Università degli Studi di Perugia

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Informatica

Seminario di Sicurezza Informatica

Autenticazione dei dispositivi RFID

Studenti:
Marco Bizzarri
Andrea Lauri

Professore:
Stefano Bistarelli

Anno Accademico 2010/2011

Indice

1 Dispositivi RFID

In questo elaborato parleremo della tecnologia RFID (Radio Frequency IDetification), introducendone i principali aspetti e puntando maggiormente l'attenzione sulla sicurezza e sulle tecniche di autenticazione.

Un RFID (Radio Frequency IDetification) è un sistema di identicazione automatica a radiofrequenza. Esso è costituito da un chip elettronico chiamato transponder o tag, dotato di memoria interna e da un'antenna e da un reader a radiofrequenza che permette l'interfacciamento a distanza con il tag e la lettura delle informazioni contenute nella sua memoria.

1.1 Struttura RFID

I Transponder, a seconda del campo di applicazione, assumono forma, dimensione e caratteristiche diverse rappresentate dal tipo di alimentazione e dalle frequenze di utilizzo.

Passivi: è il tipo di Tag più diffuso ed economico, non necessita di alimentazione propria, ma utilizza le onde elettromagnetiche che riceve dal reader. Questo Transponder non può quindi avviare una comunicazione spontaneamente. Il range di azione è limitato, nella migliore delle ipotesi riesce a raggiungere qualche metro.

Attivi: dotati di una propria sorgente di alimentazione (batteria), possono quindi emettere segnale. Spesso hanno un elevato range di comunicazione e

generalmente possiedono una memoria RAM piuttosto grande (nell'ordine del KiloByte).

Semi-Passivi: presentano caratteristiche comuni sia ai Tag passivi che a quelli attivi, hanno una batteria interna che permette di eseguire alcune operazioni di controllo (controllo potenza, monitoraggio ambiente, ecc.), ma necessitano dell'alimentazione del reader per la trasmissione dei messaggi.

In base al tipo di tag ed alla memoria interna possono essere utilizzati in diverse modalità:

Read-Only: il reader può accedere alla memoria del tag in sola lettura. I tag passivi sono di solito di questo tipo.

Write-Once e Read-Many: è possibile scrivere una sola volta nella memoria del tag, dopodiché la sua memoria è accessibile in sola lettura.

Read e Write: la memoria è accessibile il lettura e scrittura, la dimensione è nell'ordine di qualche KiloByte. I tag attivi sono di solito di questo tipo ed il loro costo è maggiore.

Un'ulteriore classificazione è data dalla frequenza che ne determinerà anche la tipologia delle possibili applicazioni. I range possibili di frequenze ed alcuni esempi di applicazioni vengono mostrati in Fig.1.1.

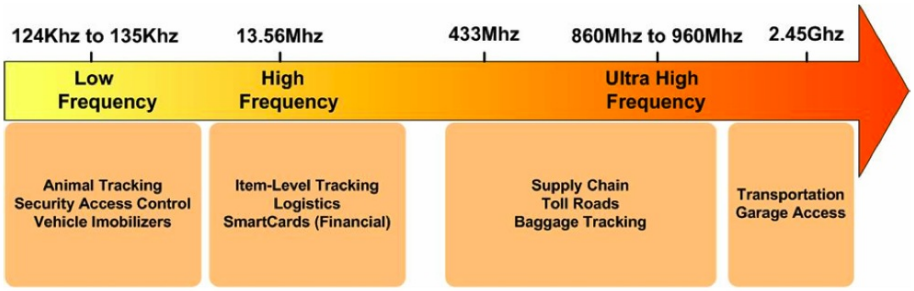

Figura 1.1: *Frequenze e bande.*

1.2 Applicazioni

I sistemi RFID possono essere utilizzati in una vasta gamma di settori. Di seguito alcuni esempi:

