
# Come farsi rubare l'automobile (o gli oggetti di valore all'interno) e, soprattutto, NON essere risarciti dall'assicurazione



1) L'inibizione del segnale del telecomando
1.1) La nostra difesa
2) La clonazione dei codici del telecomando
3) Le chiavi di avviamento con trasponder
4) Il furto dell'auto interconnessa
5) Il furto dell'auto con chiave keyless
5.1) Una possibile difesa
6) I dati registrati nel chip di memoria delle chiavi
6.1) Come farsi negare il risarcimento dall'assicurazione
7) La consulenza tecnica di parte

## 1) L’inibizione del segnale del telecomando

I ricevitori dei radiocomandi apriporta delle automobili, sono dispositivi economici e di modesta qualità. Soprattutto, dal punto di vista della selettività, ossia la capacità di non essere disturbati da un segnale con frequenza adiacente, lasciano molto a desiderare.

Questo spiega perché, a volte, capita di non riuscire a chiudere o ad aprire lo sportello tramite il telecomando. Probabilmente c'è un radiosegnale nelle vicinanze che satura il ricevitore a bordo dell'automobile. Spesso basta attendere qualche minuto per tornare al normale funzionamento.

Ma, attenzione; non sempre si tratta di disturbi casuali e involontari! Vediamo perché: La normativa europea, qualche anno addietro, prevedeva, per i radiocomandi delle automobili e per quelli apricancello, la frequenza di trasmissione di 433.920 Mhz.

Ben presto però, i malviventi si accorsero che bastava acquistare un walkie-talkie di tipo “LPD” (vedi qui a fianco) in libera vendita e di libero uso, e trasmettere sulla predetta frequenza, per bloccare il funzionamento di tutti i radiocomandi nel raggio di una trentina di metri e oltre.

Infatti, costoro si posizionavano, di preferenza, nei parcheggi di autogrill o supermercati e attendevano l'arrivo di un automobilista frettoloso e distratto che tentava di bloccare lo sportello. L'interferenza radio, stavolta tutt'altro che casuale, inibiva il funzionamento dl radiocomando. Se la potenziale vittima si accorgeva del mancato lampeggio delle frecce e, soprattutto, non udiva il “clack” dei chiudiporta, il malintenzionato interrompeva la trasmissione consentendo la regolare chiusura.


Al contrario, se l'automobilista non si avvedeva dell'anomalia e si allontanava senza aver bloccato le portiere, un complice entrava in azione, aprendo il bagagliaio e rovistando dentro l'abitacolo in cerca di merce di valore. Personal computer, tablet, apparecchi fotografici, telefoni cellulari, subivano così un indesiderato trasferimento di proprietà…

In tempi più recenti, la normativa europea ha introdotto la nuova frequenza di 868 Mhz che presenta una maggiore immunità ai radiodisturbi, in sostituzione della precedente 433.920 Mhz.

Come c'era da aspettarsi, i malviventi si sono prontamente aggiornati, dotandosi di apparecchi “jammer” come il B37 (vedi qui a sinistra), in grado di inibire le

frequenze da 315 Mhz a 433 Mhz oltre agli 868 Mhz con una larghezza di banda di +/- 3 Mhz e una potenza di uscita di circa 960 mW.
In parole semplici, questo dispositivo è in grado di inibire tutti i telecomandi apriporta, ma anche gli apricancello, da una distanza ben superiore ai 35 metri, sovrastando senza difficoltà i deboli segnali dei radiocomandi.

### 1.1) La nostra difesa

Quando vi fermate in autogrill per un caffè ristoratore o parcheggiate in un supermercato per rifornire la dispensa, se non volete che quella sosta rimanga tra i ricordi spiacevoli... controllate sempre il regolare bloccaggio delle portiere. Se il telecomando sembra improvvisamente non funzionare, chiudete le serrature con la chiave classica e.... tenete gli occhi aperti.
Tenete comunque presente che, qualora abbiate attivato l'estensione danni all'auto per furto di oggetti, se qualcuno ruba qualcosa al suo interno, la Compagnia, non rilevando segni palesi di scasso, potrebbe contestare il risarcimento adducendo la cattiva diligenza nella custodia del bene assicurato (art. 1768 c.c) ipotizzando che non siano state regolarmente chiuse le portiere.

