la Repubblica

del 24.03.2013 da pag. 21 Edizione

Il caso

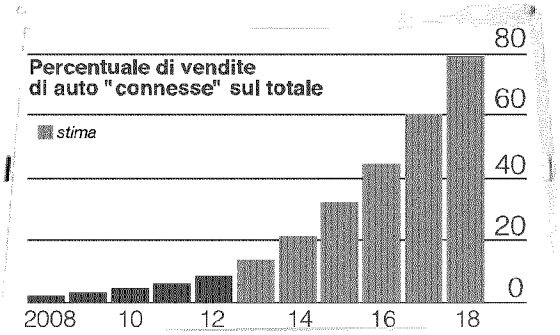
I pirati mettono a rischio la sicurezza. E i produttori corrono ai ripari

Computer di bordo, wi-fi, app così gli hacker entrano in auto

dal nostro corrispondente
ENRICO FRANCESCHINI

LONDRA

AUTO con il navigatore satellitare, auto collegate a Internet in wi-fi, auto che già si guidano da sole con il pilota automatico computerizzato. Belle le quattro ruote dell'era digitale, no? Sì, ma anche esposte a un nuovo rischio: l'hackeraggio al volante.



Computer di bordo, wi-fi e "app" così gli hacker si mettono al volante

Rischio sicurezza. E i produttori corrono ai ripari

DAL NOSTRO CORRISPONDENTE
ENRICO FRANCESCHINI

LONDRA

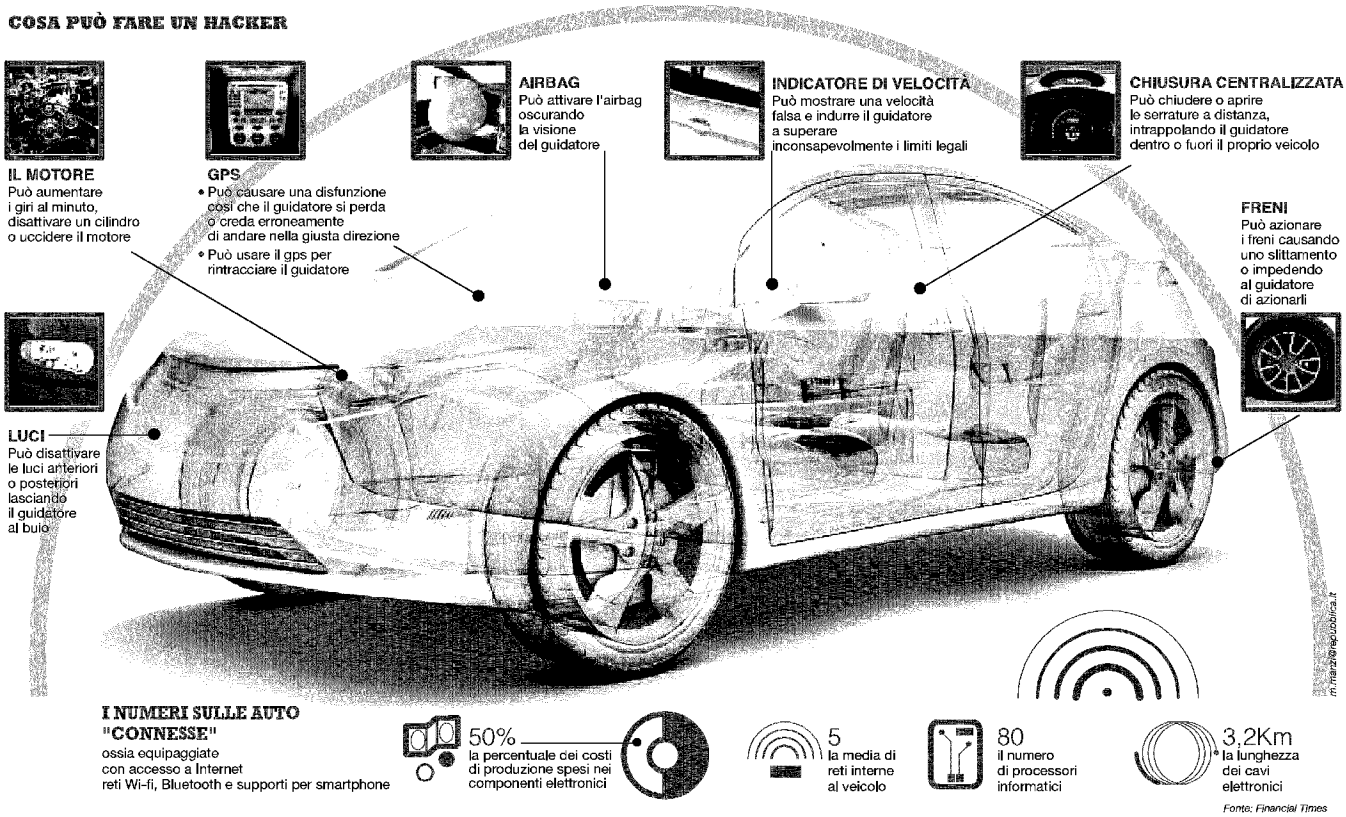
MENTRE il futuro dell'automobile, e anzi il presente, entra a vele spiegate nel web, gli esperti fanno i conti con un pericolo da fantascienza: le incursioni dei pirati on line. Che, come in un film di James Bond, possono entrarti in macchina attraverso la rete e fare di tutto: rubare informazioni, manomettere dati, spegnerti i fari, bloccarti il freno, farti sbagliare strada e perfino chiuderti dentro (o fuori), oltre naturalmente a portarti via il mezzo. Una minaccia che costringe l'industria del settore a correre ai ripari con sofisticati sistemi di protezione anti-hacker. La guerra digitale che si combatte da un pezzo attorno ai pc di casa e di ufficio si allarga insomma a un altro campo di battaglia: l'automobile.

