

Sommario

Prefazione	3
Introduzione.....	4
Capitolo 1 Introduzione alla tecnologia RF-ID.....	14
1.1 Introduzione	14
1.2 Le reti Wireless.....	15
1.3 Introduzione alla tecnologia RF-Id	18
1.4 Le origini della tecnologia RF-ID	19
1.5 L'architettura di un sistema RF-id	20
1.5.1 I Tag o Transponder.....	21
1.5.2 I Reader.....	32
1.5.3 Infrastrutture Informative per sistemi RF-ID.....	34
1.6 I principi fisici della tecnologia RF-ID.....	37
1.7 I protocolli anticollisione.....	40
1.7.1 I protocolli deterministici	40
1.7.2 Protocolli probabilistici o stocastici.....	41
1.8 La tecnologia RF-ID vs codici a barre e bande magnetiche	45
1.9 I difetti della tecnologia RF-ID.....	48
1.10 Perché questo interesse nella tecnologia RF-ID?.....	49
1.10.1 Standard Tecnologici	49
1.11 Accenno alla tecnologia NFC.....	55
1.11.1 Di cosa si tratta?	55
1.11.2 Qual è l'aspetto innovativo?	55
1.11.3 Come funziona?.....	56
1.11.4 Quali sono i vantaggi che ne derivano dal suo utilizzo?	56
1.11.5 La storia di questa tecnologia	57
Capitolo 2 Casi d'uso di sistemi RF-ID, una tecnologia silenziosamente pervasiva.....	59
2.1 Introduzione.....	59
2.2 Gestione dei Rifiuti Smart con la tecnologia RF-ID	60
2.3 Tracciabilità degli animali domestici e di allevamento	61
2.4 L'antitaccheggio.....	61
2.5 Rilevazione e monitoraggio dei parametri ambientali	62

2.6 Asset Tracking	62
2.7 Monitoraggio degli oggetti di valore in musei.....	63
2.8 Gestione Biblioteche	63
2.9 La tecnologia RF-ID e il monitoraggio degli accessi.	64
2.10 Payment RFID.....	66
2.11 Tessere e documenti di identità elettronici.....	66
2.12 Titoli di viaggio e biglietteria elettronica	67
2.13 RF-id a tutela di frodi e contraffazione.	68
2.14 RF-id e la sicurezza.	69
2.15 I sistemi RF-id al servizio delle industrie.....	71
2.16 Assistenza e manutenzione.....	74
2.17 I sistemi RF-ID impiegati nella navigazione stradale	75
2.18 La tecnologia RF-ID al servizio dei non vedenti.....	76
2.19 Lettura contatori dell'acqua.....	77
2.20 Pass cittadini per disabili e ZTL	78
2.21 Anche Facebook sperimenta l'utilizzo della tecnologia RF-ID.....	78
2.22 RF-ID nello sport	78
2.23 IdentityTag di i-Car	79
2.24 I sistemi RF-ID nella sanità.....	80
Capitolo 3 La localizzazione con i sistemi RF-ID & le problematiche di sicurezza.....	83
3.1 Introduzione.....	83
3.2 Principi di posizionamento di reti wireless indoor	84
3.3 Stima della distanza.....	85
3.4 Calcolo della distanza di un oggetto a partire da punti noti.....	86
3.5 La Vicinanza (Proximity)	86
3.6 Scene analysis o Analisi della scena	87
3.7 Sistemi di localizzazione più diffusi	87
3.7.1 Active Badge.....	88
3.7.2 Active Bat	88
3.7.3 Cricket	89
3.7.4 Radar	89
3.7.5 Smart Floor	89
3.7.6 GPS.....	90

