COMO O AUMENTO DA SEGURANÇA PODE AJUDAR O MUNDO AUTOMOTIVO

A indústria automotiva é um grande consumidor de software, quer seja software de gerenciamento de clientes, software de gerenciamento de estoque, software de projeto de peças, etc. A Kompass lista 107 pacotes de software diferentes.

Quanto ao crime cibernético na indústria automotiva, todos, desde Kaspersky até as maiores empresas como Apple, Oracle, EMC Symantec, SAP e CapGemini, estão envolvidos há muito tempo. Basta ler os inúmeros comunicados de imprensa que estão sendo emitidos atualmente. A guerra na Ucrânia poderia ter algo a ver com isso? Abaixo estão trechos de um artigo da Wikipedia que é edificante:

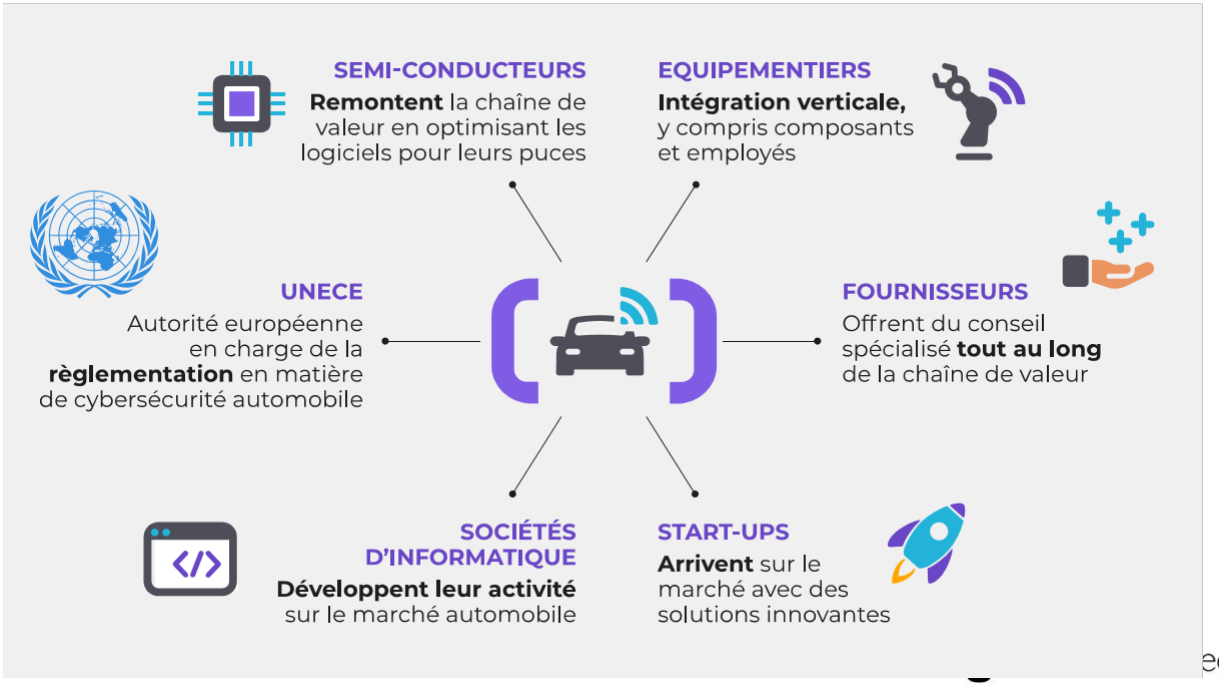
*"**A segurança de TI dos veículos** é uma questão importante nos veículos motorizados modernos. Esta questão é levada em consideração desde a fase de projeto dos sistemas embarcados.*

O veículo conectado é controlado por computadores de bordo (ECUs) interconectados. Através destas ECUs, o veículo moderno oferece novas funcionalidades que melhoram a qualidade da condução e aumentam a segurança dos passageiros. Entretanto, os fabricantes são confrontados com problemas de segurança de TI decorrentes de dispositivos como plugues ODB, Bluetooth, Wi-Fi, 3G/4G, RFID, chaves USB, CDs, que são muito comuns em veículos modernos. Cada um desses dispositivos poderia ser uma porta aberta para os hackers terem acesso aos vários computadores de bordo.

