

Cyber-sécurité automobile : la porte d'accès cellulaire

Par Francois Ortolan de chez Anritsu

Les véhicules récents introduisent de nouvelles technologies connectées visant à offrir des avantages tels que du divertissement multimédia, de nouvelles fonctionnalités de sécurité routières ou encore un rendement énergétique accru. Face à l'explosion des voitures connectées, les inquiétudes en matière de sécurité se multiplient. Ces dernières années les démonstrations de piratage comme la prise de contrôle à distance d'une Jeep en 2015 ou d'un tesla en 2016, ont prouvé que la connectivité cellulaire engendre une grande vulnérabilité des véhicules, pouvant dans certains cas mettre des vies en danger. Les voitures connectées sont la fusion entre deux mondes, celui des télécoms et celui de l'automobile. Ces mondes ayant des cycles de production et de vie très différent, les constructeurs automobiles doivent repenser leur approche traditionnelle d'une unique validation pré-commercialisation de la sécurité. La cyber-sécurité est une discipline qui nécessite une réévaluation constante des systèmes embarqué tout au long du leur cycle de vie.



Figure 1 : Exemple de prise de contrôle à distance d'une voiture (Source : Laboratoire Kaspersky [1].)

Mais comment font donc les cybercriminels pour briser les sécurités des véhicules sur un réseau cellulaire, et comment est-il possible de prévenir ces attaques à l'aide de techniques de tests de cyber-sécurité ayant fait leurs preuves ?

Les réseaux sans-fils : la voie dématérialisée

L'une des méthodes de piratage automobile les plus dangereuses consiste à pénétrer son *système télématique* à l'aide d'interfaces de communication sans fil comme le Bluetooth, le Wi-Fi ou le réseau de téléphonie mobile, dit « cellulaire ». Les systèmes télématiques sont la porte d'entrée du véhicule; ce sont des systèmes critiques car ils ne nécessitent aucune connexion physique pour accéder au véhicule. Les risques les plus importants sont ceux qui touchent aux données personnelles du conducteur, facilement accessibles et partageables. Malgré les efforts des constructeurs automobiles pour isoler les systèmes télématiques et d'info-loisirs du réseau interne critique du véhicule (bus CAN/Flex-ray/Ethernet), il existe toujours un risque potentiel que les pirates trouvent un moyen d'y pénétrer, y compris en prenant le contrôle total du véhicule. Le « bus » est le réseau interne du véhicule, qui relie tous les composants les plus importants du véhicule (moteur, transmission, capteurs et presque tous les équipements embarqués).

Les intégrateurs de systèmes tels que les équipementiers ou fabricants de systèmes télématiques s'en remettent trop souvent aux fournisseurs de systèmes d'exploitation pour garantir la sécurité de leur système. Cependant, quand une faille majeure est découverte dans le système d'exploitation public principal, il faut plusieurs mois pour qu'un correctif soit publié, tandis que la mise à jour se fait à distance via une technologie OTA (Over the Air). Les vulnérabilités sont souvent dévoilées à la communauté pour attirer l'attention des utilisateurs sur les risques existants, mais ces informations peuvent également être utilisées par les hackers, pour exploiter ces mêmes failles.

Considérations lors de la conception

Le meilleur moyen de prévenir ces attaques est de les prendre en compte lors de la conception. Lors de la première étape de conception d'un système, il est important de s'intéresser aux failles connues et aux recommandations de sécurité afin de les prendre en compte dans les spécifications du système. Un exemple représentatif est le protocole de communication TLS/SSL, le protocole sécurisé le plus utilisé, qui est constamment piraté, en raison de sa popularité [1]. Le protocole TLS/SSL est donc régulièrement mis à jour pour corriger ses failles de sécurité. Les systèmes utilisant ce protocole devront donc suivre de près son évolution et être mis à jour régulièrement.

