Failles Sécu

Transcription

Épisode 15 : Voiture autonome : Sure en toute circonstance ?

Léa : Bonjour à toutes et à tous et bienvenue à bord de ce 15ème épisode de Failles Sécu, l'émission qui vulgarise la sécurité informatique pour rendre votre vie cyber plus sûre et vous protéger des pirates. Je suis Léa, la pilote de cette émission, et aujourd'hui je demande à tous de bien attacher votre ceinture de sécurité car nous allons parler automobile dans cet épisode intitulé « Voiture autonome : Sûre en toute circonstance ? ». **[JINGLE]**
Et c'est bien sûr Toi, Charlie, qui m'accompagne, et qui comme à chaque épisode, décortique et rend intelligible les sujets les plus complexes! Salut Charlie, salut mon Amie, alors ça va ?

Charlie : Ça va très bien, je te remercie ! Ravie de te retrouver pour ce dernier épisode de l'année 2025, consacré effectivement à un problème qui touche les voitures autonomes, comme certaines Tesla.

L : Quel genre de problème ?

C : Et bien un grave problème. En effet, il s'avère que dans certaines conditions comme la nuit, les voitures autonomes peuvent ne pas reconnaître des obstacles et leur foncer dedans.

L : C'est purement théorique ?

C : Malheureusement non, l'agence de Sécurité Routière américaine la NHTSA déplorait dans son rapport de 2022, 16 accidents impliquant des Tesla, modèles X, Y, S et 3, vendues entre 2014 et 2022.

L : Donc ça concerne seulement les anciennes Tesla ?

C : Difficile à dire, mais apparemment, comme on va le voir, c'est la technologie utilisée qui est en cause et les chercheurs qui ont découvert ce problème ont publié leur article il y a 6 mois. Par conséquent, ils ont alerté Tesla pendant leur étude et Tesla a probablement effectué des changements. Mais on n'en sait rien au juste.

L : OK, mais que s'est-il passé exactement dans ces accidents dont tu parles ?

C : Et bien ces accidents impliquent presque toujours les mêmes acteurs et actrices : une Tesla en mode conduite autonome qui fonce dans un véhicule de secours se trouvant tous gyrophares allumés au milieu de la route, le tout se déroulant en pleine nuit. Un reportage du Wall Street Journal résume bien le scénario récurent grâce à une vidéo d'un accident qu'ils ont pu étudier en détails.

L : Ah oui car les Tesla filment en continu ce qu'il se passe et l'enregistre, un peu comme la boîte noire dans un avion. Tu veux qu'on la passe en direct ?

C : Bonne idée, il n'y a pas de son, mais je vais la décrire en accélérant certains passages. Hop, c'est parti. Donc la vidéo commence sur une autoroute américaine, dans le Texas, à minuit 54, en hiver 2021. La caméra piéton d'un policier filme la scène alors que celui-ci porte secours à un véhicule arrêté sur la bande d'arrêt d'urgence. En même temps, la caméra de bord d'une Tesla X de

2019 filme le trajet qu'emprunte son propriétaire alcoolisé à partir de minuit 30. Ce conducteur saoul zigzague un peu, si bien qu'après 4 minutes de route il enclenche l'Autopilot alors qu'il roule à 100 km/h. Les capteurs embarqués dans la voiture détectent qu'il n'a pas les mains sur le volant, et la voiture lui demande donc à 150 reprises de mettre les mains sur le volant pour montrer qu'il est bien attentif. Le conducteur coopère 150 fois en 45 minutes, ce qui convainc l'Autopilot de poursuivre le voyage. Au bout de 45 minutes cependant, des véhicules d'urgence font leur apparition sur la bande d'arrêt d'urgence. Il est alors 1h13 du matin. L'Autopilot ne ralentit pas car les véhicules d'urgence ne se trouvent pas sur sa voie. On voit alors apparaître à quelques centaines de mètres le véhicule du policier du début qui barre la voie. En tant qu'humain, on le voit car ça clignote de partout. Mais la caméra de l'Autopilot est perturbée par ces clignotements. Tant et si bien que la Tesla continue à filer bon train alors que l'obstacle se rapproche. C'est à seulement 30 mètres du véhicule de secours bloquant la voie qu'elle détecte cet obstacle et panique. Dans l'affolement l'Autopilot se désactive et 2 secondes plus tard c'est la collision à 90 km/h avec le véhicule de secours. 5 policiers sont blessés, tout comme le conducteur de la voiture qui avait déclenché l'arrivée des secours initialement.

L : Ah oui, c'est comme si l'Autopilot n'avait pas compris la dangerosité de la situation. Et d'après le Wall Street Journal c'est arrivé au moins 16 fois car le reportage date de 2022. Il y a pourtant un radar en plus des caméras pour détecter les objets.

C : C'est exact, mais sur ce modèle de 2019 le radar est utilisé pour détecter les véhicules en mouvement. Il n'est pas utilisé pour détecter les obstacles immobiles qui sont alors gérés par les caméras. Sinon le moindre pont, panneau de signalisation, ou tout autre objet renvoyant l'écho radar aurait fait piler la voiture.