- Monetica:
  - nuove carte di credito e pagamento o borsellini elettronici;
  - acquisto di biglietti della metro;
  - villaggi turistici.
- Biglietteria elettronica:
  - accesso a mezzi di trasporto ("contactless card"), in modo tale che non sia più necessario il terminale P.O.S.;
  - ski-lift.
- Trasporti:
  - identificazione di persone, come nel caso di documento elettronico identificativo del conducente ovvero di persone trasportate;
  - identificazione della merce;
  - per effettuare l'inventario in real-time;
  - associazione bagaglio-passeggero in aeroporto.
- Inventario dei libri nelle biblioteche:
  - identificazione e localizzazione dei libri;
  - servizio di prestito.
- Sicurezza agro-alimentare:
  - identificazione del prodotto;
  - identificazione dell'animale.
- Ambito lavorativo:
  - i tag possono essere utilizzati per assicurare lintegrità fisica e lincolumità delle persone (ad esempio disattivando i macchinari in presenza di personale non autorizzato).
  - si sostituiscono i tag sia ai badge magnetici che ai tesserini di riconoscimento.

- Gestione dei rifiuti e protezione ambientale:
  - i tag in radiofrequenza possono essere inseriti in cassonetti della spazzatura, in modo tale da registrarne e identificarne il peso a partire dall'ID specifico della zona di pertinenza.
- Controllo degli accessi:
  - sostituzione delle chiavi standard (ad esempio autovetture).
- Sicurezza all'interno degli esercizi commerciali:
  - il tag pu rivelarsi utile quale dispositivo anti-taccheggio in sostituzione dei dispositivi magnetici, cosí da riconoscere quali e quanti prodotti sono usciti.

1.3 Problematiche riguardanti la sicurezza dei sistemi RFID

L'introduzione dei dispositivi a radio frequenza possono portare a delle problematiche riguardanti la sicurezza nello scambio di informazioni e la privacy degli utenti.

Le minacce possono riguardare:

attacchi alla riservatezza ed alla privacy: le etichette potrebbero essere lette da qualsiasi reader non autorizzato.

Scenari di attacco: se in prossimità di un reader, è possibile tracciare i luoghi che una persona frequenta in un dato momento, riuscendo a capirne le proprie abitudini.

attacchi di spoofing e clonazione: i tag possono essere clonati. È anche possibile modificare il contenuto dei tag riscrivibili.

Scenari di attacco: modifiche nei documenti per falsificarli, modifiche nei tag dei prodotti in commercio, furto automobili, ecc.

attacchi Denial of Service: i tag possono essere distrutti, rimossi o cancellati. I lettori possono essere disturbati in radio frequenza.

Scenari di attacco: distruzione, rimozione o riprogrammazione di tag negli esercizi commerciali, utilizzo disturbatori di frequenza per nascondere denaro sporco o di un oggetto rubato.

malware: di solito i sistemi RFID interagiscono con altri sistemi informatici, quindi le informazioni lette non sono altro che nuovi input da validare.

Scenari di attacco: Buffer OverFlow, SQL Injection, Virus.

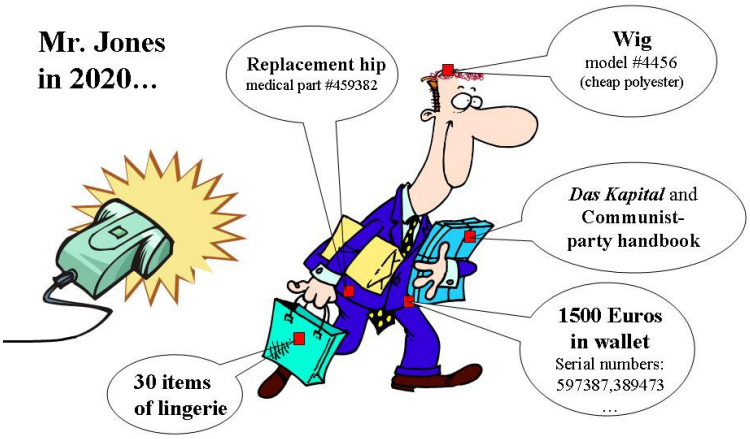

Figura 1.2: *Problema della Privacy.*

1.4 Contromisure

A fronte delle suddette minacce e vulnerabilità, specifiche contromisure possono essere rappresentate da:

software anti-virus: in grado di proteggere il lettore;

crittografia: il tipo di crittografia più utilizzato è quello a chiave simmetrica vista la scarsa capacità computazionale dei transponder;

proxying: un dispositivo di controllo per mezzo del quale il tag riesce a riconoscere i reader autorizzati attraverso l'analisi e la memorizzazione preventiva delle sue specifiche;

distanza di sicurezza: alcuni tag sono settati per essere letti solamente ad una specifica distanza;

autenticazione: particolarmente utile a prevenire i rischi di clonazione di tag o altre forme di alterazione e falsificazione dei dati.