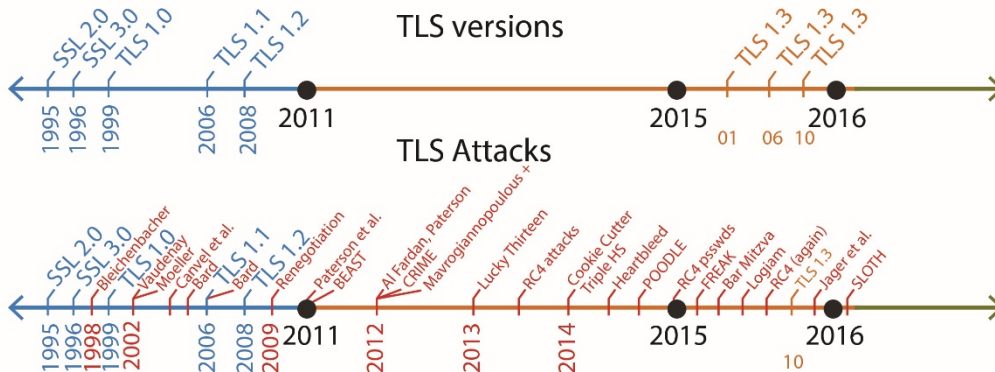


Figure 2 (Haut) Version TLS/SSL – (Bas) Failles successives

Une fois le système conçu en respectant les spécifications de sécurité, le prototype doit ensuite passer par une phase d'essais de sécurité pratique.

Vérification des points d'entrée

Les systèmes télématiques embarquent souvent des connectivités à faible portée (BT/Wi-Fi), qui constituent un accès facile grâce à des points d'accès conventionnels prêts à l'emploi, ce qui les rend plus accessibles aux pirates, mais également plus facile à tester, de manière générale. Concernant la connectivité à longue portée, appelée « cellulaire » ou « mobile », comme la 2G, 3G ou le LTE, elle s'avère plus difficile d'accès et plus complexe à vérifier, car les réseaux utilisés sont gérés par leurs opérateurs locaux.

Les risques concernant la technologie cellulaire sont alors habituellement évalués sur des réseaux de téléphonie mobile, en conditions réelles de fonctionnement. À cause de leurs différentes configurations inconnues (par exemple : ouverture de ports, filtrage, routage, etc.), la vérification en conditions réelles n'est pas une évaluation complète car elle n'offre pas une visibilité totale des failles. Une validation avec un opérateur donné ne donne pas l'assurance que ne pas se retrouver face à une faille avec un autre opérateur.

En outre, le principal inconvénient des analyses de risques en cyber-sécurité est le temps passé, et potentiellement perdu, à résoudre des problèmes qui en réalité n'en sont pas. En particulier, les « concordances faussement positives » sont le cauchemar de toutes les analyses de sécurité. Il est donc primordial de choisir le bon outil et de bien identifier les objectifs en matière de cyber-sécurité.

La validation de la cyber-sécurité avec un simulateur de réseau cellulaire

Une nouvelle approche permet de démultiplier les capacités de test pour les réseaux cellulaires : les simulateurs de réseaux cellulaires. Grâce à leur architecture ouverte, ils permettent de connecter le véhicule à un réseau contrôlé pour déjouer un certain nombre de risques potentiels qui couvrent la diversité des configurations des opérateurs réseaux. La vérification peut être automatisée et répétée dans des conditions identiques après chaque nouvelle mise à jour du logiciel de la voiture, afin de s'assurer que les failles sont identifiées et corrigées.

L'utilisation d'un simulateur de réseau tel que le MD8475A d'Anritsu est idéal car il est doté d'une interface graphique simple qui permet à l'ingénieur de configurer plusieurs cellules avec des technologies cellulaire, y compris celles qui ne sont pas nécessairement accessibles dans votre région (2G/3G/LTE-A/TD-SCDMA/EV-Do).

Les tests pratiques couvrent un certain nombre de techniques. En connectant les serveurs de test directement aux simulateurs pour accéder aux appareils via le réseau cellulaire, les types de vérifications suivants peuvent être effectués.