3.8 Schemi localizzazione RF-ID	90
3.9 La problematica sulla sicurezza.....	94
3.9.1 Dubbi e perplessità sulla tecnologia RF-ID in termini di sicurezza.	96
3.9.2 I potenziali attacchi.	97
3.9.3 Possibili scenari di attacco.	98
3.9.4 Attacco della privacy ... reale minaccia o inutile allarmismo.	99
3.9.5 Tecniche di difesa da potenziali attacchi.	100
3.9.6 Caso di studio : Passaporti con tecnologia RF-ID	102
3.9.7 Caso di studio : Le carte di credito contactless.....	106
3.9.8 Considerazione finale su questa problematica.	109
Capitolo 4 Studio pratico di un sistema RF-ID in alcuni scenari di propagazione	110
4.1 Introduzione.....	110
4.2 Chi è la IDENTEC SOLUTIONS ?	111
4.3 Dispositivi utilizzati.....	112
4.3.1 i-Q350L RTLS SENSOR.....	113
4.3.2 ILR Interrogator i-PORT M 350	114
4.3.3 La componente software.....	116
4.4 Aree simulative.....	123
4.4 Risultati sperimentali in ambienti aperti.....	126
Conclusioni sulla tecnologia RF-ID	152
Bibliografia	155
Ringraziamenti	157

Prefazione

Il percorso di studi universitario prevede il suo naturale compimento con la preparazione da parte dello studente di un lavoro di tesi in cui si va ad approfondire una particolare tematica affine al proprio indirizzo di studio.

Personalmente ho deciso di parlare della tecnologia RF-ID con cui ho avuto modo di lavorare durante i due mesi di tirocinio svolti sotto la supervisione dell'Ing. Peppino Fazio presso il laboratorio di telecomunicazione dell'Università della Calabria.

La tematica del tirocinio propostami dal tutor mi ha fin da subito affascinato e incuriosito. Si tratta di una tecnologia, come spesso succede per le innovazioni tecnologiche, nata dal mondo militare, ricca di potenzialità e dotata di una spiccata versatilità che la colloca in vari aspetti della vita quotidiana.

La tesi è strutturata in quattro capitoli in cui illustrerò l'architettura e i principi di funzionamento, i campi di applicazione, le potenzialità, i vantaggi e anche gli svantaggi che ne derivano dalla sua adozione affrontando una serie di problematiche quali la sicurezza e le tecniche di localizzazione.

Nella parte finale della tesi illustrerò il lavoro pratico svolto durante il tirocinio incentrato sulla sperimentazione dell'architettura messa a disposizione dal tutor accademico con cui ho avuto modo di costatare nella pratica le caratteristiche apprese durante la fase preliminare di documentazione.

In particolare il mio obiettivo è stato quello di valutare le prestazioni dell'architettura sul campo effettuando delle campagne simulative in aree aperte (outdoor) in completa autonomia seguendo i consigli e le indicazioni dell'Ing. Peppino Fazio.

Un lavoro sperimentale necessario a comprendere le caratteristiche del sistema e valutare attentamente come dispiegare opportunamente tale architettura per sfruttare al meglio le potenzialità della tecnologia.

Introduzione

Nel mondo di oggi l'uso dei codici è di fondamentale importanza, se ci pensiamo un attimo siamo circondati da codici alfabetici, numerici, alfanumerici e informatici. Tra tutti questi ce n'è uno che sicuramente è presente nella nostra vita da moltissimo tempo spesso senza neanche rendercene conto, si tratta del codice a barre o meglio conosciuto come bar-code.



Figure 0-1: Nell'ordine da sinistra verso destra abbiamo un esempio di scansione di un codice a barra tridimensionale mediante un comune smartphone, la struttura di un classico codice a barra che identifica un prodotto in commercio e in fine un esempio di scansione di un codice a barra presente sulla lattina di birra.

Ogni prodotto in vendita ha associato un codice che lo identifica univocamente, noi stessi siamo identificati da un codice fiscale che è codificato in bar code sul nostro tesserino sanitario per essere facilmente letto e acquisito dai dispositivi in automatico. Un codice a barre è una combinazione di linee verticali bianche e nere di spessore variabile utilizzata per codificare informazioni leggibili da appositi dispositivi ottici. Essa è la più popolare soluzione per sistemi AIDC (Automatic Identification and Data Capture) in quanto ci permette di reperire e riconoscere dei dati in maniera automatizzata non che permette di identificare con certezza, precisione e rapidità persone ed oggetti.

Il codice a barre si è affermato in tutto il mondo grazie alla facilità di generazione dei codici ad un costo di investimento molto basso.

