de vol, les

fonctions complexes de connaissance de la situation, la logique des capteurs et les affichages graphiques à haute résolution guidant le pilote. Les commutateurs et routeurs des réseaux d'entreprise contiennent d'ordinaire des millions de lignes de code pour le traitement des protocoles réseau, la gestion et la configuration, la limitation des taux d'anti-virus et les contrôles d'accès.

En bref, la complexité résulte d'une demande inexorable vers plus de capacités, la numérisation des fonctions manuelles et mécaniques et les interconnexions au sein de cet univers. Bien que cette prolifération des contenus électroniques ait été bénéfique à la société, elle est aussi en grande partie à l'origine de nos malheurs en termes de sécurité. En fait, bien des problèmes liés à la perte de qualité, à la sûreté et/ou à la sécurité dans les produits électroniques peuvent être attribués à la complexité croissante des logiciels, qui ne peut être gérée efficacement..

La complexité engendre les défaillances et celles-ci, comme les failles dues au débordement des mémoires tampons, peut être exploitée pour violer la sécurité d'un système. La complexité, bien sûr, ne peut se mesurer uniquement à la taille du code. L'augmentation linéaire de celle-ci crée bien plus qu'une augmentation de la complexité globale en raison de la croissance exponentielle des interactions entre les fonctions du code et les différents composants.

Une autre tendance évidente des systèmes embarqués est l'ajout de la connectivité réseau. Historiquement, les systèmes embarqués sont des entités autonomes, immunes aux risques d'Internet. Mais il existe aujourd'hui bien des raisons qui font qu'on les relie actuellement aux réseaux grande distance. La connectivité réseau permet la gestion à distance d'un système embarqué. Les tâches de gestion peuvent intégrer la mise à niveau d'un logiciel pour remédier à une défaillance. A titre d'exemple, les fours domestiques fabriqués par TMIO® permettent à leurs propriétaires de se connecter depuis un téléphone cellulaire ou par Internet pour allumer ou éteindre le four. Voilà que les appareils domestiques se mettent aussi soudain à avoir leurs problèmes de sécurité informatique.

L'automobile en tant qu'infrastructure essentielle

En 2010, General Motors a introduit une fonction permettant aux propriétaires de véhicules d'inhiber le verrouillage et de faire tourner leur moteur depuis n'importe endroit de la planète à partir d'un téléphone intelligent. Cette connexion à distance se superpose au système télématique de GM monté systématiquement sur tous les véhicules GM depuis 2007. Les utilisateurs doivent-ils craindre l'impact de cette connexion sur la sécurité ?

Juste avant l'annonce par GM de cette fonction d'accès à partir d'un téléphone mobile, une équipe de chercheurs universitaires a publié une étude démontrant comment des systèmes vitaux d'un véhicule – freins, papillon des gaz, etc. – pourraient être trafiqués en exploitant les failles des systèmes embarqués de la voiture.[1]

Ces chercheurs ont commandé les freins, le moteur et les verrous des portes d'une automobile via un port de diagnostic. Ils ont appris comment relier le réseau, peu protégé, à ces systèmes vitaux en utilisant les techniques de flou. Ils ont fait preuve de beaucoup de persévérance, pratiquement tous les principaux sous-systèmes fondamentaux de l'automobile ont été identifiés, assimilés puis totalement infiltrés.

[1] Koscher, Karl, et al. Experimental Analysis of a Modern Automobile. Symposium on Security and Privacy, IEEE 2010.

Les freins et le moteur ont été désactivés en marche, montrant dans quels périls extrêmes pourraient se trouver les passagers en cas d'attaque. L'article résultant de cette étude est excellent, et il est à recommander à tous les professionnels et à tous les passionnés de la sécurité embarquée.

Relier l'automobile aux réseaux cellulaire ouvre en effet une voie royale aux attaques à distance. On peut se demander pourquoi quelqu'un voudrait attaquer le réseau interne d'une automobile. Cela revient au même que se demander pourquoi quelqu'un voudrait s'attaquer au réseau électrique intelligent. Quelle meilleure façon d'engendrer une énorme catastrophe que de désactiver en même temps les freins de millions de véhicules ? L'automobile en réseau représente la menace la plus récente pour les infrastructures essentielles à laquelle sont confrontées les économies actuelles.

Cette étude démontre que nous avons des millions de véhicules vulnérables actuellement sur les routes. Nous savons maintenant que des assaillants disposeraient de moyens assez sophistiqués pour couper les freins de votre voiture alors que vous foncez sur l'autoroute. Les chercheurs à l'origine de cette étude précisent que « dans notre voiture, nous avons identifié pas moins de cinq catégories d'interfaces radio numériques recevant des entrées de l'extérieur, certaines à courte distance et d'autres sur des distances indéfinies. L'un dans l'autre, le contrôle électronique omniprésent, les réseaux internes distribués et les interfaces télématiques se regroupent de plus en plus jusqu'à former une même plate-forme d'application logicielle qui est accessible depuis un réseau externe.