## 2) La clonazione dei codici del telecomando

I moderni telecomandi apriporta per automobile, ma anche gli apricancello o quelli per basculante, adottano un sofisticato sistema per impedire la clonazione di codici.
Nel recente passato il codice non era nulla più di un treno di impulsi digitali sovrapposto al segnale radio, che si ripeteva sempre eguale a se stesso. Facile ascoltare questo segnale, tramite un ricevitore “scanner”, registrarlo e ritrasmetterlo, per aprire senza difficoltà le portiere di un'automobile o il cancello condominiale e fare “visita” a qualche appartamento.
Successivamente, le industrie elettroniche hanno messo a disposizione un nuovo sistema di codifica chiamato “*rolling code*” che cambia il codice ad ogni nuova trasmissione secondo un algoritmo riservato. Ogni volta che premiamo il tasto del telecomando viene generato un codice nuovo e valido solo per quella occasione. Registrarlo e ritrasmetterlo non servirebbe a nulla poiché quel codice non sarebbe più valido, né è possibile “indovinare” il codice successivo senza conoscere l'algoritmo che ne governa la creazione.
Il sistema si era dimostrato inviolabile per lungo tempo ma non si poteva continuare in eterno ad impedire a chi trae il proprio sostentamento economico da furti e rapine, di portare a casa il pane quotidiano, che diamine! E infatti, recentemente, l'algoritmo che governa il “rolling code” ha iniziato a mostrare alcune crepe.
Samy Kamkar è un abile  hacker e ricercatore nel campo della sicurezza, che ha studiato a lungo il sistema fino a trovarne i limiti. Sia chiaro; Samy non è un ladro, tutt'altro. È un hacker che evidenzia le debolezze dei sistemi antifurto e di quelli informatici, allo scopo di spingere i costruttori

a progettare dispositivi più sicuri.[1]

Solo quando le sue scoperte diventano di dominio pubblico, le industrie sono obbligate a fare investimenti e prendere provvedimenti (anche per salvaguardare la propria immagine).

Foto: cortesia Samy Kamkar

Vediamo nel dettaglio in cosa consiste la scoperta di Samy Kamkar: Si chiama Roll-jam (vedi foto a destra) ed è un dispositivo elettronico in grado di “ascoltare” e registrare il codice emesso da un telecomando “rolling code” al momento in cui viene premuto il pulsante di chiusura o apertura e contemporaneamente inibire per pochi istanti il funzionamento del ricevitore posto a bordo dell'automobile.

Il proprietario, avvedendosi del mancato bloccaggio delle portiere, premerà nuovamente il bottone del telecomando, generando così un nuovo codice, diverso dal precedente e chiudendo finalmente l'auto.

E qui sta il “bug” del sistema “rolling code”: la memoria del Roll-jam ha registrato il primo codice, che non è stato però utilizzato perché il ricevitore era inibito. Quindi dispone di un codice ancora valido che potrà essere usato per la prossima apertura delle portiere. Semplice ed efficace!

Ora la domanda è: quanto tempo passerà prima che i “soliti ignoti” realizzino un dispositivo analogo al Roll-jam?

In realtà già esiste un sistema di attacco al “rolling code”, molto meno efficace e mirato della creazione di Samy, tuttavia sufficiente allo scopo, basato su un attacco “brute force”.

Facciamo un esempio: il signor Rossi chiude le portiere della sua automobile con il telecomando e si allontana. Capita che giocherelli con i pulsanti, premendoli più volte quando si trova a grande distanza dalla sua auto, quindi il ricevitore non può seguire l'evoluzione dei codici che, come ho già detto, cambiano ogni volta che schiaccia il bottone. Tuttavia, quando torna indietro il telecomando funziona al primo colpo.