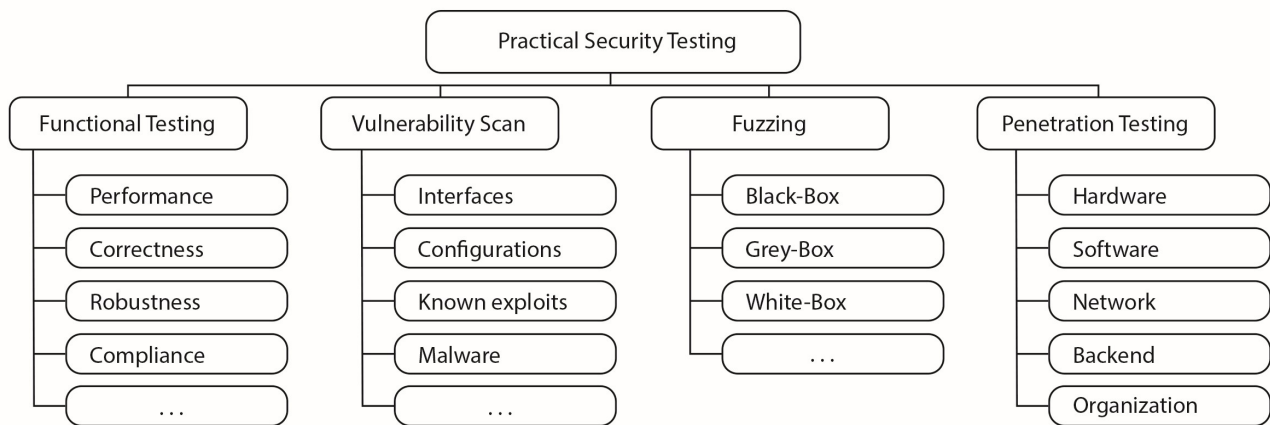


Figure 3 : Tests pratiques de sécurité



Figure 4 : Utilisation de serveurs de tests avec logiciel avec des simulateurs de réseaux

Tests fonctionnels de sécurité

Les tests fonctionnels vérifient toutes les fonctions liées à la sécurité qui se trouvent dans le système de test, en s'assurant de leur bon comportement et de leur robustesse. Cette étape est similaire à un test fonctionnel général mais se concentre sur les fonctionnalités de sécurité. Elle valide les spécifications de conception et permet de mesurer les performances du système.

L'exemple récent de piratage d'un véhicule Jeep a montré qu'un port laissé ouvert (le port 6667) a conduit à la possibilité de prise de contrôle des fonctions vitales de la voiture : direction, freins, phares, verrouillage des portes, ainsi que la mise à zéro du compteur de vitesse et du compte-tours, arrêt du moteur et débrayage de la transmission afin de rendre inefficace la pédale d'accélérateur. Une simple analyse des ports aurait suffi pour prévenir cette prise de contrôle, à l'aide d'un outil tel que Nmap/Zenmap[4] pendant le test de fonctionnalité.

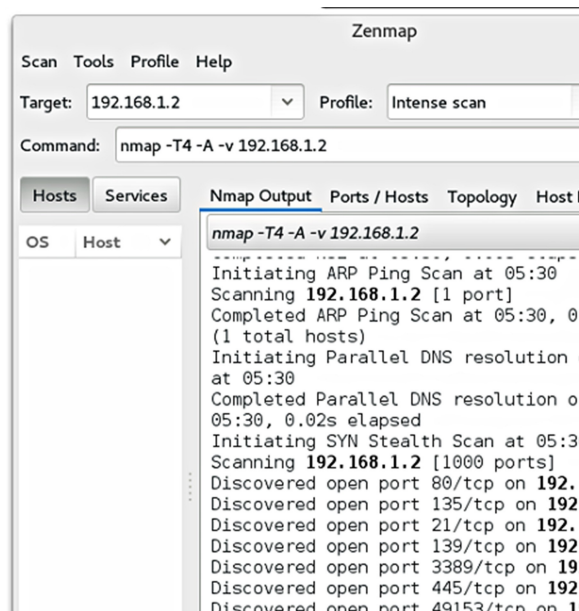


Figure 5 : Analyse des ports à l'aide de nmap/zenmap

Certains opérateurs réseaux ferment dorénavant ce port pour des raisons de sécurité, car de nombreux chevaux de Troyes utilisent ce port pour pénétrer les systèmes [3]. En utilisant un simulateur de réseau pour la vérification, avec l'ensemble des ports ouverts, on est assuré de tester l'ensemble du système.

Recherche de vulnérabilités

La recherche de vulnérabilité consiste à une vérification du système pour les failles de sécurités courantes déjà connues. Plusieurs logiciels de sécurité répertorient des configurations et des failles. La qualité de l'analyse des failles est entièrement dépendante d'une mise à jour fréquente de leurs bases de données.

Telsa a récemment publié une mise à jour pour corriger plusieurs vulnérabilités majeures sur son Model S. Le système multimédia de la voiture utilisait en effet un navigateur obsolète qui contenait un WebKit vieux de 4 ans comportant une faille qui pouvait potentiellement permettre à un cybercriminel de hacker la voiture à distance et d'en démarrer ou arrêter le moteur. En théorie, un hacker aurait pu créer une page web hébergeant du contenu malveillant qui lui aurait permis, si quelqu'un entrait sur se faux site web, d'avoir accès au système multimédia du véhicule. [3]

L'un de ces outils populaires de recherche de faille est OpenVAS. Sa base de données est régulièrement mise à jour avec les dernières failles connues. Pour chaque vulnérabilité, il indique son niveau de risque et les méthodes potentielles pour la corriger.

