Sicurezza e protezione dei dati sono argomenti che quando si parla di Near Field Communication, in particolare sul fronte delle card in cui è integrato un chip a radiofrequenza, sono molto dibattuti. La diffusione di applicazioni Nfc ha incrementato notevolmente lo sviluppo di una pluralità di sistemi di sicurezza, utili per la protezione dei dati sensibili contenuti nei microchip. Il problema è che glii attuali sistemi di protezione non riescono a garantire che i dati privati non vengano letti da reader non autorizzati.

Nicolai Marquardt, PhD presso l'università di Calgary, ha ideato, a questo proposito, alcuni prototipi di chip Rfid con diverse tipologie di protezione. In occasione della conferenza Computer Human Interaction di Atlanta, Marquardt ha colto l'occasione per annunciare che il suo progetto permetterà di impedire la lettura dei chip non autorizzata. Obiettivo della ricerca condotta dallo studioso è infatti quello di sviluppare un sistema che consente di sapere quando una tessera dotata di chip Rfid viene interrogata, in modo tale che le prossime generazioni di chip Rfid, applicati su passaporti e carte di credito, non siano soggetti a fenomeni di hacking.

Il ricercatore, grazie alla collaborazione con il centro Microsoft Research nel Regno Unito, ha sviluppato quattro tipi distinti di controller Rfid:

La prima tipologia di controllore restituisce un feedback diretto al possessore della card. In questo modo appena viene eseguita la transazione di lettura, si viene avvisati con un segnale audio-visivo o tattile.

Alla seconda tipologia appartengono i tag controllabili. É stato, infatti, previsto un tipo di chip che deve essere abilitato alla transazione attraverso un tasto fisico. Appartengono alla stessa categoria i chip sensibili al tatto.

La terza tipologia prevede tag dotati di sensori che reagiscono a parametri esterni. Infatti il gruppo di ricerca ha previsto tag attivabili alla luce, in modo tale che il chip non sarà attivabile se lasciato in tasca. Un altro tipo è sensibile all'incluzione, in modo tale che possa essere utilizzato solo se viene posizionato parallelamente rispetto alla superficie di lettura.

L'ultimo gruppo sfrutta proprietà di proximity. I chip che appartengono a questa categoria di

protezione permettono, in qualsiasi istante, la lettura delle informazioni non soggette a riservatezza. I dati soggetti a maggiore privacy verranno quindi rilevati solo quando ci si trova in prossimità del lettore Rfid abilitato.

Attualmente, in questa fase della ricerca, l'unico problema di tali prototipi è che sono relativamente grandi e alcuni necessitano ldi essere alimentati con una batteria.

Il mercato, comunque, è in grande fermento. Secondo la società americana Abi Research le vendite mondiali di chip per il wireless short range (Bluetooth, Nfc, Uwb, 802.15.4, Wi-Fi) dovrebbero quest'anno superare il miliardo di unità, il che significherebbe un 20% rispetto al 2009. E da qui a quattro anni la moviemntazione si attesterebbe a quota 5 miliardi. È facile prevedere che gli investimenti nella near filed communicaiton continueranno a crescere potenziando i vatantaggi associati all'utilizzo di questa tecnologia.