1.5 Autenticazione

L'autenticazione nei sistemi RFID è il procedimento con il quale tag e reader dimostrano cioè di essere dispositivi legittimi. Sorgono dei problemi quando reader legittimi vogliono raccogliere informazioni da tag non legittimi e vice versa, in particolare da quelli contraffatti. La duplicazione di dispositivi non protetti è piuttosto semplice e richiede di effettuare uno scanning del tag e la sua successiva duplicazione. L'approccio più generico e sicuro è l'uso di protocolli di autenticazione già largamente usati nelle reti o nelle smart cards. Esistono diversi protocolli di autenticazione standard, tuttavia gran parte delle aziende preferiscono usare dei loro sistemi di autenticazione proprietari.

1.5.1 Tecniche di Autenticazione

I metodi di autenticazione nei sistemi RFID possono essere raggruppati in tre principali categorie:

- password systems
- Challenge-Response
- Zero-Knowledge

I sistemi basati su password offrono il tipo di autenticazione piú debole mentre i metodi zero-knowledge sono generalmente basati su problemi matematici difficili da calcolare ed implementare, quindi concentreremo l'attenzione sui metodi challenge-response (sfida-risposta) che sono quelli maggiormente utilizzati. Questi metodi basano il processo di autenticazione su uno scambio di informazione reciproca tra tag e reader a cui si aggiungono spesso tecniche di crittografia sia a chiave simmetrica che asimmetrica.

Normalmente la prima tecnica é la piú usata vista la minore capacitá computazionale richiesta dato che i sistemi RFID hanno generalmente un hardware poco performante a causa delle dimensioni estremamente limitate dei tag.

L'autenticazione a chiave simmetrica puó quindi essere effettuata con un algoritmo di cifratura a chiave privata o puó essere basato su una funzione hash con chiave.

Di seguito descriveremo alcuni dei protocolli standard di tipo challenge-response più utilizzati per l'autenticazione che sono definiti dallo standard ISO 9798-2.

Crittografia minimalista (Kill-Pin)

Il primo protocollo mostra una tecnica di crittografia poco espansiva, definita minimalista che viene applicata su tag Low-Cost.

Con il termine "minimalista" si intende l'uso di operazioni crittografiche estremamente semplici, come lo *XOR Esclusivo* e comparazione di stringhe. Questo schema si basa sullo **Pseudonym throttling** dove tag e reader conservano una lista degli identificatori utilizzati come chiavi di autenticazione.

Il protocollo è basato su una mutua autenticazione e presenta tre liste di pseudonimi dove ognuno ricopre un ben preciso ruolo.

α**:** ogni suo elemento serve ad avviare la procedura;

β**:** ogni suo elemento serve per autenticare il reader al tag;

γ**:** ogni suo elemento serve ad autenticare il tag al reader.

Tale sistema per essere efficiente necessita che sia il tag che il reader si trasmettano sempre gli stessi valori, per ovviare quindi a questo problema i singoli elementi vengono aggiornati utilizzando delle chiavi *one-time pad* che il reader crea e trasmette al tag nelle varie sessioni di autenticazione. Questo rende impossibile un eventuale attacco in quanto non si conosco i valori della sessione successiva.

Vediamo uno schema dettagliato di questo protocollo come mostrato in Fig.1.3.