Name	Status	Reports		Severity 
		Total	Last	
Immediate scan of IP 10.101.239.74	Done	1 (1)	Aug 9 2016	6.4 (Medium)
Immediate scan of IP 192.168.1.1	Done	1 (1)	Aug 9 2016	N/A
Immediate scan of IP 192.168.1.2	Done	4 (4)	Aug 10 2016	10.0 (High)

Figure 6 : Vérification typique à l'aide d'OpenVAS sous Linux (distribution Kali 2.0)

L'utilisation d'OpenVAS sur un réseau réel s'avère souvent compliquée car la plupart des tests de fonctionnalité peuvent être bloqués par les pare-feu.

Fuzzing

La technique du « fuzzing » va encore plus loin pour trouver de nouvelles failles, en envoyant systématiquement et de manière aléatoire des données erronées vers le système cible pour vérifier le comportement inconnu et potentiellement critique d'un système.

En utilisant un simulateur de réseau, un ingénieur peut créer de nombreux protocoles de fuzzing. Grâce à son interface contrôlable, il est également possible de reproduire le comportement anormal d'un réseau cellulaire, comme « rejeter » ou « ignorer ».

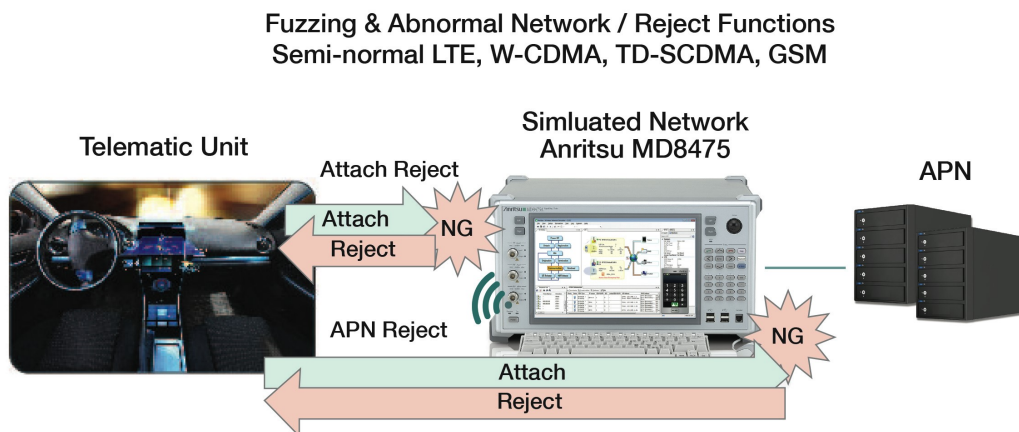


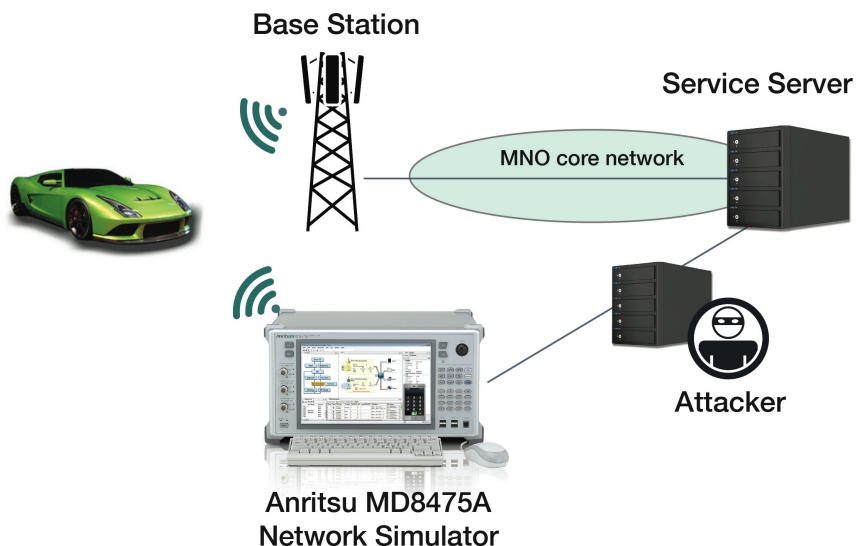
Figure 7 : Test typique du rejet de la connexion ou de l'APN

Là encore, la technique du fuzzing s'avère compliquée sur un réseau réel, car le réseau ne peut pas se permettre de se comporter de manière anormale.

