Question

Après avoir brièvement présenté et résumé le(s) document(s), vous répondrez à la question :
Est-il possible de créer des systèmes embarqués sans aucune faille ? Que faudrait-il alors faire pour prévenir les conséquences de telles failles ?

Questions préparatoires

Ces questions ne sont là que pour vous aider à comprendre le document. Leurs réponses n'apparaitront pas forcément dans la réponse à la question principale.

1. Décrire le fonctionnement normal de la serrure connectée, et de la voiture.
2. Décrire, dans les deux cas, ce que pourrait faire une personne mal intentionnée.
3. Donner des avantages et inconvénients de ces objets connectés.
4. Comment est-il possible de faire en sorte d'éviter ces conséquences négatives avec des objets connecté ?

Barème

⚠ **Avertissements** ⚠ Votre note ne pourra pas être supérieure à la moyenne :
- si votre podcast n'est que la liste des réponses aux questions préparatoires ;
- si votre texte de présentation est la transcription de votre podcast.

Texte de présentation (... / 4)	**Prestation** (... / 6)
Titre Vous avez proposé un titre, court, clair, et percutant. **Forme** Vous avez rendu une courte présentation, en français correct, sans (trop) de fautes d'orthographe. **Fond** Elle présente correctement le podcast, pour donner envie de l'écouter. **Bibliographie** Elle est présente, et les références sont assez précises pour pouvoir retrouver le document d'origine.	**Pertinence** Le contenu est pertinent et intéressant. Il n'y a pas hors sujet, et la question a sa réponse. **Vulgarisation** Le contenu est suffisamment vulgarisé pour que les auditeurs et auditrices ne connaissant ni le sujet ni le document le comprenne. **Plan** Le contenu est structuré. **Bibliographie** Vous citez le ou les documents présentés. **Crédits** Vous citez tous les membres du groupes (même celles et ceux que ne parlent pas), en respectant le nom ou pseudonyme choisi.

SNT > INFORMATIQUE EMBARQUÉE > ENJEUX PIRATES

Question

Après avoir brièvement présenté et résumé le(s) document(s), vous répondrez à la question :
Est-il possible de créer des systèmes embarqués sans aucune faille ? Que faudrait-il alors faire pour prévenir les conséquences de telles failles ?

Questions préparatoires

Ces questions ne sont là que pour vous aider à comprendre le document. Leurs réponses n'apparaitront pas forcément dans la réponse à la question principale.

1. Décrire le fonctionnement normal de la serrure connectée, et de la voiture.
2. Décrire, dans les deux cas, ce que pourrait faire une personne mal intentionnée.
3. Donner des avantages et inconvénients de ces objets connectés.
4. Comment est-il possible de faire en sorte d'éviter ces conséquences négatives avec des objets connecté ?

Barème

⚠ **Avertissements** ⚠ Votre note ne pourra pas être supérieure à la moyenne :
- si votre podcast n'est que la liste des réponses aux questions préparatoires ;
- si votre texte de présentation est la transcription de votre podcast.

Texte de présentation (... / 4)	**Prestation** (... / 6)
Titre Vous avez proposé un titre, court, clair, et percutant. **Forme** Vous avez rendu une courte présentation, en français correct, sans (trop) de fautes d'orthographe. **Fond** Elle présente correctement le podcast, pour donner envie de l'écouter. **Bibliographie** Elle est présente, et les références sont assez précises pour pouvoir retrouver le document d'origine.	**Pertinence** Le contenu est pertinent et intéressant. Il n'y a pas hors sujet, et la question a sa réponse. **Vulgarisation** Le contenu est suffisamment vulgarisé pour que les auditeurs et auditrices ne connaissant ni le sujet ni le document le comprenne. **Plan** Le contenu est structuré. **Bibliographie** Vous citez le ou les documents présentés. **Crédits** Vous citez tous les membres du groupes (même celles et ceux que ne parlent pas), en respectant le nom ou pseudonyme choisi.

Gilbert Kallenborn, 01net.com, *Le protocole Z-Wave met votre maison connectée à la portée des pirates*, 28 mai 2018.

https://www.01net.com/actualites/le-protocole-z-wave-met-votre-maison-connectee-a-la-portee-des-pirates-1457870.html

Si vous utilisez des serrures interconnectées au travers d'une passerelle sans fil Z-Wave, vous ne devriez pas être rassurés. Il s'avère en effet que cette technologie [...] est vulnérable à une attaque par rétrocompatibilité baptisée « Z-Shave » permettant de prendre le contrôle de tous les appareils connectés à la même passerelle Z-Wave.

Il suffirait d'être à proximité pour, par exemple, envoyer une commande d'ouverture à une serrure connectée et pénétrer dans l'habitation. Pour rappel, Z-Wave est une technologie maillée et décentralisée, largement utilisée dans les produits domotiques. L'usage de passerelles n'est pas obligatoire. Il permet, toutefois, d'ouvrir l'accès au réseau Z-Wave au monde extérieur (Internet).

Andy Greenberg, WIRED, traduit par Louis Paternault, *The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse*, 8 janvier 2016.

https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

Il y a presque exactement un an, Chrysler a rappelé 1,4 millions de véhicules après que deux hackers aient montré à WIRED qu'ils pouvaient prendre le contrôle du système informatique de la Jeep à distance, par internet.

[...]

