



Tesina di Sicurezza su reti RFId: Sicurezza e Privatezza

di Buono Gaetano, Garofalo Tania

Prof. Alfredo De Santis

OUTLINE:

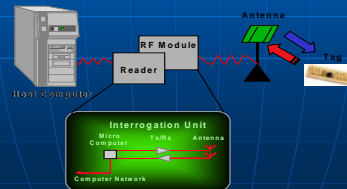
- Cos'è un RFId
- Componenti
- Classificazione RFId
- Integrità dei dati trasmessi
- Applicazioni
- Approcci per la protezione della Privacy

Cos'è un RFId ?

- **RFId** è l'acronimo di **Radio Frequency Identification**
 - (traducibile con **I**dentificazione a **r**adio **f**requenza)
- E' una tecnologia per la identificazione automatica di oggetti, animali o persone.
- Il sistema si basa sul leggere a distanza informazioni contenute in un tag RFId usando dei lettori RFId.

RFId: Componenti (1)

- RFId tag
- Reader o transceiver
- Sistema di elaborazione dati (PC) middleware server



RFId: Componenti (2)



Moderno tag con lettore



RFID Reader to RFID Tag: Up to 85 meters



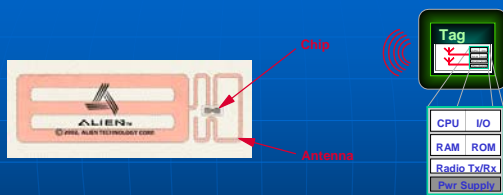
Combined RFID & Barcode

Il tag (1)

- Caratteristiche:
 - Dispositivo passivo
 - riceve energia dal lettore
 - Ha un range di diversi metri
 - è un "etichetta intelligente" che grida il suo nome e/o dato.



Il tag (2)



Costo = 0.05 €

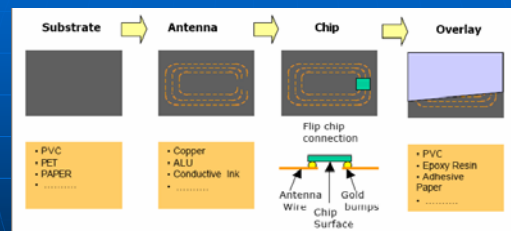
Le proprietà di un tag base

- Piccola memoria
 - Identificatore di 64-128 bit
- Piccola potenza computazionale
 - Diverse migliaia di porte
 - Non permette reali funzioni crittografiche

Tag RFID ulteriori caratteristiche

- Kill/disable
- Write once
- Write many
- Anti-collision
- Security and encryption
- Standards compliance

Tag RFID processo di assemblaggio



Formato dei Tag

- flessibili con forma di carta di credito
- forma di disco e moneta
- tag dedicati
 - modellati in supporti di plastica usati da contenitori
- tag duri con cassa di resina epossidica
- tag a forma di chiave

Tipi di Tag

- I transponder passivi
 - utilizzano l'onda a radio frequenza, generata dal lettore, sia come fonte di energia per alimentare il circuito integrato che per trasmettere e ricevere dati.
- I transponder semi-passivi
 - (backscatter assistito da batteria) hanno batterie incorporate e quindi non necessitano di alcuna energia proveniente dal campo del lettore per alimentare il circuito integrato
- I transponder attivi
 - autoalimentati da batteria e possiedono un trasmettitore attivo a bordo.
 - generano l'energia a radio frequenza trasmettendo autonomamente i dati.

I Tag

	Vantaggi	Svantaggi
Passivi	<ul style="list-style-type: none"> • Basso Costo • Tempi di vita più lunghi 	<ul style="list-style-type: none"> • Distanze limitate
Semi-Passivi	<ul style="list-style-type: none"> • Grande distanza di comunicazione 	<ul style="list-style-type: none"> • Costosi • Impossibile stabilire lo stato della batteria
Attivi	<ul style="list-style-type: none"> • Grande distanza di comunicazione 	<ul style="list-style-type: none"> • Costosi • Impossibile stabilire lo stato della batteria

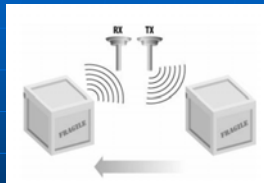
Il Lettore (1)

- Il lettore deve comunicare con i tag utilizzando RF (Radio Frequency)



Qualche esempio di lettore

Il Lettore (2)