Ironie du sort, OnStar – un système de sûreté et de sécurité – peut maintenant être le moyen utilisé pour des attaques distribuées à distance. Les passagers d'un véhicule souhaitent disposer d'Internet à l'intérieur et d'applications de leurs téléphones intelligents pour contrôler un certain nombre de commodités - mais ils seraient surpris d'apprendre que ces mêmes interfaces peuvent être reliées au train de transmission du véhicule. Les constructeurs automobiles n'avaient peut-être pas ce type de sécurité en tête quand ils ont conçu les modèles qui existent actuellement, mais il est évident qu'ils doivent prendre le train en marche. Il leur faut collaborer étroitement avec les spécialistes de la sécurité embarquée, au départ de chaque projet et avant de concevoir l'architecture de l'électronique de bord et du réseau interne d'un véhicule.

Rôle prépondérant des systèmes embarqués dans les infrastructures essentielles

Le réseau électrique intelligent implique d'ajouter des connexions à distance entre des millions de foyers et des réseaux dorsaux commandant la génération et la distribution d'électricité. Ces systèmes dorsaux sont protégés par les mêmes technologies de sécurité (pare-feu, authentification des accès en réseau, détection d'intrusion et systèmes de protection) qui défendent aujourd'hui les banques et les gouvernements contre les attaques véhiculées par Internet. Pourtant des intrusions dans ces systèmes se produisent couramment et atteignent leur but. La capacité à contrôler la distribution d'électricité représente évidemment des risques pour la sûreté, et l'impact potentiel sur une importante partie de la population augmente l'attrait de la cible. Le réseau électrique intelligent, si son architecture n'est pas étudiée correctement du point de vue de la sécurité, peut offrir aux états des nations hostiles une voie d'attaque toute tracée, sans même que les assaillants aient à quitter le confort de leurs salles à manger. Chaque système embarqué se trouvant sur le parcours – depuis le terminal intelligent jusqu'aux concentrateurs de réseaux – doit être sécurisé. Les services publics et leurs fournisseurs commencent tout juste à

développer la stratégie de sécurité et l'architecture informatique du réseau électrique intelligent, et il existe maintenant une opportunité en or de prévoir la sécurité dès le départ.

Des assaillants sophistiqués

L'utilisation accrue des systèmes embarqués dans le commerce, les infrastructures critiques et les fonctions essentielles à la vie humaine font qu'ils intéressent également des assaillants bien déterminés et pleins de ressources. Les systèmes de contrôle industriel embarqués gérant les réacteurs nucléaires, les raffineries de pétrole et autres infrastructures essentielles représentent une opportunité pour qui voudrait infliger des dommages à grande ampleur.

Le ver Stuxnet est certainement le premier logiciel malveillant à viser directement les systèmes embarqués de contrôle de processus et il démontre l'incroyable potentiel de sophistication des attaques contre la sécurité des systèmes embarqués. Stuxnet a infiltré les systèmes de contrôle de processus de Siemens au niveau de centrales nucléaires par l'intermédiaire des postes de travail Windows utilisés par les opérateurs pour configurer et surveiller l'électronique de contrôle embarquée. La plupart des interrogations soulevées par Stuxnet parmi les spécialistes de la sécurité ont porté autant sur l'identité des assaillants et sur leurs motifs que sur le niveau de sophistication sans précédent de l'attaque, laquelle a utilisé une structure de systèmes furtifs intelligents et exploité pas moins de quatre failles de jour zéro dans Windows. Ce sont ces failles qui ont permis à Stuxnet d'accéder au contrôleur Siemens lui-même et d'y télécharger le logiciel malveillant, ce qui implique que les assaillants avaient une connaissance intime du logiciel et du matériel embarqués dans le contrôleur.

Stuxnet montre également l'interdépendance qui existe souvent entre les systèmes embarqués et les systèmes de TI. Les réseaux de supervision (SCADA) sont contrôlés par de banals PC. En réponse à Stuxnet, le responsable de la Cyber Commande au Ministère de la Défense américain a recommandé la création d'un réseau isolé pour les infrastructures essentielles[2]. Ceci peut paraître une approche bien radicale, mais c'est précisément ainsi que bien des gouvernements protègent leurs réseaux classifiés, compartimentés, les plus sensibles. Cet isolement physique entraîne une perte de rendement qui peut être corrigée par l'utilisation de solutions d'accès à haut niveau d'assurance autorisant un ordinateur client à accéder en toute sécurité à de multiples postes de travail virtuels et réseaux dorsaux isolés. Ces systèmes de contrôle d'accès utilisent les plus récentes et les meilleures des interfaces homme-machine Windows ou Linux mais ne dépendent pas de ces dernières pour leur sécurité.