Tuttavia il bar-code ha dei limiti, e più passa il tempo più questi limiti diventano visibili:

- Si tratta di una tecnologia di sola lettura
- Il codice deve essere visibile per essere scansionato e acquisito
- Se si rovina o si sporca diventa impossibile leggere il codice
- Si può analizzare un solo bar-code alla volta, dunque la lettura è sequenziale.

Tutti questi svantaggi non sono presenti in una altra tecnologia che esiste già da diversi anni ma che solo recentemente si sta affermando e che potrebbe prendere il posto dell'ormai storico codice a barre; Sto parlando della tecnologia RF-ID.

RF-ID acronimo di Radio Frequency IDentification è spesso descritta come l'insieme delle tecnologie in grado di consentire l'identificazione univoca e a distanza di oggetti di qualunque natura, animali e addirittura persone attraverso specifici sistemi che utilizzano le onde radio. I protagonisti di un sistemi RF-ID sono essenzialmente i ricetrasmittitori (o TAG RF-ID) che, interrogati via radio, rispondono e identificano univocamente gli oggetti ad essi associati.

Basato sui sistemi sviluppati durante la seconda guerra mondiale, ha subito nel tempo numerose evoluzioni, le ultime delle quali legate principalmente ai livelli di miniaturizzazione dei sistemi che ne hanno permesso la grande diffusione attuale, cominciata negli anni '90.

Un sistema RF-ID è composto essenzialmente da tre elementi base:

- Un transponder, comunemente chiamato Tag, in grado di contenere un identificativo univoco ed eventualmente altri dati se equipaggiati da memorie capienti.
- Un'antenna capace di leggere i dati contenuti nei tag tramite radiofrequenza.
- Un lettore o Reader che è il dispositivo, fisso o portatile, deputato alla lettura del tag RF-ID, in grado di convertire le onde radio del tag in un segnale digitale che può essere trasferito su un computer.
- Un'infrastruttura software il cui compito è quello di filtrare e elaborare opportunamente i dati ricevuti dai reader e renderli disponibili al sistema informativo aziendale.

Tali sistemi svolgono essenzialmente le stesse funzioni del codice a barre o della banda magnetica, tuttavia non è necessario che tag e reader siano visivamente a contatto diretto fra loro (principio noto come "non line-of-sight") per poter essere letti o scritti e ciò permette di lavorare in luoghi ostici ovvero in presenza di polvere, sporco o qualsiasi altro agente che può fungere da impedimento ma soprattutto è possibile leggere più tag in uno stesso istante scongiurando la lunga e fastidiosa lettura sequenziale. Tuttavia non dobbiamo tralasciare il fatto che i tag RF-ID sono più costosi

rispetto ai codici a barre, ma molto spesso il rapporto costi/benefici è generalmente vantaggioso. Sarebbe comunque sbagliato pensare che la tecnologia RF-ID soppianterà il codice a barre; Molto più verosimilmente, è che le due tecnologie coesisteranno.

La possibilità di leggere simultaneamente più tag porta a valutare l'eventualità di collisione fra i transponder, una problematica che si presenta quando si sovrappongono le onde radio di diversi trasponder letti contemporaneamente da un reader che può confondere il segnale. Esistono sistemi di anti-collisione utilizzati per gestire la lettura simultanea di più tag. Questi sistemi sfruttano degli algoritmi che "scaglionano" i segnali provenienti dai tag, regolando gli intervalli di tempo nei quali devono essere letti. In questo modo non si verificano interferenze ed è possibile prevenire eventuali errori.

La tecnologia RF-ID è basata sul trasferimento di dati mediante campi elettromagnetici. Le informazioni riguardanti l'oggetto sono memorizzate su un supporto chiamato transponder o tag, ad esso associato. Queste informazioni possono essere dati correlati all'oggetto, oppure semplicemente un numero seriale unico che funge da chiave di accesso ai dati presenti all'interno di un database remoto legati a quello specifico oggetto.

Il tag è il vero protagonista dell'architettura RF-ID esso è composto da un Chip ed una antenna. Il Chip, grande pochi millimetri, è la parte "intelligente" costituita da una memoria non volatile contenente un codice unico, il quale viene trasmesso tramite l'antenna (circuito di trasmissione del segnale) all'apparato lettore che controllerà i dati ricevuti.