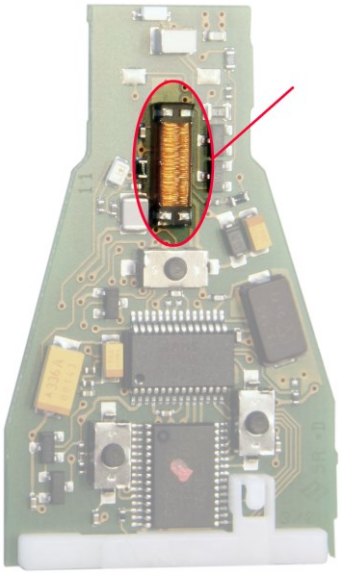
La spiegazione è semplice: il costruttore del “rolling code” ha previsto un'ampia “finestra” di tolleranza fra un codice ed il successivo, per la precisione si tratta di 256 codici, proprio per aggirare simili problemi. Inoltre dovete sapere che la parte elettronica delle chiavi di cui stiamo trattando viene prodotta da un ristrettissimo numero di aziende che si avvalgono di algoritmi standard, aumentando così, anche se involontariamente, le possibilità di successo della malavita.

Il risultato è un ulteriore “bug” del sistema: Il “ladrus tecnologicus” dispone di un ricevitore sulla frequenza del “rolling” in grado di esaminarne il codice e di trasmetterne in rapida sequenza un centinaio di “probabili” a partire da quello copiato fino a trovare la combinazione corretta. Non è un sistema efficiente; nessun “brute force attack” lo è, ma se il ladro dispone di tempo sufficiente, potete stare certi che il nostro automobilista ha buone possibilità di tornare a casa con i mezzi pubblici. Ok, ok, ho capito! Non basta aprire le portiere per rubare un'automobile. Le macchine attuali hanno le chiavi di avviamento dotate di “trasponder” che impedisce la messa in moto

girando semplicemente il blocchetto di accensione. Questo lo so anche io; ma seguitemi nel prossimo paragrafo e vedrete...

### 3) Le chiavi di avviamento con trasponder

Intorno alla metà degli anni '90, le case automobilistiche, in un'ottica di contrasto dei furti di auto, vista la facilità con cui questi venivano portati a termine, iniziarono a implementare minuscoli dispositivi elettronici all'interno dell'impugnatura delle chiavi di avviamento, trasformando la semplice chiave meccanica in un dispositivo "*meccatronico*" tale da dialogare con la centralina di avviamento attraverso l'invio di codici digitali bi-univoci.



Era nato il "*trasponder*", (vedi, nella foto a destra, l'area evidenziata) acronimo di "*transmitter/responder*", un dispositivo elettronico privo di batteria e abbinato ad ogni veicolo, che viene alimentato per induzione elettromagnetica mediante una bobina installata intorno al blocchetto di accensione. Quando si gira l'avviamento, un segnale radio intorno ai 500 Khz viene inviato dalla centralina di iniezione alla chiave che risponde con il codice di identificazione contenuto nella propria memoria. Solo se la "password" viene riconosciuta, l'immobilizer consente l'accensione del motore, rendendo obsoleta ed insufficiente la semplice incisione meccanica della chiave.

Oggi, i transponder di ultima generazione a 128 bit sono in grado di gestire un numero di codici pari a 340 seguito da 36 zeri, una cifra astronomica. Tuttavia, le statistiche sui furti di automobili elaborate ogni anno dal Ministero degli Interni, dimostrano come le difese contro tale reato, pur se più difficile da portare a termine, sono più apparenti che sostanziali.

Al di là della semplice asportazione mediante l'uso illegale di un carro-attrezzi, più comune di quanto non si creda, si deve ricordare un sistema di sicurezza voluto dalle normative europee sulla circolazione dei veicoli a motore.

Allo scopo di prevenire il blocco del motore causato da un'avaria dell'immobilizer, magari mentre si sta effettuando un sorpasso, il dispositivo prevede la propria autodisabilitazione quando il veicolo marcia a velocità superiori ad una certa soglia (generalmente 25 Km/h).

Purtroppo questa necessaria forma di prevenzione degli incidenti può essere sfruttata per il furto. Basta infatti spingere l'automobile, con il cambio in folle, lungo una discesa fino a superare tale soglia minima e solo allora inserire una marcia, rilasciare la frizione e girare il blocchetto di

accensione, in questo ordine, per avviare il motore che, una volta in moto, non si spegnerà durante le eventuali soste.
Altro sistema usato per il furto consiste nella sostituzione della centralina di iniezione elettronica con altra precedentemente modificata a livello di "*eprom*"[2] in modo da disabilitare il riconoscimento del codice dell'immobilizer. Tale sostituzione comporta solo un paio di minuti di lavoro.