Il sistema è abbastanza efficiente anche se con alcune pecche; ogni comunicazione richiede la trasmissione di 3kl bit, dove l è la lunghezza dei pad e k il

Tag		**Reader**
$d \leftarrow (c \bmod k) + 1$ $c \leftarrow c + 1$ $\alpha' \leftarrow \alpha_d$	$\xrightarrow{\alpha'}$	Se è un valido pseudonimo per un dato tag T_x, allora: $i \in \{1,2,...k\}$ Seleziona un α' non è piu valido $tag \leftarrow x$ $\beta' \leftarrow \beta_i$ $\gamma \leftarrow \gamma_i$ Altrimenti Autenticazione fallita
Se $\beta' \neq \beta_d$ allora Autenticazione fallita Altrimenti $\gamma' = \gamma_d$	$\xleftarrow{\beta'}$ $\xrightarrow{\gamma'}$	Se $\gamma' \neq \gamma$ o $\gamma' = \perp$ allora Autenticazione fallita Altrimenti Genera il nuovo insieme di pad $\widetilde{\Delta}_k$ **Autenticazione Riuscita**
Aggiorna $(\Delta_k, \widetilde{\Delta}_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$ $\kappa \leftarrow \kappa \oplus livepad(\Delta_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$	$\xleftarrow{\widetilde{\Delta}_k}$	Aggiorna $(\Delta_k, \widetilde{\Delta}_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$ $\kappa \leftarrow \kappa \oplus livepad(\Delta_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$

Figura 1.3: *Schema protocollo Crittografia Minimalista.*

numero degli pseudonimi, un attaccante che riesce ad inserirsi nell'ultima fase del protocollo e ad inviare falsi one-time pad al tag può provocare Denial of Service ed infine i vari pseudonimi non sono riutilizzabili.

Tag senza Crittografia Estensiva

Questo tipo di protocollo utilizza delle semplici operazioni tra matrici. In un sistema RFID, ogni tag memorizza una coppia di matrici quadrate M_1 e M_2^{-1} di dimensione p x p e il reader mantiene le inverse delle due matrici. Inoltre tag e reader condividono una chiave K di dimensione rp dove r è un fattore intero (generalmente indica il numero di tag presenti nel sistema).

La chiave K deve essere scelta in modo che il prodotto $X = K_i M_i$ sia unico per ogni $1 < i <$ r. Ad ogni sessione di autenticazione viene usata, da tag e reader, l'i-esima componente del vettore K, dove $1 < i < r$.

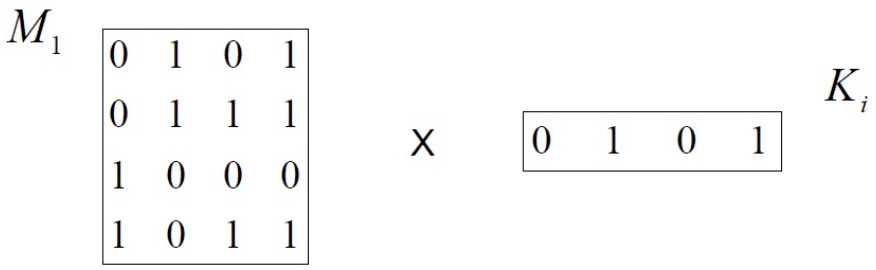

Figura 1.4: *Moltiplicazione matrice-vettore del protocollo.*

Come lavora il protocollo è mostrato in Fig.1.5

La sicurezza del metodo sta nel riuscire a mantenere segrete le matrici e le loro inverse, dato che queste non vengono mai trasmesse. Questo rende il protocollo sicuro ad attacchi **known-ciphertext**, il che è una buona garanzia per i sistemi RFID. Un avversario non può nemmeno tracciare il tag in quanto non sa quale si stia autenticando al momento. Inoltre non può decodificare le comunicazioni (non conosce le matrici).