L : Ah oui et puis Tesla fait reposer son système Autopilot principalement sur les caméras.

C : Exactement, c'est leur mantra : « Priorité aux caméras ». Et c'est pourquoi des chercheurs de l'Université Ben Gurion du Negev en Israël ont justement étudié les différents systèmes d'aide à la conduite qu'on trouve sur Internet, ainsi que la vidéo issue de la caméra frontale d'une Tesla modèle 3 de 2023, qu'ils ont récupérée par USB au format vidéo standard.

L : Attends, on trouve des systèmes d'aide à la conduite en vente légalement sur Internet ?

C : Oui ce sont des sortes de caméras intelligentes qui se placent sur le pare-brise et qui peuvent te fournir des alertes en cas de danger. Elles n'ont bien sûr aucun contrôle ni sur le volant ni sur les pédales. Tu ne transformes pas ta Twingo en Tesla autonome pour 99€ !

L : Ah ah OK. Et qu'ont-ils fait ensuite avec ces caméras ?

C : Eh bien, ils se sont remis dans les conditions des accidents. Et en lisant attentivement les rapports détaillés des accidents publiés par la Sécurité Routière Américaine, ils ont trouvé des facteurs communs à tous ces accidents : à chaque fois, une Tesla avec l'Autopilot enclenché, circule la nuit et rencontre sur son chemin un véhicule de secours tous gyrophares allumés.

Ils ont donc placé une voiture sous un abris pour simuler la nuit, lui ont adjoint un gyrophare clignotant qu'ils ont trouvé en ligne, et ils ont filmé la scène avec les caméras qu'ils avaient à leur disposition. Ensuite ils ont envoyé ces vidéos dans un logiciel de reconnaissance d'objet tel YOLO.

L : Et qu'ont-ils découvert ?

C : Ce qu'ils ont découvert est édifiant. Lorsque la lumière du gyrophare est éteinte, le logiciel de reconnaissance d'objet détecte la voiture de manière quasi certaine. Par contre, dès que le gyrophare s'illumine, le logiciel n'est plus si sûr que ça de la présence de la voiture de secours. Si bien que l'objet passe sous le seuil de détection et n'est donc plus considéré comme une voiture au milieu de la route, mais comme quelque chose d'inexistant. Par conséquent, avec ces éléments en main, l'Autopilot voit la voiture puis la perd à cause du clignotement du gyrophare. Et cette mauvaise détection est exacerbée par les reflets parasites qui se produisent à l'intérieur de la lentille de la caméra.

L : Et c'est probablement ce qu'il s'est produit dans les accidents relatés dans le rapport. Par contre, je ne comprends pas pourquoi ça n'arrive pas plus souvent, car les lumières clignotantes sont fréquentes sur la route, notamment quand tu croises une autre voiture phares allumés. Par conséquent les reflets parasites, la caméra doit en voir souvent sur la route, la nuit.

C : Tu as raison, mais les gyrophares des secours sont particuliers : ils clignotent rapidement contrairement aux phares d'une voiture que tu croises. Et ils alternent rouge / bleu, contrairement aux phares qui éclairent blanc ou jaune. Et les gyrophares sont placés en hauteur. Par conséquent la caméra est non seulement éblouie, mais comme en outre son logiciel de reconnaissance d'objet fait à base de réseaux neuronaux n'a pas été entraîné sur des voitures éclairées en rouge ou bleu, il détecte tout sauf une voiture. Imagine qu'on te montre une photo complètement surexposée, avec du bleu ou du rouge et du flou partout, et qu'on te demande de décrire la scène. Tu auras bien du mal à reconnaître les vrais objets, car ça évoque chez Toi d'autres objets. Et bien pour le logiciel de reconnaissance d'objet, c'est pareil, il est perdu.

L : C'est ce qu'on voit dans la vidéo du Wall Street Journal du début, l'Autopilot se désactive car il ne comprend plus rien. Donc on comprend bien le problème de sécurité routière que ça pose, qui plus est pour les premiers secours. Attends je te vois gesticuler… Ce n'est pas tout ?

C : Et bien non, car si ça pose un problème évident pour la sécurité routière, ça pose aussi une menace plus large. Car cette vulnérabilité, si l'on peut la nommer ainsi, pourrait être exploitée à des fins malveillantes. Par exemple, un acteur malintentionné pourrait installer une lumière particulière à un endroit stratégique comme à un croisement très fréquenté par exemple, et provoquer un accident ou viser particulièrement un véhicule.

L : Euh, là quand même c'est un peu tiré par les cheveux.

C : Aujourd'hui ça parait de la science-fiction, mais demain ? Souviens-toi de l'attaque par martèlement de mémoire (Row Hammer en anglais). Cette attaque consistait à accéder plein de fois d'affilé au même contenu d'une mémoire vive, pour faire changer le contenu voisin. Ça a été d'abord décrit en laboratoire, puis des pirates s'en sont emparés pour voler des clés secrètes sur des serveurs.

