PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5217 di Lunedì 01 agosto 2022

La debolezza dei telecomandi utilizzati in tutte le moderne autovetture

I telecomandi degli autoveicoli nel tempo si sono evoluti, passando dalla trasmissione di codici fissi a codici evolutivi, ma recenti esperienze dimostrano che questo passaggio è lungi dal garantire adeguata sicurezza al proprietario dell'autovettura.

La stragrande maggioranza dei moderni veicoli è dotata di un sistema di sicurezza chiamato Remote keyless entry ? RKE. Il proprietario ha in dotazione un telecomando, con una portata di qualche metro, che invia una sequenza codificata al ricevitore, a bordo dell'autovettura. La ricezione di un corretto segnale consente l'apertura degli sportelli e la messa in moto.

Questo sistema ha funzionato abbastanza bene per parecchi anni, finché i malviventi non misero a punto una tecnica per catturare la sequenza codificata, che operava su una frequenza ben nota. In Italia, tempo addietro, alcune aree di servizio in autostrada erano diventate terreno minato per tutti i proprietari di autovetture, perché all'interno di essi operavano bande ben organizzate.

I fabbricanti hanno reagito a questa situazione inventando una nuova tecnologia, chiamata rolling code. Con questa tecnologia il codice che viene inviato, per l'attivazione e lo sblocco dei sistemi di sicurezza dell'autovettura, non è fisso, ma cambia ad ogni trasmissione.

Ovviamente è stato modificato anche il dispositivo di ricezione, bordo dell'autovettura, che deve essere in grado di accettare, mano a mano che vengono inviati, i nuovi codici.

Il problema che nasce da questa soluzione è legato al fatto che il proprietario potrebbe accidentalmente premere il telecomando, trovandosi a notevole distanza dall'autovettura. In questo caso il contatore all'interno del telecomando avanza di un passo, mente il contatore all'interno del ricevitore, posto nell'autovettura, non avanza. Questo sfasamento fra il codice inviato ed il codice accettato può portare alla impossibilità di accedere all'autovettura.

Ecco perché alcuni fabbricanti hanno introdotto una funzionalità di risincronizzazione, che consiste nell'inviare dei comandi in una sequenza consecutiva, permettendo di risincronizzare il dispositivo emittente ed il dispositivo ricevente.

Questa debolezza strutturale dell'architettura di comando viene chiamata, con un termine inglese piuttosto insolito Rolling-PWN.

PWN è l'abbreviazione di pwned; un moderno dizionario on-line afferma che questa parola ha avuto origine in un gioco on-line, chiamato Warcraft, laddove un progettista delle mappe aveva sbagliato nello scrivere la parola "owned", che significa di proprietà. Oggi questa parola significa che qualcheduno o qualche cosa viene dominato da un altro soggetto, sia nei giochi on-line, sia, in tempi più recenti, nella sua posizione in Internet.

Applicando questa interpretazione, l'espressione Rolling- PWN significa che il sistema rolling code è stato violato da qualcuno.

Poiché questo attacco non lascia alcuna traccia, è assai difficile, per il proprietario di un autoveicolo, rilevare, anche a posteriori, un tentativo di attacco e questa situazione è indubbiamente oltremodo preoccupante.

Gli esperti, che hanno illustrato questa tecnica di attacco, l'hanno applicata nei confronti di una marca di automobili, assai diffusa, ottenendo risultati sempre positivi, almeno dal punto di vista della violazione effettuata.

L'azienda produttrice di questi autoveicoli è stata contattata e non ha dato risposta.

La situazione è ulteriormente aggravata dal fatto che oggi sono facilmente acquistabili su Internet dei dispositivi, in grado di catturare il segnale codificato trasmesso e memorizzarlo, per una successiva ritrasmissione.

La ripetuta trasmissione dello stesso segnale fa avviare la procedura di risincronizzazione fra trasmettitore e ricevitore, mettendo in pratica l'autoveicolo a completa disposizione dell'attaccante.

Ancora una volta, si vede come purtroppo la migrazione verso sistemi completamente digitali può sembrare assai comoda, da un punto di vista operativo, ma può creare debolezze difficilmente superabili.

Ecco perché sono ancora oggi numerose le autovetture, di un certo livello, che abbinano il sistema di sblocco dell'accesso ad una chiave fisica, che permette l'avviamento del veicolo.

L'abbinamento di difese fisiche ed elettroniche rappresenta, ancora una volta, la difesa più efficace.

Adalberto Biasiotti

www.puntosicuro.it