1.5.2 Autenticazione forte con AES

Questo protocollo é basato sull'algoritmo di cifratura AES (Advanced Encryption Standard), diventato lo standard nel 2001, dato il suo elevato livello di

Reader		**Tag**
Invia un messaggio di inizio sessione. Il messaggio potrebbe contenere il valore *i*.	hello, *i* →	Preso *i*, calcola: $X \leftarrow K_i M_1$ Avvia il timer
Identifica ed autentica il tag in base al valore di X $K_i = XM_1^{-1}$ Genera la nuova chiave K_{new} di taglia *p* Calcola: $Y \leftarrow (K_1 \oplus K_2 \oplus ... \oplus K_r)M_2$ $Z \leftarrow K_{new} M_2$	← X	
	Y, Z →	Ferma il timer Autentica il reader calcolando: $YM_2^{-1} = (K_1 \oplus K_2 \oplus ... \oplus K_r)$ Recupera la nuova chiave calcolando: $K_{new} \leftarrow ZM_2^{-1}$

Figura 1.5: *Schema protocollo Tag senza Crittografia Estensiva.*

sicurezza e la sua facile implementazione sull'hardware dei dispositivi RFID.

La sicurezza del protocollo é garantita dall'algoritmo di cifratura utilizzato e funziona correttamente sia per l'autenticazione unilaterale che per la mutua autenticazione.

Autenticazione unilaterale

Vediamo come il protocollo lavora con questo tipo di autenticazione:

- il reader invia al tag un numero casuale r_B;
- il tag lo cifra con la chiave condivisa K e rimanda il risultato al reader.

A questo punto il reader pu facilmente decifrare il valore, confrontarlo con quello di partenza e attestare l'identit del tag.

Reader -> Tag	:	C_1
Tag -> Reader	:	$R_1 = e_K(C_1)$
Reader	:	If $d_K(R_1) = C_1$ Autenticazione riuscita

Figura 1.6: *Algoritmo AES unilaterale.*

Mutua autenticazione

Il protocollo per la mutua autenticazione analogo:

- il reader invia al tag un numero casuale r_B;
- il tag lo cifra con la chiave K, cifra un altro numero causale r_A da lui generato ed invia la coppia al reader;
- Il reader, una volta verificata l'identit del tag, scambia la sequenza dei numeri random li cifra con la chiave K e li rimanda al tag.

A questo punto tag e reader sono autenticati a vicenda.

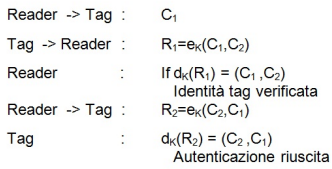

Figura 1.7: *Algoritmo AES con mutua autenticazione.*

Questo metodo di autenticazione é particolarmente adatti in sistemi chiusi dove ogni componente pu essere controllato da un dispositivo centrale (es: controllo bagagli in aeroporto, spedizioni). In applicazioni in cui non epresente una componente centrale ma le componenti possono essere cambiate in modo dinamico, la distribuzione e la gestione delle chiavi risulta piú complessa.

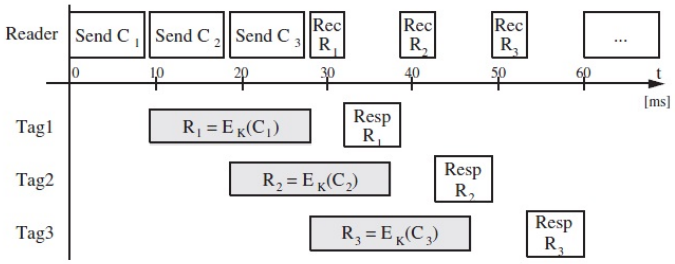

Figura 1.8: *Schema di autenticazione multipla.*

Bibliografia

[1] **Strong Authentication for RFID Systems Using the AES Algorithm** di Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer

[2] **www.rfidguru.eu**

[3] **RFID Viruses and Worms** di Melanie R. Rieback, Patrick N. D. Simpson, Bruno Crispo, Andrew S. Tanenbaum

[4] **RFID Security and Privacy: A Research Survey** di Ari Juels del RSA Laboratories

[5] **www.rfid.org**

[6] **www.rfidjournal.com**

[7] **RFID Systems and Security and Privacy Implications** di Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels

[8] **An Introduction to RFID Technology** di Roy Want, Intel Research

[9] **RFID: A Technical Overview and its Application to the Enterprice** di Ron Weinstein, Johns Hopkins University