PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3711 di giovedì 04 febbraio 2016

I rischi delle automobili informatiche

Oggi una quota crescente delle automobili in commercio è dotata di una forte componente informatica. Sono state già date varie dimostrazioni del fatto che è possibile attaccare i sistemi informatici e creare problemi oltremodo gravi. Di A.Biasiotti.

Il fatto che le moderne automobili siano dotate di sistemi informatici di comando e controllo, fra loro in collegati mediante bus ad alta velocità, e siano inoltre dotate di collegamento Wi-Fi e Bluetooth, crea dei problemi che solo adesso si stanno rivelando nella loro vera dimensione.
I giornali hanno dato ampio risalto al fatto che una moderna autovettura della Fiat Chrysler è stata attaccata da hacker, che hanno potuto intervenire sul sistema frenante.

La situazione è diventata talmente grave, che è stato addirittura organizzato un incontro sulla sicurezza delle automobili informatiche, a Dresda, per evidenziare ai fabbricanti quanto sia grave il problema e come essi sino ad oggi abbiano sottovalutato la necessità di adottare misure di protezione.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[DVD016] ?#>

Secondo un esperto, oggi già vi sono, in una autovettura di moderna concezione, più di 50 punti di attacco nel sistema informatico che gestisce l'automobile.
D'altro canto, che i sistemi di controllo di apparati meccanici possono essere attaccati, portando alla distruzione degli apparati stessi, è stato dimostrato dall'ormai famoso virus Stuxnet, che ha distrutto le centrifughe, che il governo iraniano utilizzava per aumentare la concentrazione di particelle radioattive nell'uranio. Secondo gli esperti, esistono due soli tipi di autovetture informatiche:

- quelle che sono state già attaccate e quelle che certamente saranno attaccate!

Ad esempio, i sensori di distanza, che permettono di frenare automaticamente una autovettura, se si avvicina troppo ad una vettura che la precede, sono decisamente esposti ad attacchi ed è quindi possibile, per un hacker, costringere una vettura a frenare, indipendentemente dalla volontà del guidatore.

Un altro spettacolare filmato, che è stato mostrato in una mostra di categoria, fa vedere come una automobile possa essere guidata fuori strada e fatta precipitare in un fossato, senza che l'autista abbia alcuna possibilità di controllo.

Una recentissima dimostrazione, particolarmente drammatica, fa riferimento ad una moderna vettura, dotata di specchietti elettrici, comandati dal bus informatico di bordo. Inserendosi su questo bus, che è facilmente accessibile dall'esterno, è possibile inserirsi nel sistema informatico di comando e controllo della autovettura, sostituendo a tutti gli effetti il guidatore.
In pratica, si deve sottolineare che mano mano che una automobile diventa un computer, o meglio un sistema di computer inter collegati, si manifestano gli stessi problemi che capitano in una rete composta da un server con alcuni pc client.

La soluzione non sembra facile ma è già un grande passo avanti il fatto che i maggiori fabbricanti mondiali di autovetture informatiche si siano resi conto del problema e abbiano cominciato ad affrontarlo, impegnando adeguate risorse.

Un aspetto che già si è manifestato, riguarda il fatto che queste autovetture devono essere dotate di un punto di accesso, debitamente protetto, che permetta di aggiornare costantemente il software, per far fronte ad eventuali debolezze, che si manifestino dopo che l'autovettura è stata messa su strada.

Un'altra soluzione, assai interessante, riguarda la adozione di protocolli crittografici leggeri, come quelli descritti nella norma ISO 29192, per proteggere lo scambio dei dati tra i vari computer di bordo.

Il vantaggio di utilizzare la crittografia leggera sta nel fatto che non è necessario appesantire oltremodo l'informatica di bordo, che ha delle capacità di elaborazione sostanzialmente limitate.

Come al solito, nuovi traguardi portano nuove sfide e speriamo che i tecnici automobilistici ed informatici le sappiano vincere.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it