Come ho avuto modo di accennare, il tag può essere sia letto che scritto da un reader o controller e ne esistono di vari tipi.

Una prima classificazione può essere fatta in base alla sorgente di alimentazione e dunque possiamo distinguere tag passivi, attivi o semi-passivi.

I tag passivi sono il tipo più economico, in quanto non avendo una fonte di alimentazione propria, si alimentano dallo stesso campo elettromagnetico del lettore, il quale induce una corrente nell'antenna del transponder. Ciò significa che il Tag è utilizzabile solo se esposto al Reader.

I tag semi-passivi sono invece dotati di batteria, che tuttavia non alimenta il tag fino quando questo non riceve un segnale dal lettore.

In fine abbiamo i tag attivi i quali essendo dotati di batteria sono capaci di emettere continuamente un segnale di identificazione che consente una localizzazione costante e offrono una maggiore portata al segnale radio e una maggiore distanza di lettura. Quest'ultima tipologia di tag costano di più dei tag passivi e sono più indicati per tracciare il trasporto di beni di valore sulle lunghe distanze.

Per via della loro fonte di energia autonoma, i tag attivi possono essere equipaggiati di sensori di varia natura utili nel campo del monitoraggio.

I sistemi RF-ID, oltre al tipo di tecnologia attiva o passiva, differiscono anche per la gamma di frequenze in cui operano. Di fatto per comunicare fra loro il tag e il reader devono essere sintonizzati alla stessa frequenza.

La gamma di frequenze da utilizzare dipende dal tipo di applicazione.

In generale con l'aumentare della frequenza aumentano la distanza di lettura, le velocità di trasferimento dei dati e il numero di possibili letture simultanee, viceversa diminuiscono i costi di produzione e la grandezza fisica del tag.

Tuttavia le alte frequenze comportano una degradazione delle prestazioni di lettura in presenza di liquidi e di metalli i quali tendono ad assorbire o deviare le onde radio.

L'RF-ID può operare a diverse frequenze:

- Basse frequenze [LF] (125 – 134 kHz)
- Alte frequenze [HF] (13,56 MHz)
- Altissime frequenze [UHF] (852 – 926 MHz)
- Micro onde (2,45 GHz)

Ciascuna banda ha i suoi vantaggi e svantaggi. Le frequenze più basse funzionano meglio in presenza di liquidi, metalli o persone. Le alte frequenze hanno più norme da osservare.

Le frequenze LF inferiori ai 135 kHz sono utilizzabili a livello mondiale, di fatto questa banda è disponibile in tutti i principali paesi: Europa, Nord America e Giappone, tale frequenza è utilizzata per trasmettere limitate quantità di dati a brevi distanze. Per quanto riguarda la frequenza HF di 13,56 MHz i Tag sono standardizzati a livello

mondiale, tuttavia soffre di un bit rate e di un raggio operativo molto basso si parla di 1-2 metri.

Il vantaggio di alzare la frequenza permette di costruire antenne di dimensioni ridotte, quindi adatte a dispositivi portatili, con distanze che raggiungono anche i 10 metri per Tag passivi in particolari condizioni. Anche in assenza di un perfetto allineamento tra il Tag e il Reader, si ottengono buoni livelli di comunicazione.

Per quanto riguarda i tag a Microonde a 2,45 GHz hanno problemi di condivisione dello spettro con altre applicazioni: le Wireless LAN, i forni a microonde e i cordless, per esempio.

Tuttavia le dimensioni dei Tag diventano molto ridotte, con raggio di lettura di decine di metri per soluzioni attive, e fino a qualche metro per quelle passive. Non vi è il problema della visione diretta tra Tag e Reader, ma ha dei costi maggiori rispetto alle frequenze più basse per via della presenza di batterie e di sensori vari.

Secondo le normative ISO, i tag LF e HF possono essere solo passivi, mentre i tag a frequenze UHF e micro-onde possono essere anche semiattivi o attivi.

I transponder o tag, per quanto riguarda le operazioni di lettura e scrittura, possono essere classificate in “read only” (sola lettura), “write once & read many” o WORM (una scrittura, tante letture), “read & write” (lettura e scrittura).