- Alcuni lettori presentano due antenne
 - Una per ricevere dati
 - Una per trasmettere dati
- Il lettore deve inoltre interagire con il sistema di elaborazione dati mediante un protocollo
 - Bluetooth
 - Wireless
 - RS 232 o RS 422

Classificazione

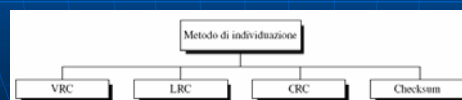
- Classifichiamo i sistemi RFID in base alle seguenti caratteristiche
 - Frequenza di lavoro
 - Raggio d'azione e quindi distanza massima di applicabilità.
 - Tipo di accoppiamento fisico

Integrità dei dati Trasmessi (1)

- Gli errori sono suddivisi in
 - errori single-bit (bit singolo)
 - multiple-bit (più bit)
 - burst (raffica)
- E' necessario introdurre metodi semplici ed efficaci per la loro individuazione:
 - doppio invio della medesima unità di dati
 - Al ricevente spetta il compito di confrontare bit per bit le due copie della stessa unità
 - Pregi: la trasmissione perfettamente affidabile, essendo infinitesima la probabilità di due errori sullo stesso bit
 - Difetti: tremendamente lenta.

Integrità dei dati Trasmessi (2)

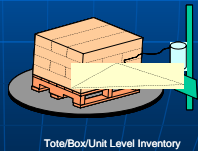
- non è necessario ripetere l'intera unità dati bensì:
 - aggiungere pochi bit scelti in modo opportuno.
 - questa tecnica è nota come ridondanza
- Esistono quattro diversi tipi di codici di controllo ridondanti



Applicazioni della tecnologia RFId (1)

■ Campi di applicazione

- Trasporti
- Militare
- Industriale
- Medico
- Automotive
- Altri



Applicazioni della tecnologia RFId (2)

■ Trasporti

- Gestione e controllo dei bagagli all'aeroporto
- Gestione della composizione del treno
- Bigliettazione elettronica e car sharing nel trasporto pubblico locale

■ Militare

- identificazione del veicolo militare
- identificazione materiale da guerra
- sigillo dei materiali da guerra e nucleare

Applicazioni della tecnologia RFId (3)

■ Industriale

- Catena di rifornimento

■ Medico

- Trasporto farmaceutico
- Controllo paziente

■ Automotive

- Identificazione veicoli in aree di parcheggio
- Accesso veicoli in autostrada
- Accesso controllato in zone a traffico limitato

Applicazioni della tecnologia RFId (4)

■ Altro

Marchatura Elettronica degli animali



Dispositivo di pagamento



Eventi Sportivi

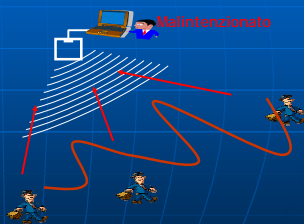


Problemi di privacy

■ Furto di dati personali



■ Tracciamento



Privatezza e Sicurezza



Due esigenze contrastanti

- Tutelare la *privacy*
- Identificare i beni non acquistati



RFId un pericolo per la privacy possibile scenario (1):

- La casalinga entra nel primo magazzino, acquista i beni usando la tessera punti ed esce.
- Il primo magazzino tiene traccia di
 - chi ha comprato cosa e quando
 - viene segnalato agli addetti di riempire gli scaffali
 - viene stimato quando questa persona avrà nuovamente bisogno di questi prodotti

RFId un pericolo per la privacy possibile scenario (2):

- Terminata la spesa al primo magazzino la casalinga entra nel secondo magazzino, apparecchiatura legge tutti i tag nelle buste
 - A questo punto:
 - nei tag è segnato il codice del prodotto
 - il sistema identifica i biscotti
 - nei tag non è scritto nulla, ma in maniera non legale il concorrente entra in possesso dei dati del primo magazzino ed attua le politiche commerciali
- i due magazzini si alleano e si scambiano le informazioni, se uno vende i biscotti, l'altro cerca di vendere il latte.

Approcci per la protezione della Privacy

- Uccisione dei Tag (The "Kill Tag")
- Gabbia di Faraday
- Disturbo intenzionale attivo
- Privacy bit
- "Smart" Tag RFId
 - il metodo Hash-lock
 - il metodo ri-cifratura (re-encryption)
 - il metodo Silent TreeWalking
- Protocollo singulation tree-walking
 - Blocker Tag

Uccisione dei Tag (The "Kill Tag")

Si cancella il tag RFId quando il prodotto esce dal negozio



Il consumatore rinuncia ai vantaggi della tecnologia
Non è utilizzabile per le banconote

Gabbia di Faraday

Un foglio metallico blocca la comunicazione con il lettore



Utile per i portafogli
Inappropriato per altri prodotti

Disturbo intenzionale attivo

Scopo: bloccare e/o disturbare l'operazione di ogni vicino lettore RFID.