Stuxnet démontre le besoin de meilleures réglementations gouvernementales en matière de sécurité dans les systèmes embarqués industriels essentiels, et le fait que ces réglementations doivent stipuler un niveau d'assurance plus élevé que les pratiques commerciales standard de la Technologie de l'Information (TI). L'un des principaux dogmes touchant à la sécurité informatique est qu'il est difficile, peu sage, et souvent financièrement et/ou techniquement inenvisageable, d'adapter une fonction de sécurité à un système qui n'a pas été conçu à la base pour celle-ci.

Le seul exemple moderne de certification de sécurité à haut niveau d'assurance d'un logiciel se trouve dans les systèmes d'exploitation embarqués sécurisés gérant des informations classifiées et cruciales pour la mission. Par exemple, le microyau

[2]http://www.nytimes.com/2010/09/24/us/24cyber.html

INTEGRITY de Green Hills Software a été conçu pour le niveau d'assurance EAL 7, et c'est la première technologie de logiciel à être ainsi certifiée selon un haut niveau d'assurance en vertu des Common Criteria (figure 1). Ce certificat lui a été alloué sous les auspices d'un programme du gouvernement américain destiné à protéger les informations sensibles à bord de l'avion de combat F-35 Joint Strike Fighter.



National Information Assurance Partnership

Common Criteria Certificate

Common Criteria

is awarded to

Green Hills Software, Inc.

Note: This evaluation contains results that are not mutually recognized in accordance with the provisions of the CCRA: only the evaluation results of EAL4 components are mutually recognized.

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3) ISO/IEC 15408. This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: INTEGRITY-178B Separation Kernel
Evaluation Platform: INTEGRITY-178B Real Time Operating System (RTOS), version IN-ICR750-0101-GH01_Rel running on Compact PCI card, version CPN 944-2021-021 w/PowerPC, version 750CXe
Assurance Level: EAL6+, High Robustness

CCTL: Science Applications International Corporation
Validation Report Number: CCEVS-VR-VID10119-2008
Date Issued: 01 September 2008
Protection Profile: US Government Protection Profile for Separation Kernels in Environments Requiring High Robustness, Version 1.03, 29 June 2007

Original Signed By
Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By
Information Assurance Director
National Security Agency

Figure 1 – Certificat de sécurité à haute robustesse

Les conditions à remplir sont un processus très rigoureux de conception, développement et test, la validation continue des circuits touchant à la sécurité en cours d'exécution, des mécanismes sécuritaires de mise à jour et distribution, et des méthodes formelles pour prouver mathématiquement les politiques de sécurité du système. La norme exige de résister à un test de pénétration par les pirates informatiques de haut vol de la National Security Agency américaine qui ont accès au code source. Ce niveau de sécurité est destiné tout spécialement à protéger les ressources vitales contre des assaillants sophistiqués et déterminés.

Les enjeux et les menaces sont les mêmes pour les infrastructures essentielles, ainsi que l'a illustré l'attaque de Stuxnet sur les centrales nucléaires. Tous les logiciels des systèmes de contrôle industriel ne sont pas tenus de respecter ces critères rigoureux, mais seulement les composants chargés d'isoler les fonctions essentielles du reste du système. Cette base de traitement de toute confiance comprend le système d'exploitation et un petit nombre de composants essentiels comme un module d'authentification cryptographique qui empêche tout accès non autorisé aux fonctions de contrôle à sécurité critique..

Confrontés à un environnement réglementaire plus rigoureux et au risque accentué pour la vie humaine et la santé d'une entreprise, les développeurs des systèmes embarqués doivent apprendre à penser « sécurité » tout comme ils pensent actuellement « fonctionnalités », « capacité mémoire » ou « déboguage ». Le besoin de créer des systèmes embarqués sécurisés doit infiltrer tous les niveaux de l'organisation. La formation des développeurs doit comprendre des publications sur la sécurité, la participation à des conférences techniques avec travaux sur la sécurité, le guidage des principaux fournisseurs du matériel et du logiciel d'un projet, et l'exposition régulière aux événements d'actualité. La direction doit comprendre les enjeux de la sécurité embarquée et être acquise à la nécessité de cette formation. Ce point de vue sur la sécurité doit être partagé par les différents responsables des composants individuels, de l'intégration de ces composants, ainsi que du succès du

produit total. En fait, doivent être conscients des enjeux de la sécurité embarquée les vice-présidents, directeurs généraux et cadres des entreprises créant des systèmes de contrôle industriel essentiels, et ils doivent prévoir des architectures et des applications à haut niveau d'assurance partout où c'est indispensable.

Stuxnet est un signal d'alarme aux personnes impliquées dans le développement, la gestion, le déploiement et la chaîne logistique des systèmes embarqués industriels essentiels. La bonne nouvelle est que les normes à haut niveau d'assurance auxquelles doivent aspirer les développeurs existent déjà et ont fait leurs preuves pour les composants logiciels importants comme pour les systèmes définitifs. Nous devons simplement copier le succès de cette formule en l'appliquant à davantage de logiciels, de projets et de secteurs impliqués dans la protection des ressources vitales contre des assaillants déterminés et pleins de ressources cherchant à les détruire.