Le prime due tipologie rappresenta un’evoluzione tecnologica del codice a barre, in quanto le informazioni immagazzinate sul microchip, una volta scritte, non possono essere modificate. Le altre due tipologie di tag possono essere utilizzate come una memoria dinamica, in quanto le informazioni sul chip sono aggiornabili in ogni momento, per esempio lungo i passaggi della filiera produttiva; Tuttavia è chiaro che risultano essere più costosi dei tag di sola lettura.

La funzionalità di un sistema RF-ID è in gran parte dipendente dall’infrastruttura informativa associata al sistema medesimo. Una celebre proposta di architettura è stata sviluppata da EPC Global.

Cardine di questa architettura è il servizio ONS (Object Name Service).

La logica di funzionamento è molto semplice, dato che i tag associati ai singoli oggetti memorizzano in genere solo l’EPC (Electronic Product Code) dell’oggetto medesimo, il

servizio ONS collega l'EPC letto dal tag con le informazioni ad esso associate residenti su una base di dati remota.

Dunque l'ONS rende disponibile le informazioni relative all'oggetto (identificato dal tag tramite EPC) attraverso internet nel formato PML (Physical Mark-up Language).

Il servizio ONS per come funziona è molto simile al servizio di rete DNS (Domain Name Service) in grado di associare ad un nome simbolico (URL) un indirizzo IP dell'Host su cui sono residenti i dati. L'ONS risolvendo la dipendenza che lega un EPC con il relativo URL è in grado di consentire un accesso immediato alle informazioni e la possibilità di abbinare al prodotto servizi complementari che vanno ad accrescere il valore del prodotto per i consumatori e per la supply chain.

L'RF-ID, tecnologia dalla spiccata natura trasversale, interseca una pluralità di settori applicativi, declinati in aree di mercato altrettanto variegate.

La tecnologia RF-ID è nata con l'intento di poter identificare univocamente, immediatamente e soprattutto in automatico qualsiasi tipologia di oggetti; Questa funzione è molto utile nelle operazioni della logistica aziendale tanto da andare a snellire le operazioni di inventario con cui molte aziende devono fare i conti.

Tale tecnologia è anche in grado di identificare persone, favorendo dunque un controllo automatizzato nell'accesso in aree o velocizzando le tempistiche di pagamento dei prodotti o servizi si pensi ad esempio alle carte di credito tanto pubblicizzare denominate contactless card.

Grazie alla possibilità di integrare dei sensori all'interno dei tag attivi questa tecnologia si presta anche nelle misurazioni di grandezze fisiche.

Questa soluzione è ideale per la catena del freddo dei prodotti di largo consumo, alimentari e farmaceutici.

Per non parlare della localizzazione della posizione fisica di un oggetto o di una persona.

Tale funzionalità può riguardare il banale rilevamento del passaggio di un oggetto con TAG attraverso un varco, ad un più complesso tracciamento della posizione di un TAG nel tempo e nello spazio con una adeguata precisione.

Sono dunque svariati i campi di applicazione di tale tecnologia, sia va dall'automazione di processo fino al campo farmaceutico medicale per passare dai distributori

automatici, alla manutenzione e service, i pagamenti tramite terminali POS, l'autenticazione del prodotto a tutela del brand a contrasto della contraffazione, il controllo degli accessi, i sistemi di antifurto e la gestione della logistica.

L'adozione di standard internazionali nell'identificazione dei prodotti e nella gestione della comunicazione con i Tag è di vitale importanza. Per questo motivo ci sono stati negli ultimi anni vari tentativi per creare delle specifiche che standardizzano i vari aspetti delle operazioni di un sistema RFID. I benefici della standardizzazione si possono riassumere nei seguenti punti:

- Aumentare la confidenza dei consumatori nelle nuove tecnologie
- Ampliare i mercati per i produttori, incoraggiare la concorrenza a livello globale e ridurre i prezzi per l'utente finale
- Promuovere lo sviluppo tecnologico dei sistemi RFID in tutto il mondo
- Facilitare lo sviluppo di applicazioni incoraggiando l'interoperabilità
- Fornire piattaforme di sviluppo per prodotti complementari (software, hardware e accessori)

Data la moltitudine di frequenze e tipi di Tag si può tranquillamente affermare che non esiste un lettore in grado di leggere qualsiasi tipo di tag.