Privacy bit

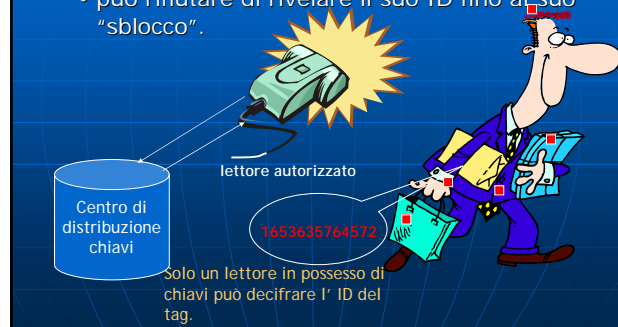
- Viene utilizzato un bit di privacy situato nella memoria di un tag RFID
 - fornisce informazioni sullo stato di privacy del tag.
 - Lo stato del bit di privacy ci informa se il tag può essere letto o meno.
- Esempio: Alice acquista un prodotto, all'uscita dal negozio il bit di privacy del tag RFID viene settato a true. Questo significa:
 - quel tag non può più essere letto.
 - Il settaggio del bit può essere eseguito soltanto da un lettore in possesso di un codice pin prestabilito.

"Smart" Tag RFID

- Consiste nel rendere i tag RFID più potenti
 - Aggiungendo funzionalità crittografiche
- Le istanze dell'approccio proposte sono:
 - il metodo Hash-lock
 - il metodo ri-cifratatura (re-encryption)
 - il metodo Silent TreeWalking

Metodo Hash-lock (1)

- un tag deve essere "locked"
 - può rifiutare di rivelare il suo ID fino al suo "sblocco".



Metodo Hash-lock (2)

- Quando il tag è bloccato gli viene assegnato un valore (o meta-ID)
- Il tag è sbloccato solo alla presentazione di una chiave x tale che:
 - $y = h(x)$ per una funzione hash standard one-way h .
 - La chiave x è posseduta dal lettore RFID
- Nell'esempio del supermercato, i tag devono essere bloccati una volta giunti alla cassa, in modo tale da
 - non fornire i dati una volta che il tag è fuori
 - Il cliente può sbloccare il tag mediante un pin, posto ad esempio sulle tessere fedeltà distribuite da molti supermercati.

Problemi

- Non è pratico gestire un insieme di PIN per il blocco/sblocco di tag
- I consumatori assocerebbero un PIN per un insieme di tag
 - rendendo il sistema Hash-lock più debole.

Metodo ri-cifratura (1)

- Arj Juels e R. Pappu (J&P) hanno ideato uno schema che impiega il crittosistema El-Gamal con
 - Una chiave pubblica P_k
 - Una chiave privata S_k mantenuta da una agenzia competente.
- Un tag RFID contiene un unico identificatore S
 - S contiene #seriale della banconota.
- S è codificato con la chiave pubblica P_k ottenendo un cifrato C
 - il tag RFID trasmette il cifrato C
 - solo l'agenzia sopra citata può decifrare C per ottenere S (testo in chiaro)

Metodo ri-cifratura (2)

- Per contrastare la tracciabilità J&P propongono che il testo cifrato C sia periodicamente ri-cifrato.
- Negozi e banche posseggono reader RFID che ri-cifrano con chiave pubblica P_k .
- Le proprietà algebriche del crittosistema El-Gamal
 - permettono di passare da C a C_1 (nuovo Cifrato) con
 - chiave pubblica P_k e svincolato dal testo di partenza
 - senza cambiamenti del testo in chiaro S

Metodo ri-cifratura (3)

- Per prevenire ri-codifiche arbitrarie
 - non tutti gli utenti possono ri-codificare i tag sulle banconote.
- J&P propongono che le banconote contengano il pin che consente l'accesso in scrittura del tag RFID
 - per leggere tale pin occorre uno scanner.
- Riepilogando:
 - per ri-cifrare un tag occorre:
 - Chiave pubblica P_k
 - Scanner capace di leggere il pin dalla banconota.
 - pin (per l'accesso in scrittura, letto dallo scanner)

Metodo Silent TreeWalking (1)

- Questo metodo illustra come rendere "silenzioso" il protocollo singulation tree-walking esaminato nelle slides successive.
- Essendo un metodo che utilizza tag intelligenti ("Smart ") è stato trattato in questa sezione.