### 4) Il furto dell'auto interconnessa

Le automobili del futuro, e in generale tutti i mezzi di trasporto, saranno sempre più elettriche, condivise (il cosiddetto "*car sharing*"), a guida autonoma e connesse a internet. La strada è oramai tracciata e questa prossima rivoluzione è tanto certa quanto inevitabile, per contrastare l'inquinamento dell'aria che respiriamo e prevenire gli incidenti.
Quanto la connessione a internet sia una buona idea è ancora da dimostrare; basti pensare alle possibilità di uso non autorizzato del sistema da parte di aggressori che, prendendone il controllo, potrebbero aprire le portiere e avviare il motore, dopo aver disabilitato l'antifurto, sottraendo il veicolo al legittimo utilizzatore o disabilitando da remoto alcune funzionalità attraverso la modifica del software o iniettando "*malware*"[3] all'interno del sistema, come è già stato fatto durante un esperimento negli USA, facendo entrare in funzione, da remoto, i freni di un'auto in movimento.
Nell'estate del 2015 sono stati richiamati dal mercato moltissimi veicoli Jeep Cherokee perché era stato scoperto un *bug* nel sistema "*UConnect*$^{tm}$" che lo rendeva facile bersaglio di cyber attacchi, mentre problemi analoghi hanno colpito altre note marche del settore automobilistico, che ovviamente hanno preso gli opportuni provvedimenti.
Stiamo prestando la dovuta attenzione alla sicurezza che riguarda questo genere di connessioni a internet? Una soluzione ai diversi problemi di sicurezza che emergono è sempre possibile, ma si tratta di processi onerosi che riguardano l'aggiornamento dei sistemi o addirittura la sostituzione di alcune loro parti.
È pur vero che tutte le comunicazioni con entità esterne prevedono una protezione tramite l'autenticazione reciproca, la crittografia dei messaggi di comunicazione, l'interposizione di "*firewall*"[4] ecc. affinché sia garantito che solo le comunicazioni autenticate e autorizzate possano accedere al sistema, ma è altrettanto vero che schiere di *hackers*[5] (sarebbe più corretto chiamarli *black-hat hackers*) penetrano quotidianamente in computer che *sembravano* superprotetti. Una volta che avranno a disposizione moltitudini di automobili, credete che cambieranno le loro insane abitudini o rinunceranno alla loro smania di mostrare al mondo quanto sono bravi?
Un discorso a parte va fatto a proposito delle compagnie di assicurazione; state pur certi che queste ultime saranno vivamente interessate all'interconnessione automobile/internet/GPS, se non altro per contrastare le frodi basate su incidenti simulati, ricostruendone *ex post* la dinamica, o per favorire il ritrovamento di veicoli rubati (e assicurati contro il furto). Tuttavia, una riflessione sorge spontanea: cosa succede se, in caso di incidente, con ragione, la compagnia può dimostrare che l'assicurato aveva uno stile di guida spericolato, cambiava improvvisamente corsia o superava

spesso i limiti di velocità, non allacciava la cintura di sicurezza, usava il telefonino durante la guida. Pensate che risarcirà il danno senza avvalersi di clausole quali il concorso di colpa?[6] Negare il consenso a una simile profilazione adducendo ragioni di privacy, potrebbe portare alla esclusione di alcuni benefit. Primo fra tutti, vantaggi economici nel costo dell'assicurazione.
(La "scatola nera" proposta da alcune compagnie a fronte di uno sconto sulla polizza RC e furto, già oggi ha queste potenzialità, per così dire, leggermente invasive…).