Con il termine "agile Reader" la EPC Global², associazione privata che porta avanti la normazione sui sistemi RFID, identifica quei lettori che possono leggere tipi diversi di tag, di vari produttori, operando anche a frequenze differenti (ma sempre all'interno della propria banda di lavoro).

I lettori devono rispettare rigorosamente le normative internazionali che regolamentano le trasmissioni radio che variano da paese a paese ed è chiaro come questo sia uno dei problemi, oltre ai costi ancora elevati, che frenano la diffusione su larga scala della tecnologia RFID.

Lo spettro delle frequenze di fatto è regolamentato in maniera differente in ciascun paese, creando un ostacolo alla circolazione di Tag standard su scala mondiale, in particolare per la banda UHF, dove si prevede la crescita più significativa.

Inoltre va osservato che le differenti normative presenti nei vari continenti prevedono anche diverse potenze di emissione radio da parte degli apparati trasmettenti.

Le grandi potenzialità di questa tecnologia e la sua elevata pervasività hanno portato alla luce un altro problema importante ovvero quello della tutela della privacy.

Di fatto la tecnologia prevede che ogni oggetto venga etichettato e dunque indirettamente anche l'uomo in qualche modo risultata essere "etichettato" il che lo rende tracciabile e spiabile.

Questa eventualità ha destato molti sospetti e preoccupazioni tanto da spingere il garante della privacy a legiferare su tale argomento al fine di regolamentarne l'utilizzo. Alcuni Stati USA hanno approvato legislazioni per regolare l'utilizzo delle etichette elettroniche. Dal punto di vista della logistica non sussistono problemi di Privacy in quanto l'EPC Gen2 prevede che i tag contengono solamente un codice univoco ovvero una sorta di numero di serie.

Tuttavia le preoccupazioni principali riguardano la possibilità che la tecnologia possa essere utilizzata per violare la privacy del possessore degli oggetti "taggati".

Le principali obiezioni sono:

1. la consapevolezza o meno dell'utente che un prodotto contenga un RF-ID;
2. le informazioni contenute nell'RF-ID;
3. la associazione possessore/TAG.

Il primo punto è al momento allo studio delle diverse legislature ma emerge un quadro univoco sulla necessità che i clienti siano informati dell'esistenza del tag, che possa essere disattivato tramite un comando KILL e che sia data la possibilità agli utenti di verificare la disattivazione o più semplicemente dare loro la possibilità di rimuoverli fisicamente.

Il secondo punto riguarda le informazioni contenute nei tag. Nel caso di prodotti di largo consumo le informazioni nei tag sono codificate secondo EPC Gen2, ovvero il tag presente sui prodotti contiene solo un indicativo seriale. La pubblica opinione richiede che tali dispositivi siano "oscurabili" o semplicemente rimossi una volta varcate le casse del supermercato e/o negozio. Il terzo punto riguarda la possibilità di associare una persona ad un prodotto. È possibile che una persona male intenzionata possa leggere i codici dei tag dei prodotti che uno acquista a distanza e possa sapere le abitudini di consumo di ciascuna famiglia. Teoricamente questo sarebbe possibile

ispezionando la "spazzatura" di casa nostra o semplicemente accedendo alle banche dati legate alle innumerevoli carte fedeltà che normalmente sottoscriviamo.

Deve essere chiaro che il tag non detiene un identificativo del proprietario, tuttavia non è assolutamente impossibile potervi risalire.

Tuttavia ad una prima analisi tali preoccupazioni possono risultare esagerate considerate le distanze di lettura limitate.

Di fatto nel caso dei tag 13.56Mhz la distanza di lettura prevista è di 30 al più 60 cm mentre per i UHF, usati per la logistica, è di 6 - 10 metri

Inoltre i tag UHF non hanno buone prestazioni in prossimità di liquidi (pensate che il corpo umano è composto al 95% da liquidi) e quindi male si prestano per pedinare una persona. Per non parlare dei costi a cui bisogna andare in contro per realizzare un architettura RF-ID in grado di tracciare gli spostamenti di una persona, sicuramente è meno costoso seguire gli spostamenti tramite la triangolazione del GSM che disseminare il territorio di antenne di un valore Euro 3,000 ogni 10 metri.