Metodo Silent TreeWalking (2)

- La minaccia del sistema è:
 - La presenza di una spia che ascolta la trasmissione broadcast del lettore di tag.
 - La trasmissione può essere catturata da centinaia di metri.
- Stephen A. Weis suggerisce di cifrare la trasmissione dei lettori, così che una spia non possa capire le ID che vengono lette
Questo sistema
 - non difende da attacchi attivi (attacchi il cui obiettivo è alterare o danneggiare le informazioni)

Protocollo singulation tree-walking (1)

- Un lettore RFID è abilitato a comunicare con un solo RFID alla volta, quando più tag rispondono all'interrogazione contemporaneamente il lettore RFID rileva una collisione.
- Occorre un protocollo di ordinamento che permette al lettore RFID di comunicare con un tag alla volta
 - Protocollo singulation tree-walking

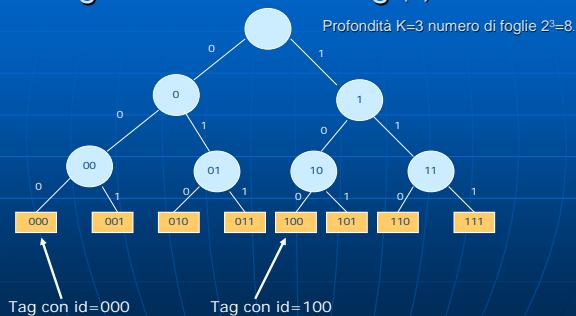
Protocollo singulation tree-walking (2)

- Consideriamo un albero binario completo di profondità k
 - Il ramo sinistro ed il ramo destro di ciascun nodo sono etichettati rispettivamente con '0' ed '1'.
- La radice di questo albero ha profondità 0 ed è etichettata con la stringa vuota
- Un nodo a profondità d in questo albero è identificato mediante un prefisso binario $B=b_1b_2\dots b_d$
 - rappresentante la sequenza di etichette dei rami attraversati nella path che va dalla radice al nodo

Protocollo singulation tree-walking (3)

- Se $d < k$ allora il nodo ha due figli a profondità $d+1$
 - etichettati con $B||0$ e $B||1$ rispettivamente:
 - Figlio sinistro e figlio destro
 - $||$ indica l'operazione di concatenazione
- Le 2^k foglie dell'albero hanno associate un'etichetta di k bit che rappresenta il numero seriale del tag.
- La figura seguente mostra ciò che è stato detto.

Protocollo singulation tree-walking (4): L'albero



Protocollo singulation tree-walking (5)

- Supponiamo che stiamo cercando i tag aventi i numeri di serie con prefisso $B= b_1b_2\dots b_d$.
- Il lettore parte da un nodo con etichetta B , richiede il $d+1$ esimo bit
 - tutti i tag il cui numero seriale contiene il prefisso B rispondono al lettore con il bit $d+1$.
 - tutti gli altri tag rimangono in silenzio.

Protocollo singulation tree-walking (6)

- Ogni tag trasmette uno "0" se si trova nel sottoalbero sinistro del nodo B , ed "1" se si trova nel sottoalbero destro del nodo B
- Un caso particolare:
 - I tag in entrambi i sottoalberi di B rispondono simultaneamente con
 - uno "0" ed un "1", creando una collisione nella trasmissione del bit
 - In tal caso il lettore riprende ricorsivamente la ricerca con una nuova interrogazione a partire da $B||0$ e successivamente da $B||1$.
 - DFS ricorsiva, (Visita in profondità).

Protocollo singulation tree-walking (7)

- Se invece i tag rispondono tutti con uno stesso bit b , allora risiedono tutti nello stesso sottoalbero
 - in tal caso il lettore riparte dal nodo $B||b$, ignorando gli altri sottoalberi.
- Quando l'algoritmo raggiunge una foglia (a profondità k) restituisce in output l'etichetta di k bit ad essa associata.