Tests de pénétration

Le test pénétration vise à vérifier la sécurité de l'ensemble du système, sur le plan logiciel et matériel. Un « testeur humain intelligent » essaie d'exploiter toutes les failles découvertes lors des étapes précédentes, de manière « sophistiquée », basée sur de nombreuses années d'expérience du hacking, dans le but de changer le comportement du système cible.

Les simulateurs de réseau sont appréciés par les « hackers bien intentionnés » pour leur flexibilité et leurs capacités de traçage avancées à l'aide d'outils comme Wireshark. Le traçage des paquets de données n'est en général pas possible sur un réseau cellulaire, car le flux de données passe directement dans le réseau fermé de l'opérateur. En revanche, un simulateur de réseau permet d'effectuer des simulations d'attaques d'interception (ou « Man-In-The-Middle » en anglais). Le simulateur peut lire les paquets qui passent via son interface et éventuellement les modifier. Cette technique peut être utilisée pour forger de fausses informations afin de potentiellement accéder aux véhicules.



De manière générale, les opérateurs réseau sont considérés comme fiables, quoique de récents événements ont montré qu'ils peuvent être hackés ou que des gouvernements peuvent y avoir accès, grâce à des « interceptions légales ». L'exemple le plus récent est le cas du gouvernement iranien, qui a compromis la validation par SMS du célèbre service de chat Telegram [5].

Normes et recommandations

À l'heure actuelle, il n'existe aucune certification claire pour l'industrie automobile, il n'existe que des recommandations. Or, une norme générale de certification de sécurité, garantissant certains niveaux de sécurité pour les systèmes automobiles, s'avèrerait particulièrement utile. Une telle norme serait toutefois sans doute assez difficile à mettre en place, à cause de la nature changeante des risques de sécurité.

Certaines organisations ont fait des efforts pour rédiger un ensemble de règles générales à suivre lors de la conception traditionnelle de systèmes automobiles et de l'intégration et des phases de test des voitures.

La SAE (*Society of Automotive Engineers*) a publié ses premières recommandations officielles (SAE J3061™) incluant la cyber-sécurité dans le processus existant d'analyses liées aux niveaux d'intégrité de sécurité automobile (ASIL, *Automotive Safety Integrity Level*) [6]. Elles décrivent une méthodologie à suivre pour l'analyse des menaces et l'évaluation des risques.

Cette initiative constitue un bon cadre de référence pour l'industrie, pour qui la cyber-sécurité ne constitue pas un socle de connaissances traditionnel. La voiture connectée présente un défi au long cycle de développement traditionnel pour intégrer les technologies de l'information et de la communication. Toute faille de sécurité peut mener à incriminer différents fournisseurs, c'est pourquoi il est primordial de repenser la chaîne d'approvisionnement pour prendre en compte la cyber-sécurité.

Conclusion

Pour conclure sur ce chapitre de la cyber-sécurité, il n'est pas inutile de rappeler que le moyen le plus courant utilisé par les hackers est l'erreur humaine. Les chevaux de Troyes installés de manière non intentionnelle par l'utilisateur reste le principal risque d'attaque. L'attaque par « ingénierie sociale » constitue une autre méthode en plein essor ; elle consiste à utiliser des techniques de hameçonnage (« phishing ») pour inciter l'utilisateur à fournir lui même son mot de passe. Constituant de loin le type d'attaque le plus efficace, seule l'éducation à la sécurité peut réellement permettre d'éviter ce type de comportement en sensibilisant le public aux problèmes de sécurité.

[1]<https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/>

[2][Connected and Autonomous Vehicles workshop -Secure communication in autonomous vehicles](#), Professor Cas Cremers (University of Oxford)

[3] <https://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/>

[3]<http://www.speedguide.net/port.php?port=6667>

[4]<https://nmap.org/zenmap/>

[5]<https://www.wired.com/2016/08/hack-brief-hackers-breach-ultra-secure-messaging-app-telegram-iran/>

[6]<https://interact.gsa.gov/sites/default/files/J3061%20JP%20presentation.pdf>

[7]<https://www.anritsu.com/en-GB/test-measurement/products/md8475a>