L : Ok je vois, il est plus sûr de s'en protéger dès maintenant. Et les chercheurs proposent une solution ?

C : Oui ils en décrivent une qui permet d'augmenter la confiance du système d'aide à la conduite dans ces conditions précises sans altérer son fonctionnement en condition normale.

L : Ouah passionnant ! Merci Charlie pour cet … éclairage ! Tu veux ajouter quelque chose ? Il nous reste quelques minutes.

C : Et bien volontiers ! Mi octobre, donc il y a un peu plus d'un mois, une enquête issue d'un consortium de journalistes internationaux a montré comment on pouvait tous être localisés, à n'importe quel moment, à la demande de n'importe qui dans le monde, et sans être infecté par le moindre espiongiciel.

L : Beh, on le sait déjà, les opérateurs téléphoniques nous géolocalisent en permanence, c'est inhérent au fonctionnement des réseaux mobiles.

C : Je suis d'accord avec Toi, mais tu as manqué une information cruciale dans mon propos qui est que tu peux être géolocalisée par N'IMPORTE QUI dans le monde. Et c'est arrivé à des militants qui ont pu être intimidés, et c'est aussi arrivé à des personnes qui ont été liquidées.

L : Donc tu veux dire que si je suis un dissident russe en exil par exemple, si le KGB connaît mon numéro, alors il peut me retrouver en passant par un service spécial, même si j'ai un vieux téléphone sans connexion internet ?

C : Oui c'est ça. Et ce service dénommé Altamides existe depuis près de 20 ans. Il a été créé par un ancien ingénieur de chez Siemens, et opère depuis l'Indonésie. Il utilise un système de signalisation téléphonique antédiluvien qui regroupe plusieurs protocoles.

On appelle ce système « SS7 » pour système de signalisation numéro 7 et il permet aux opérateurs d'échanger des informations techniques indispensables, par exemple pour savoir dans quelle zone se trouve un mobile ou pour router un appel.

C'est l'opérateur mobile qui le gère, donc ça n'arrive jamais sur ton téléphone, c'est pour cette raison qu'il n'y a rien à pirater chez la cible. Par contre, pour l'exploiter, il faut avoir accès à l'infrastructure d'un opérateur mobile pour envoyer des messages SS7, grâce à l'obtention d'une adresse globale appelée GT. Comme ce n'est pas sécurisé, n'importe quel GT autorisé, peut demander au GT de n'importe quel autre réseau dans le monde de localiser plus ou moins précisément un numéro de téléphone.

L : Qu'est ce qui cause ces approximations dans la localisation ?

C : Oh, bonne question. En fait la précision de la géolocalisation dépend de la densité de relais téléphoniques présents autour du numéro ciblé. À la campagne, tu as moins d'antennes mobiles qu'en ville, donc tu auras probablement une précision plus faible dans la position de ta cible. Mais les pirates peuvent utiliser des méthodes plus avancées pour améliorer cette précision. Et c'est certainement ce qu'est capable de faire Altamides puisque l'appli a permis des éliminations précises d'opposants.

L : Mais comment font les pirates ou les sociétés d'espionnage comme celle qui commercialise Altamides pour avoir une adresse globale ou GT et envoyer ses messages SS7, c'est accessible à tout le monde ?

C : Excellent point ! Les sociétés d'espionnage vont tout simplement acheter le droit d'envoyer des messages de signalisation auprès d'un opérateur téléphonique peu regardant. Longtemps la société First Wap qui commercialise le logiciel Altamides a payé l'opérateur national du Liechtenstein pour pouvoir envoyer ces signaux.

L : Ah oui, quand même ! Des messages des signalisation envoyés depuis le cœur de l'Europe pour espionner le monde entier. Et personne ne s'est aperçu de la supercherie ?

C : Et oui, car c'était une utilisation contractuellement légitime et légale du SS7. C'est seulement quand des journalistes sont tombés sur une immense base de données regroupant des millions de lignes obscures et qu'ils l'ont analysée, que l'opérateur télécom du Liechtenstein a mis fin au contrat le liant à First Wap.

L : Je reste un peu sans voix ! Tout ceux qui disent « oui moi j'utilise un vieux Nokia 33 machin, car au moins on ne peut pas me géolocaliser », et bien ils se mettent le doigt dans l'œil. Ça me rappelle les explosions des Pagers au Liban en 2024. Je ne sais pas si les services secrets Israëliens ont utilisé cette méthode à base de messages SS7 pour avoir la position de leurs cibles, mais ça serait techniquement plausible.

Encore un génial épisode, merci Charlie.

C : C'est toujours un plaisir pour moi Léa. En plus, on n'a pas eu à apprendre de nouvelles voix cette fois, donc c'est allé super vite pour enregistrer l'épisode !

L : Ouaiiis ça fait 2 émissions qu'on tient, j'espère que ça va durer ! Et je rappelle l'adresse pour nous dire quelles voix nous imitons : « failles au pluriel sécu tout attaché @ intracherche.fr ». On se retrouve vite Charlie !

C : Avec joie Léa, à la prochaine !**[JINGLE]**