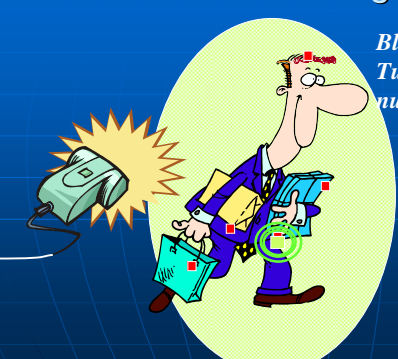
Protocollo singulation tree-walking (8): Running time

- Per leggere un tag il lettore RFID deve contattare al più k nodi per chiedergli il bit successivo.
 - Poiché l'albero ha profondità k .
- Alla fine dell'algoritmo il lettore RFID ha letto un certo numero di tag.
- Il running time dell'algoritmo è limitato superiormente dal prodotto di k ed il numero di tag letti dal lettore RFID.

Le Zone

- Tutti i tag che condividono lo stesso prefisso risiedono nello stesso sottoalbero
 - esempio tutti i prodotti fabbricati dalla stessa ditta condividono lo stesso prefisso e quindi lo stesso sottoalbero
- Generalmente differenti prefissi di ID possono corrispondere a differenti zone (o sottoalberi)
 - Esempio
 - tutte le ID inizianti per 1 identificano la privacy zone (zona in cui non è possibile interrogare i tag RFID)
 - tutte le ID inizianti per "010" identificano la zona di carico/scarico merci

Blocker Tag



Blocker tag simula Tutti i possibili serial number dei tag!!

Blocker tag in pratica (1)

- Un blocker tag è un tag con capacità computazionali superiori ad uno normale
 - esso è programmato per simulare tutto l'insieme dei 2^k possibili numeri seriali dei tag RFID
- Il protocollo "singulation tree-walking" per l'identificazione dei tag chiede ricorsivamente:
 - "Qual è il tuo prossimo bit?"

Blocker tag in pratica (2)

- Il blocker tag risponde sempre con entrambi 0 ed 1
 - creando una collisione
- Il lettore RFID non riesce a capire quali tag sono effettivamente presenti
- Questa collisione forzata porta il lettore RFID ad eseguire una ricorsione su tutti i nodi causando l'esplorazione dell'intero albero.
- Il numero di tutti i tag è enorme ed il lettore RFID va in stallo

Blocker tag in pratica (3)

- Un blocker tag che si comporta come descritto prende il nome di "full blocker".
- Un blocker tag può far credere che elementi rubati siano ancora presenti in magazzino.
- Il blocker tag può essere utilizzato in modo tale da simulare e bloccare effettivamente solo un sottoinsieme di tag
 - chiamiamo un simile blocker tag "blocker parziale" o anche "blocker selettivo".

Blocker tag in pratica (4)

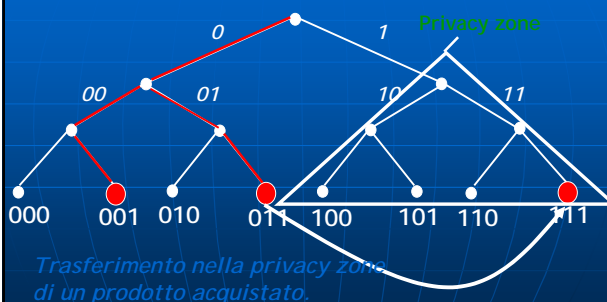
- Questa caratteristica di bloccaggio selettivo può essere usata ad esempio per impedire la lettura dei tag aventi:
 - il prefisso '0' nel suo numero seriale
 - i tag iniziati con un '1' possono essere letti senza interferenza.
- In questo modo possiamo mirare ad una particolare zona per proteggerla.

Esempio

Prendiamo ad esempio un supermarket assumiamo che:

- I tag hanno un bit di privacy (primo bit a sinistra)
- Tutti gli elementi nella privacy zone hanno privacy bit settato a true
 - la privacy zone è la zona in cui non è possibile interrogare i tag RFID
- I prodotti nel supermarket hanno il bit di privacy a false.
- Quando un prodotto viene venduto il bit viene settato a true.
 - Per settare il bit di privacy è richiesto un pin.

Blocking with privacy zones



Link Visitati (1)

- [RSA Laboratories](#)
 - Articoli analizzati:
 - RFID Privacy: A Technical Primer for the Non-Technical Reader
 - RFID Security and Privacy: A Research Survey
 - The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy
 - RFID Privacy: An Overview of Problems and Proposed Solutions

Link Visitati (2)

- [RFID Journal](#): in cui è possibile reperire articoli su nuove applicazioni degli RFID.