www.silicon.fr

Date : 21/08/2014

Aurélien Francillon, Eurecom : « une même faille peut toucher de multiples systèmes embarqués »

Par : Reynald Fléchaux

La première étude à grande échelle sur la sécurité des firmwares dans l'embarqué (routeurs, caméras IP, set top boxes…) a permis de cerner toute l'étendue du problème. Un de ses auteurs, issu de l'école **Eurecom**, commente pour Silicon.fr les principales conclusions de ces travaux.

Après la publication de leur étude remarquée sur la sécurité des firmwares, une équipe de recherche d'**Eurecom**, une école d'ingénieurs en télécommunications située à Sophia Antipolis, présentait hier les résultats de ses travaux dans le cadre de Usenix, une conférence sur la sécurité des systèmes d'information qui se tient en ce moment à San Diego. L'étude menée par deux professeurs assistants d'**Eurecom** (Davide Balzarotti et Aurélien Francillon) et deux doctorants (Andrei Costin et Jonas Zaddach) se base sur l'analyse de 26 000 packages logiciels renfermant des firmwares destinés à des systèmes embarqués. Elle montre qu'une grande proportion d'entre eux renferme des vulnérabilités relativement simples à débusquer. Et que ces dernières se retrouvent couramment d'un firmware à l'autre, des constructeurs différents intégrant parfois les mêmes sous-systèmes conçus par des sous-traitants.

Quelques heures avant la présentation de ladite étude sur la scène de Usenix, nous nous sommes entretenus avec Aurélien Francillon.

Silicon.fr : D'où est venue l'idée de mener une étude quantitative sur la sécurité des firmwares embarqués ?

Aurélien Francillon : La sécurité des systèmes embarqués est mon sujet de travail depuis des années. L'idée de cette étude est née d'un double constat : le nombre de systèmes embarqués en exploitation a explosé ces dernières années que d'un constat ; et si de nombreux exploits ont mis en lumière le manque de sécurité des firmwares, cela reste des cas individuels issus d'analyses manuelles. Or ces dernières présentent deux inconvénients : elles sont coûteuses et elles ne passent pas à l'échelle. D'où la méthode que nous avons employée consistant à collecter un grand nombre de packages logiciels pour mener une étude à grande échelle. L'un des intérêts de cette démarche réside dans le fait qu'elle permet de mettre en évidence des relations jusqu'alors inconnues entre des systèmes. Par exemple, certaines cartes SD disposant d'une connexion WiFi comportaient une faille connue au niveau du serveur Web embarqué. Par comparaison, via le calcul d'un indice de similitude entre les fichiers issus des firmwares, on a retrouvé cette même faille dans les systèmes d'un autre fabricant, systèmes pourtant basés sur une architecture différente.

De nouveau, votre étude souligne la présence de failles résultant de négligences ou d'erreurs pourtant bien connues, comme des backdoor officiellement présentes pour des opérations de maintenance ou de tests (lire par exemple des affaires récentes de ce type ici ou ici)…

Notre étude se base en effet sur des classes de vulnérabilité connues. Et, parmi celles-ci, les failles de type mots de passe stockés en dur, présence de ports ou de comptes de débogage ou accès à des clefs publiques de connexions à distance SSH représentaient un tiers des cas.

Si on se place du point de vue de l'assaillant, votre étude montre également qu'industrialiser des attaques contre les systèmes embarqués est tout à fait envisageable…

Oui, c'est vrai même si ce n'était pas du tout l'optique de notre étude. Par ailleurs, la faisabilité de ce type d'attaques a déjà été démontrée en 2012, avec ce qu'on a appelé l'Internet census (un botnet de 420 000 machines infectées, essentiellement des routeurs mal protégés, NDLR).

Comment pourrait-on améliorer la situation assez déplorable que dépeint votre étude ?

La première étape consiste à bien connaître ladite situation et l'analyse à grande échelle des vulnérabilités des firmwares y participe. Après, c'est avant tout une question économique, et non technique. La sécurité coûte cher. Il faut sensibiliser les utilisateurs, les habituer à payer plus pour des systèmes sécurisés. Or, aujourd'hui, surtout dans le grand public, la prime est donnée aux constructeurs qui proposent rapidement des nouveautés, offrent des produits riches fonctionnellement et à bas prix. Trois impératifs qui vont à rebours d'une amélioration de la sécurité. L'existence de standards, d'une certaine forme de régulation pourrait aider. Par exemple, les critères communs dans le domaine de la carte à puce obligent les fabricants à mener un certain nombre de tests.

Si on se réfère aux systèmes d'information classiques, l'embarqué ne souffre-t-il pas également d'un manque d'organisation dans la gestion des patch de sécurité ?

Aujourd'hui, cette structure n'existe tout simplement pas, les utilisateurs n'ayant souvent à leur disposition aucun moyen centralisé d'effectuer des mises à jour de sécurité. Dans le peu de cas où celles-ci existent, les utilisateurs ne sont généralement pas au courant de leur sortie et leur application n'est en tout cas pas automatique. Ironiquement, des systèmes de mises à jour automatiques existent pour certaines set top boxes ou télévisions, mais l'objectif consiste plutôt à amener de nouvelles fonctionnalités.

Votre étude intègre des firmwares de tous types, provenant d'acteurs de toutes tailles. Avez-vous observé des différences entre de petits acteurs positionnés sur une niche par exemple et des géants mondiaux comme Siemens, Xerox ou Samsung ?

Nous n'avons pas étudié cet aspect en particulier, mais aucune corrélation entre la taille des fabricants et la présence ou non de vulnérabilités ne semble se dégager. Nombre de très grandes entreprises réutilisent des éléments venus d'ailleurs ou revendent des sous-systèmes, voire des systèmes entiers, provenant de sous-traitants. Sur un modèle de caméra IP, nous avons ainsi récupéré les clefs RSA publique et privé. Via Zmap (un scanner de ports TCP), nous avons pu retrouver 32 000 caméras connectées à Internet utilisant le même couple de clefs, des caméras émanant de fabricants différents. En réalité, ces matériels sont totalement identiques ; seule la marque change.

Quelles sont les prochaines étapes de vos travaux ?

Nous travaillons à réaliser des analyses plus poussées pour identifier des vulnérabilités moins évidentes dans les firmwares. Par ailleurs, nous souhaitons perfectionner le site Web que nous avons mis en ligne en parallèle de la publication de l'étude. Pour l'instant, ce service permet de désassembler des packages logiciels. Nous allons y ajouter la publication de rapports d'analyses basées sur des corrélations et la recherche de failles simples.