## 5) Il furto dell'auto con chiave keyless

La tecnologia si evolve e, gradualmente, le chiavi meccaniche stanno lasciando il campo ai sistemi "keyless" che consentono l'apertura delle portiere e addirittura l'avviamento del veicolo, tenendo semplicemente la chiave in tasca e premendo un pulsante. Una bella comodità (e un bellissimo gadget), non c'è dubbio, ma… la sicurezza?
Lo sfondamento dei finestrini e la forzatura delle serrature? Comportamenti oramai obsoleti per il "ladrus tecnologicus" che lavora con i guanti per non lasciare le sue impronte, ma… si tratta di guanti bianchi!
La tecnologia keyless è in grado di rilevare la chiave, o meglio, i codici emessi dalla sua elettronica, quando è in prossimità del veicolo. Purtroppo però la chiave può essere eccitata, ossia spinta a trasmettere codici, avvicinandosi con un dispositivo piuttosto semplice e poco costoso. Il segnale così captato viene amplificato e ritrasmesso attraverso un congegno che funziona in modo simile a un ponte radio.
Così facendo si aggira il problema dei codici della chiave keyless poiché il sistema usa la chiave stessa, quella originale, per aprire e mettere in moto l'auto anche da notevole distanza. Solo che lo fa all'insaputa del legittimo proprietario.

### 5.1) Una possibile difesa

Esistono in commercio delle bustine di plastica metallizzata con caratteristiche antistatiche il cui costo è di pochi centesimi di euro. Normalmente servono per immagazzinare e trasportare circuiti elettronici particolarmente sensibili alle cariche elettrostatiche come, ad esempio, le memorie RAM dei computer.
Riponendo la chiave keyless al loro interno, questi sacchetti si comportano come gabbie di Faraday, isolandola ed impedendone l'accoppiamento wireless con i dispositivi di cui sopra.
Ovviamente, quando ci si avvicina alla propria macchina, si deve estrarre la chiave dal sacchetto, pena la mancata apertura della portiera ed il mancato avviamento del motore. Non è il massimo della comodità, siamo d'accordo, ma neanche tornare a casa a piedi lo è!

## 6) I dati registrati nel chip di memoria delle chiavi

Nell'impugnatura delle chiavi di avviamento della vostra automobile, c'è molto più dell'immobilizer (cap.3) o del telecomando apriporta. Quasi nessuno sa che c'è anche un chip di memoria che registra una lunga serie di parametri relativi al veicolo (vedi tabella seguente) utilizzati dai centri di assistenza autorizzati ai fini della manutenzione periodica programmata. Ogni volta che usate la vostra automobile, nel momento in cui parcheggiate e spegnete il motore questi parametri vengono aggiornati.

| | | | |
|---|---|---|---|
| N° telaio | WBAWB7▓▓▓P▓▓▓▓ | Liquido freni | 07.06. ▓ 00:00 |
| Marca | BMW | Tensione batteria | 14,57 Volt |
| Prodotto | Vettura | Contenuto serbatoio | 25 litri |
| N° tipo | WB71 | Temperatura antigelo | 99 °C |
| Modello | 335i N54 | Temperatura esterna | 15,3 °C |
| Serie | E92 | Km medio/settim. 2 mesi | 150 Km/sett. |
| Tipo base | WB71 | Km medio/settim. 6 mesi | 319 Km/sett. |
| Codice colore | 0354 | Chilometraggio residuo | |
| Chilometraggio | 58.200 | Prossimo servizio | |
| Data di lettura | 21.09. ▓ 16:10 | LED servizio | |
| Variante chiave | 8 | Codice interv. in scadenza | Sconosciuto |
| Sottovariante chiave | 6 | Attributi chiave estesi | |
| Num. personalizzaz. chiave | 0 | Codice paese veicolo | ECE |
| Cod. descriz./colore interni | LCD1 | Data consistence1 | 255 |
| Origine | K | Data consistence2 | 255 |
| Ultimo aggiornamento | 24.02. ▓ 09:00 | Data consistence3 | 255 |
| Equipaggiamento | 02.05.07 | Data consistence4 | 254 |
| Prima immatricolazione | 19.07. ▓ | Livello olio motore | Livello Ok |
| Revisione | 07.07. ▓ | Inform.Engine Oil code | 0 |
| Controllo gas di scarico | 07.07. ▓ | Inform.Engine Oil description | Livello Ok |

Nel malaugurato caso la vostra vettura venisse rubata, la compagnia assicuratrice vi chiederà la consegna di entrambe le chiavi di avviamento in dotazione, pena il mancato risarcimento del danno.