È possibile leggere oltre i 10 metri alimentando le antenne oltre i 2 Watt, ma in tale caso si sta commettendo un crimine, di fatto occorre una licenza da parte del Ministero delle Telecomunicazioni oppure possono farlo agenti ed investigatori in quanto molto costoso e rischioso e non scalabile su una intera popolazione.

Il problema della privacy si pone realmente se ci sono dati sensibili residenti su CHIP RF-ID oltre al numero univoco del chip stesso, si pensi ad esempio ai passaporti o alle carte di credito contactless.

Tuttavia è chiaro che il semplice fatto che ogni RF-ID abbia un numero univoco lo renda di fatto un "braccialetto elettronico" con il quale è possibile tracciare gli spostamenti e le abitudini di una persona, nonché un pericolo per la sicurezza per la persona stessa, potendo essere seguita da malintenzionati dotati di lettore RFID. Nel terzo capitolo di fatto andrò ad approfondire il caso dei passaporti e delle carte di credito contactless che stanno entrando nella vita delle persone e che quotidianamente vengono utilizzate ignorando purtroppo i rischi a cui si va incontro.

Si è infatti dimostrato come questa nuova generazione di documenti elettronici, se pur rappresentano una forte innovazione , per via dei loro principi di funzionamento sono molto semplici da rintracciare e interrogare, e il fatto che spesso i dati vengano scritti

su tali supporti senza un minimo di crittografia permettono a malintenzionati di poterli scansionare e acquisire per poi riutilizzarli a completa insaputa del proprietario alimentando fenomeni di furto di identità e soprattutto borseggio elettronico.

Di fatto per quanto riguarda le carte di credito contactless si è riusciti in pochi secondi a rintracciare i dati della carta semplicemente avvicinando alla tasca dell'ignara vittima un banale smartphone equipaggiata di una piccola antenna e un'applicazione scaricabile sui principali player. Le soluzioni a contrasto di tali fenomeni esistono e vanno dalla banale schermatura delle carte di credito o passaporto acquistando dei speciali portafogli in grado di garantire tale protezione ai sofisticati algoritmi di crittografia che garantiscono integrità, riservatezza e autenticazione dei dati.

Con questo non voglio creare diffidenza in questa tecnologia, anzi voglio far capire come i sistemi RF-ID possono rivoluzionare realmente la nostra vita in meglio e basta leggere il secondo capito di questa tesi in cui passo in rassegna a solo alcuni casi d'uso reali o solo allo stato embrionale prototipale che semplificano e permettono di fare un passo in avanti in un modo sempre più smart, sicuro e dinamico.

C'è tuttavia un detto popolare molto comune che dice "fatta la legge, trovato l'inganno" se pur apparentemente può sembrare non appropriato a questo contesto in realtà il suo significato rende meglio l'idea di come ogni cosa presente tra noi che nasce con un fine nobile presto viene impropriamente convertita in un arma che può seriamente danneggiare la vita basti pensare alla bomba atomica, alle armi nucleari o batteriche, e di questo fenomeno purtroppo ne sa qualcosa la tecnologia un esempio fra tanti è internet e i social nati per unire e mettere in comunicazione virtuale gente sparsa in tutto il mondo e che è diventato terreno fertile per maniaci, truffatori, hacker generando nuovi crimini 2.0 quali furti di identità, pirateria informatica, cyber bullismo e tanto altro ancora ed è chiaro come i sistemi RF-ID non fanno eccezione.

Questo non deve però essere un pretesto per scoraggiarci e perdere ogni fiducia nel progresso tecnologico, ma al contrario deve essere uno stimolo per noi ingegneri ad ingegnarci nel trovare soluzioni a contrasto di questi comportamenti fraudolenti e per gli utenti finale un motivo in più per non prendere ogni cosa così come ci viene detta e data ma essere sempre critici e consapevoli di quello che ci accade intono e non chiuderci a riccio perché in fondo non tutto il male viene per nuocere.