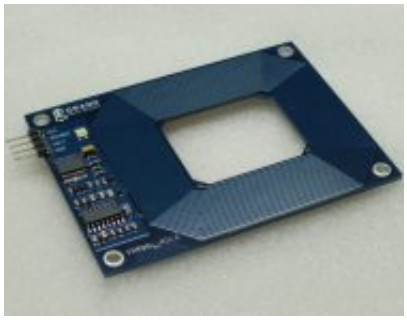
I chips RFID possono essere hackerati: i metodi d’attacco e quelli di difesa

Date : 29 settembre 2016



In telecomunicazioni ed elettronica con l’acronimo RFID - dall’inglese Radio-Frequency IDentification, ovvero “identificazione a radiofrequenza” - si intende una tecnologia per l’identificazione e/o memorizzazione automatica di informazioni inerenti a oggetti, animali o persone. Il funzionamento dei comunemente detti “chips” si basa sulla capacità di memorizzare dati da parte di particolari etichette elettroniche - chiamate “tag” - e sulla capacità di queste di rispondere all’interrogazione a distanza da parte di appositi apparati fissi o portatili - chiamati “reader”. Questa identificazione avviene mediante radiofrequenza, grazie alla quale un reader è in grado di comunicare e/o aggiornare le informazioni contenute nei tag che sta interrogando.

I dispositivi RFID sono presenti in moltissimi oggetti che utilizziamo ogni giorno: carte di credito, libri, beni alimentari, dispositivi medici, passaporti e addirittura nei nostri animali domestici.

La quantità di informazioni che i vostri chips RIFD contiene è dunque a dir poco enorme ed è molto importante conoscere i rischi di questa tecnologia e i metodi tramite i quali proteggersi.

I dispositivi RFID utilizzano essenzialmente due tipi di tag:

- tags passivi: richiedono un segnale radio per essere ricevuti e letti dai rispettivi reader. Questo significa che operano su piccole distanze e non possono trasmettere una grande quantità di informazioni. Ne sono un esempio i chip contenuti nelle carte di credito
- tags attivi: contengono batterie locali grazie alle quali possono trasmettere una maggiore quantità di dati coprendo una distanza più ampia. Dispositivi di questo tipo sono quelli montati nelle automobili che permettono la riscossione automatica del pedaggio autostradale

E’ allarmante quanto sia semplice trovare online strumenti per hackerare un dispositivo RFID, è addirittura possibile comprare, per meno di 20 dollari, interi kit tramite i quali costruire uno scanner di lettura di chips. Sono inoltre presenti online numerosi “tutorial” che spiegano passo passo come chiunque, con una minima capacità di programmazione, possa costruire un proprio reader.

Captare il segnale di oggetti contenenti chips RFID e leggerne il contenuto equivale ad avere pieno accesso a tutte le informazioni che contengono.

Quali sono i metodi per proteggersi dalla lettura a distanza?

Si crede che avvolgere la carta di credito in fogli d’alluminio sia una maniera efficace per proteggerla da scanner illeciti, non è del tutto vero: l’alluminio, sebbene riduca la distanza dalla quale è possibile la lettura, non fermerà i dispositivi più vicini.

E’ sempre più diffusa la vendita di portafogli “protetti”, tuttavia questa protezione risulta spesso essere un semplice foglio di alluminio posizionato all’interno dell’oggetto.

Le tasche e portafogli più sicuri, al fine di proteggere i vostri chips, sono quelli contenenti una gabbia di Faraday. Per evitare l’acquisto di oggetti non efficienti il consiglio è cercare protezioni che riportino nella descrizione le parole “Electromagnetically Opaque” - immune alle frequenze elettromagnetiche e ovviamente stare attenti che il portafogli sia nella nostra tasca!