Em 2015, os pesquisadores americanos Chris Valasek e Charlie Miller exploraram a vulnerabilidade do sistema multimídia e assumiram o controle das funções de segurança e conforto (freios, volante, potência do motor, limpadores de pára-brisa) e de entretenimento (volume do rádio do carro). Esta demonstração a partir de um computador externo remoto destaca as deficiências de segurança das aplicações em veículos. Estes dispositivos são responsáveis pela troca de informações entre o veículo e/ou o motorista e o sistema informático do fabricante, bem como pelo processo de autenticação e a criptografia dos códigos de bordo.

Para antecipar e evitar esses ataques cibernéticos, a indústria de veículos conectados e/ou autônomos e fabricantes de equipamentos estão trabalhando cada vez mais com especialistas em segurança para encontrar soluções ou contramedidas. Os desafios econômicos, tecnológicos e sociais são proporcionais a este desafio.

Fonte: The automobile, the latest cybersecurity defication?



ecurity

Todos eles enfatizam arquiteturas proprietárias que protegem as comunicações e processos entre o veículo (de carros a caminhões, ônibus e, claro, veículos militares) e a nuvem e/ou seus sistemas de comunicação proprietários.

Para simplificar, existem três padrões de segurança cibernética

- WP29 U
- UN 155 "Uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system" *Esta é a norma utilizada pela UTAC.*
- ENISA 2019

Estas normas ajudam a tornar os veículos seguros desde o momento em que são construídos até o momento em que são utilizados.
Tanto o comportamento quanto a construção são seguros.

Entretanto, as novas normas que estes parceiros estão implementando não dizem respeito à confirmação do motorista de que seu veículo está conectado à Internet.

Além disso, com exceção de uma, estas normas não são aprovadas pela UTAC[1] que é o laboratório automotivo quase oficial. É a autoridade reconhecida que valida todos os procedimentos e veículos automotivos. Em outras palavras, é bom que o mundo automotivo esteja tornando o ambiente motor/veículo/comunicação seguro, mas este acionamento de segurança não parece levar em conta a importância de envolver o usuário, quem quer que ele seja.

Entretanto, a aplicação destas normas de segurança cibernética não pode ser feita sem o acordo do último elo: o motorista no sentido amplo. Isto corre o risco de criar um mal-entendido de sua parte: "*mais uma vez algo está sendo escondido de nós",* exceto que neste caso não é poluição, mas sim o próprio controle do veículo. E exceto que, em alguns casos, ela está em vigor há 10 anos sem ser anunciada.

Pensemos positivamente: privamos este último elo, o motorista, de uma informação forte: ele está protegido contra agressões externas.

Especialmente porque as leis européias exigem que as interações atendam ao padrão PSD2 "na área de características de segurança, o elemento mais sensível do PSD2 é a generalização da autenticação multi-fator (AMF) para certas transações, incluindo pagamentos on-line.

Parece normal, então, dado o preço desses veículos, que a norma PSD2 se aplique a eles.

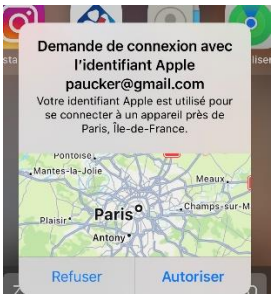
O que esta norma realmente faz? É necessário um segundo acordo de validação a ser solicitado a um comprador (em nosso caso, um motorista). GTCs eletrônicos, por assim dizer. Em outras palavras, é normal proteger um veículo, mas o motorista deve saber disso e concordar com ele. Caso contrário, há o risco de escândalos no estilo VWgate quando jornalistas ou organizações de consumidores tomam consciência da opacidade das práticas dos fabricantes.

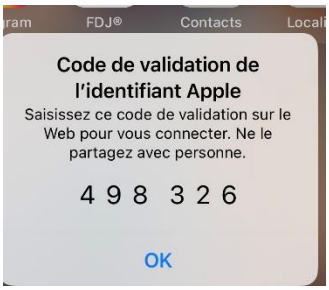
[1] UTAC = **Union technique de l'automobile du motocycle et du cycle**, é uma entidade privada, controlada e financiada principalmente pela indústria automotiva francesa.