Infatti, nel contratto assicurativo la compagnia pone determinati vincoli, tra cui quello di custodire il bene con la "diligenza del buon padre di famiglia" (art. 1176 c.c.), concetto utilizzato nel linguaggio giuridico per indicare un vero e proprio criterio di comportamento dell'obbligato nell'adempiere l'obbligazione.

Nella fattispecie di cui parliamo è certamente implicita una condotta tesa a non facilitare in alcun modo eventuali furti, ad esempio, lasciando l'automobile con le chiavi inserite nel cruscotto o anche poggiate all'interno del veicolo, agevolando così l'opera dell'eventuale ladro.

Per questa ragione, il risarcimento del danno è subordinato alla consegna di entrambe le chiavi del mezzo, oltre alla denuncia del reato alle competenti Autorità.

Ma, attenzione! Proprio la consegna delle chiavi, come da contratto, vi si potrebbe ritorcere contro. Ne parliamo nel prossimo paragrafo.

### 6.1) Come farsi negare il risarcimento dall'assicurazione

Niente di più facile; basta aver smarrito una delle due chiavi, non averne fatto denuncia alle Autorità e non aver comunicato il fatto alla vostra compagnia di assicurazione con raccomandata r.r. (ovviamente prima che il furto sia avvenuto).

Per quanto tutto ciò possa sembrare assurdo o eccessivo, questa negligenza comporterà inevitabilmente il mancato indennizzo.

Le compagnie assicurative si debbono tutelare, oltre che da eventuali comportamenti negligenti dell'assicurato, anche dai tentativi di frode. Qualcuno, troppo disinvoltamente, potrebbe vendere la propria automobile dopo averla trasferita all'estero, magari in paesi dove il locale Pubblico Registro Automobilistico non è particolarmente efficiente, lasciando all'acquirente una delle due chiavi, per poi denunciare il furto al rientro in Italia.

Al fine di aggirare la richiesta di consegna di entrambe le chiavi, costui potrebbe trovare una chiave esteticamente identica presso qualche autodemolitore.

Per questo le compagnie hanno adottato la prassi di far "leggere" dai concessionari autorizzati i dati contenuti nella memoria delle chiavi, allo scopo di accertarne la corrispondenza con il veicolo rubato.

Come potete vedere, nella prima riga della tabella precedente si trova il numero di telaio dell'auto. Si tratta di un dato non riscrivibile, ovviamente, così come alcuni altri, senza avere l'apposito software in dotazione ai soli concessionari autorizzati.

In alcuni casi che ho trattato, come CTU su incarico del magistrato, ho esaminato chiavi nelle quali il numero di telaio non corrispondeva o il circuito elettronico era stato fabbricato anni prima della data di immatricolazione della vettura oggetto di furto né era congrua la data nel campo "Prima immatricolazione".

In un paio di casi è capitato che la data "Ultimo aggiornamento" non corrispondesse affatto con quella della denuncia del furto, dando l'impressione che l'automobile fosse stata guidata dopo tale denuncia e alimentando così i sospetti di un tentativo di frode. Succede più spesso di quanto non si creda!

La realtà, tuttavia, è ben diversa: la data di "Ultimo aggiornamento" viene copiata dal calendario/orologio nel cruscotto dell'auto ma questa informazione deve essere inserita dal guidatore. Se questi trascura di immetterla o di correggerla in occasione dell'ora legale/invernale, potrebbe non esserci corrispondenza cronologica fra la data/ora del furto e quella di ultimo uso del veicolo.

Infatti, non ci sono sistemi di immissione automatica e non modificabili della data/ora attraverso il segnale orario o mediante il navigatore satellitare. È chiaro quindi che questi dati non possono avere valore forense, nell'accezione del termine quando vuole indicare informazioni certe e non alterabili, analogamente a quanto previsto e normato nell'informatica forense, dove la lettura e/o duplicazione dei dati digitali è sottoposta a rigide procedure che ne garantiscano la genuinità.