«Le auto sono diventate dei congegni internettizzati», dice Ralf Lamberti, capo del dipartimento telematico della Daimler, al *Financial Times*, che ha dedicato ieri un ampio servizio alla questione, «e dunque dobbiamo proteggere i nostri veicoli dagli attacchi cibernetici». Le automobili moderne sono in pratica un computer in movimento, spiegano gli esperti al quotidiano finanziario, tanto è vero che il software di bordo e le apparecchiature elettroniche rappresentano ormai il 50 per cento delle spese per produrle. Ciascuna è equipaggiata con oltre 3 chilometri di cavi elettronici e digitali. E più aumenta la connettività online, più si moltiplicano le possibilità di intrusione da parte dei pirati informatici. In un test compiuto da ricercatori dell'università di California a San Diego, per esempio, un'auto procede su una strada a 60 chilometri di velocità. Alle sue spalle, dall'interno di un secondo veicolo, un hacker riesce a entrare nei computer della prima vettura, il cui sistema di freni elettronico viene di colpo disattivato. La macchina non è più in grado di fermarsi.

Uno scenario da film di 007, per l'appunto, che diventa realtà quotidiana. E non è l'unico di questo genere. I pirati possono spegnere le luci esterne e interne di un veicolo, facendolo piombare nell'oscurità. Possono incrementarne la velocità o bloccarne il motore. Possono aprire l'airbag, oscurando la visione di guida di chi è al volante. Possono aprire o chiudere le serrature dell'auto. Possono manomettere il navigatore satellitare, fornendogli false informazioni, in maniera che il guidatore segua istruzioni sbagliate, si perda o non arrivi alla destinazione prescelta. O altrimenti possono semplicemente rubargli il percorso designato ed essere in grado di sapere dove andrà, pedinandolo da grande distanza. E non è l'unico furto di informazioni che sono in grado di compiere: possono altresì entrare nei computer, tablet o telefonini all'interno di un'auto e derubarli di informazioni di ogni tipo, da numeri di telefono a carte di credito, da documenti a filmati.

Per difendersi, l'industria automobilistica ha già predisposto dei "firewall", delle pareti digitali che impediscono l'accesso a sollecitazioni esterne. Un altro meccanismo di difesa è separare la rete computerizzata dei sistemi di guida da quella delle comunicazioni e dell'intrattenimento. Ma con l'auto che diventa sempre più computerizzata (Google ha recentemente diffuso il video di una vettura che si guida da sé, e due stati americani, California e Nevada, autorizzano già la circolazione di macchine con pilota automatico), si moltiplicano le opportunità di attacchi cibernetici. Ai pericoli della vecchia autostrada d'asfalto si aggiungono quelli dell'autostrada informatica.

la Repubblica
del 24.03.2013 da pag. 21 Edizione



Sempre più tecnologia sui veicoli: ormai sono come pc viaggianti

In pericolo portiere e centraline. Ma anche airbag e freni possono finire sotto attacco

Il manager

"Ma il futuro sono auto che si controllano con lo smartphone"

VINCENZO BORGOMEO

IL PUNTO d'incontro intelligente tra automobile e Internet è la chiave di tutto. Si apre un mondo di servizi che a breve potrebbero essere gestiti da smartphone. Quali in particolare? «Si va dalle regolazioni della macchina — spiega Doug VanDagens, direttore globale servizi di connettività di Ford — alla gestione degli appuntamenti in officina, all'acquisto di servizi aggiuntivi e molto altro ancora. Le auto possono cambiare prestazioni ad esempio in base a chi le guiderà: madri, figli, padri. La tecnologia già c'è e noi la proponiamo di serie su molti modelli, il passo successivo sarà poter cambiare settaggi in remoto».

Gli attacchi di hacker sono uno scenario possibile?

«Non siano in un film, ma nella realtà. Noi garantiamo ai nostri clienti livelli sempre più elevati di innovazione senza nessun pericolo».

Però voi siete stati il primo costruttore d'auto al mondo a partecipare ad un progetto open source per realizzare informazione e intrattenimento a bordo. Come funziona?

«In pratica abbiamo regalato alla comunità di programmatori il codice sorgente su cui realizzare le applicazioni destinate a smartphone e tablet compatibili con il nostro sistema in auto».

Perché tutto questo?

«Vogliamo solo supportare attivamente chi crea app e affiancare il lavoro di chi guarda alle auto come a un potenziale importante per i propri prodotti. Partecipare ad un progetto open source dimostra il nostro impegno nei confronti del mondo dello sviluppo del software, che ci aiuterà a garantire servizi mai visti prima. E le nostre app dialogano con tutti gli altri sistemi».