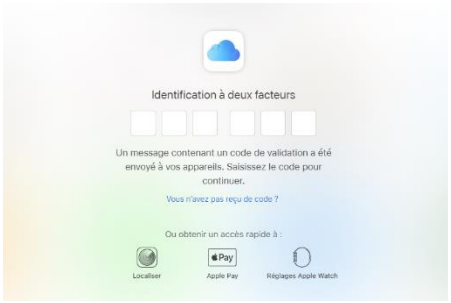
Como funciona a dupla assinatura, em sua maioria

Com relação a este ato de validação, dupla assinatura legal ou forte autenticação, existem proteções postas em prática pelo mercado.

Por exemplo, na Apple você recebe uma mensagem inicial para verificar se é você quem está solicitando a conexão, seguida por um código que você tem que copiar na transação em andamento ou simplesmente abrir um software (photoshop, por exemplo). É um pouco incômodo.







Hoje, a grande maioria desses sistemas funciona através do envio de um código por SMS.

UM SMS é hackeável e a única proteção é que o SMS é válido por menos de 10 minutos, em média. Isto explica o número de transações fracassadas. É necessário fazer malabarismos entre duas janelas do mesmo terminal ou fazer malabarismos com duas telas separadas PC e smartphone. Então este código tem que ser transcrito na própria transação, sem erros, pois o número de caracteres tende a ficar mais longo.

Em geral, os sistemas existentes :

- Correr na nuvem para que não haja controle local
- Fontes dos EUA. Sem controle e sem a certeza de que o sistema é realmente opaco

Em conclusão, a dupla assinatura ou assinatura reforçada, na maioria dos casos, permanece hackeável hoje em dia e é um processo bastante complexo, pois exige a transferência sem erros de todos os códigos únicos e difíceis de lembrar.

O que nos torna únicos

A patente da Segurança Aumentada facilita o acordo sobre o desencadeamento de proteções de segurança cibernética, revertendo o pedido de prova.
Procedimento atual: o fabricante envia um código diferente por SMS cada vez que o motorista tem que reinseri-lo em um teclado

Procedimento de Segurança Aumentada: o motorista só tem que digitar a senha escolhida, que é fácil de lembrar e é implementada no espaço seguro pela Segurança Aumentada.
Este código será sempre o mesmo a cada solicitação, já que a segurança é fornecida pelo ambiente do software e não por um código hacker enviado por um SMSM não seguro.

Um exemplo: o procedimento de Segurança Aumentada pode ser traduzido em uma mensagem exibida em uma das telas do veículo "*Você concorda em estar conectado a nossa segurança cibernética*" seguida por um espaço onde o motorista digitará seu código de 4 a 6 dígitos, conhecido apenas por ele, em um teclado virtual que será exibido. Naturalmente, isto também pode ser usado para ligar o veículo.

Economiza tempo, mas também simplifica os procedimentos para os motoristas. A experiência tem mostrado que quanto mais complexo for o procedimento, maior será a chance de que ele seja contornado.

Em conclusão, a Segurança Aumentada propõe uma interface patenteada entre o veículo e o fabricante que irá desencadear atividades de segurança cibernética com o consentimento do motorista. A
Segurança Aumentada desempenha esta função de forma rápida e muito simples. Tanto quanto sabemos, não há procedimento equivalente:

- Patente Européia
- Possuímos 100% de nosso código, nossas fontes.
- Solução horizontal, em plataforma cruzada
- Integração com as soluções dos fabricantes.
- As assinaturas duplas são 100% seguras, o que não é o caso de muitos procedimentos atuais que utilizam SMS que são "hackable".
- Forte segurança dos terminais utilizados, mas também dos servidores, criando uma continuidade ao longo da cadeia, desde o remetente até o receptor.
-

Em conclusão, a Segurança Aumentada oferece uma verdadeira Autenticação Forte, que dará aos motoristas controle sobre as comunicações de seus veículos, uma característica que será ainda mais desenvolvida.