Inoltre, si deve considerare che l'"Ultimo aggiornamento" è subordinato al superamento di una

velocità e/o di una percorrenza kilometrica minima, variabile a seconda del software adottato dalla casa automobilistica. Al di sotto di questi parametri i dati registrati rimarranno quelli precedenti creando, ancora una volta, inspiegabili discordanze fra l'orario di ultimo utilizzo della vettura e quello, presunto, del furto.

## 7) La consulenza tecnica di parte

Da quanto visto sinora, si trae l'amara conclusione che, in non pochi casi, la persona assicurata contro il furto, dopo aver subito il danno dovrà rassegnarsi anche alla beffa del mancato risarcimento.
In questi casi, contestare le conclusioni della compagnia assicuratrice attraverso una perizia tecnica di parte che evidenzi i limiti oggettivi dei dati contenuti nella memoria della chiavi, o descriva le tecniche adottate dai malviventi per sottrarre l'automobile al legittimo proprietario aggirandone le difese, può costituire la chiave di volta per vedere riconosciute le proprie ragioni ottenendo il giusto ristoro dei danni subiti.

**Note**

1) https://en.wikipedia.org/wiki/Samy_Kamkar nella parte relativa a "Automotive security research".

2) Eprom; acronimo di Erasable Programmable Read Only Memory. Si tratta di memorie programmabili e cancellabili, di sola lettura, oramai obsolete, che vengono gradualmente sostituite dalle EEprom o dalle memorie "flash". Sono usate in un'infinità di dispositivi elettronici e quindi anche nelle centraline di iniezione del carburante dei moderni motori. I software digitali registrati nelle Eprom/ EEprom/ Flash sovraintendono alle condizioni di esercizio del motore, governandone tutte le funzioni vitali, dall'iniezione del carburante nei cilindri, alla corretta fase della scintilla nella camera di scoppio ad altri fondamentali parametri.

3) Malware; acronimo di "*malicious software*" (software dannoso o codice maligno). Si tratta di software usato per interferire con le operazioni svolte da un computer, al fine di rubare informazioni sensibili (dati delle carte di credito o codici di accesso all'internet banking) o accedere a sistemi informatici privati. Può anche criptare i dati del computer bersaglio, tentando di estorcere denaro per la decriptazione.

4) Firewall; termine inglese per indicare un muro tagliafuoco o una parete refrattaria. In informatica, indica un software di sicurezza avente lo scopo di filtrare gli accessi alle risorse di un sistema controllando tutto il traffico che questi scambia con l'esterno.

5) Hacker; esperto di sistemi informatici e di sicurezza informatica che studia il modo di introdursi in reti protette allo scopo di acquisire un'approfondita conoscenza del sistema scoprendone i

punti deboli allo scopo di migliorarne la sicurezza. Vengono meglio definiti come “white hat hackers”, in contrapposizione con i “black hat hacker” o crackers che tentano di aggirare le difese dei sistemi informatici al fine di trarne profitto o provocare danni.

6) La presunzione di responsabilità concorrente dei conducenti, regolata dal secondo comma dell’art. 2054 c.c. limitatamente al danno derivante dalla circolazione di veicoli, si applica quando le risultanze probatorie non permettono di accertare in quale misura il comportamento dei due conducenti abbia causato l'evento dannoso.
Tuttavia, anche qualora venga accertata la colpa esclusiva di uno dei due, non per questo l'altro si libererà automaticamente dalla presunzione di corresponsabilità. È necessario, infatti, che dimostri di avere osservato le norme sulla circolazione e quelle di comune prudenza (Cass. 07/02/1997, n.1198 e Cass. 26/10/1992, n. 11610).

**Sitografia**


www.altalex.com/

http://www.brocardi.it/codice-civile/

https://www.octotelematics.com/it/focus/auto-interconnessa

http://www.ilgiornale.it/news/interni/1025706.html

http://motori.virgilio.it/info-utili/come-i-ladri-rubano-le-auto-provviste-di-satellitare/84018/

http://punto-informatico.it/2886489/PI/News/come-ti-cracko-automobile.aspx

http://www.ilgiornale.it/news/cronache/rolljam-lultima-arma-dei-ladri-auto-funziona-1159856.html




**Torna alla Home Page:** http://www.perizieforensi.com/