L'an passé, [les chercheurs en cybersécurité Valasek et Miller] ont pris le contrôle d'une voiture à distance, et l'ont arrêtée sur la route nationale I-64 — pendant que je la conduisais. [...] Ils sont maintenant capables de réussir des tours encore plus inédits et dangereux, comme provoquer des accélérations non prévues, écraser les freins ou tourner le volant à n'importe quelle vitesse. « Imaginez que l'an passé, au lieu de couper la transmission sur la nationale, nous ayons tourné le volant à 180 degrés » demande Chris Valasek. J'imagine bien. Mais il précise quand même : « Vous ne seriez pas au téléphone avec nous en ce moment. Vous seriez mort. »

[...]

Et ne vous trompez pas, disent les hackers de voiture : d'autres méthodes sans fil d'attaque de voitures seront trouvée, tôt ou tard.

« Il y aura presque certainement d'autres vulnérabilités à distance dans le futur », dit Karl Koscher, un chercheur à l'université de Californie, à San Diego [...].

Comme ces scientifiques, Miller et Valasek ne cherchent pas à créer de chaos sur la route, mais à aider à créer de meilleurs protections avant que les attaques informatiques contre les voitures ne deviennent une vraie menace. [...] Les fabricants de voiture devraient aussi considérer que les pirates informatique finiront par trouver une brèche à distance, et construire des systèmes qui réduisent les conséquences désastreuses de telles failles. « Il faut savoir ce que les pirates vont faire ensuite, comment s'en protéger, et que certaines protections ne fonctionneront pas, comme nous l'avons montré » dit Miller.

Dans un article qui devrait être publié au moment de leur conférence Black Hat, Miller et Valasek recommandent aux constructeurs d'aller plus loin pour éviter le genre de manipulations qu'ils ont mises en évidence. Par exemple, ils suggèrent que les constructeurs n'autorisent pas certains tests potentiellement dangereux à moins qu'un interrupteur physique ne soit actionné par le garagiste.

Snt > Informatique embarquée > Enjeux Pirates

Gilbert Kallenborn, 01net.com, *Le protocole Z-Wave met votre maison connectée à la portée des pirates*, 28 mai 2018.

https://www.01net.com/actualites/le-protocole-z-wave-met-votre-maison-connectee-a-la-portee-des-pirates-1457870.html

Si vous utilisez des serrures interconnectées au travers d'une passerelle sans fil Z-Wave, vous ne devriez pas être rassurés. Il s'avère en effet que cette technologie [...] est vulnérable à une attaque par rétrocompatibilité baptisée « Z-Shave » permettant de prendre le contrôle de tous les appareils connectés à la même passerelle Z-Wave.

Il suffirait d'être à proximité pour, par exemple, envoyer une commande d'ouverture à une serrure connectée et pénétrer dans l'habitation. Pour rappel, Z-Wave est une technologie maillée et décentralisée, largement utilisée dans les produits domotiques. L'usage de passerelles n'est pas obligatoire. Il permet, toutefois, d'ouvrir l'accès au réseau Z-Wave au monde extérieur (Internet).

Andy Greenberg, WIRED, traduit par Louis Paternault, *The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse*, 8 janvier 2016.

https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

Il y a presque exactement un an, Chrysler a rappelé 1,4 millions de véhicules après que deux hackers aient montré à WIRED qu'ils pouvaient prendre le contrôle du système informatique de la Jeep à distance, par internet.

[...]

L'an passé, [les chercheurs en cybersécurité Valasek et Miller] ont pris le contrôle d'une voiture à distance, et l'ont arrêtée sur la route nationale I-64 — pendant que je la conduisais. [...] Ils sont maintenant capables de réussir des tours encore plus inédits et dangereux, comme provoquer des accélérations non prévues, écraser les freins ou tourner le volant à n'importe quelle vitesse. « Imaginez que l'an passé, au lieu de couper la transmission sur la nationale, nous ayons tourné le volant à 180 degrés » demande Chris Valasek. J'imagine bien. Mais il précise quand même : « Vous ne seriez pas au téléphone avec nous en ce moment. Vous seriez mort. »

[...]

Et ne vous trompez pas, disent les hackers de voiture : d'autres méthodes sans fil d'attaque de voitures seront trouvée, tôt ou tard.

« Il y aura presque certainement d'autres vulnérabilités à distance dans le futur », dit Karl Koscher, un chercheur à l'université de Californie, à San Diego [...].

Comme ces scientifiques, Miller et Valasek ne cherchent pas à créer de chaos sur la route, mais à aider à créer de meilleurs protections avant que les attaques informatiques contre les voitures ne deviennent une vraie menace. [...] Les fabricants de voiture devraient aussi considérer que les pirates informatique finiront par trouver une brèche à distance, et construire des systèmes qui réduisent les conséquences désastreuses de telles failles. « Il faut savoir ce que les pirates vont faire ensuite, comment s'en protéger, et que certaines protections ne fonctionneront pas, comme nous l'avons montré » dit Miller.

Dans un article qui devrait être publié au moment de leur conférence Black Hat, Miller et Valasek recommandent aux constructeurs d'aller plus loin pour éviter le genre de manipulations qu'ils ont mises en évidence. Par exemple, ils suggèrent que les constructeurs n'autorisent pas certains tests potentiellement dangereux à moins qu'un interrupteur physique ne soit actionné par le garagiste.