Università degli Studi di Perugia
Facoltà di Scienze MM.FF.NN.
Corso di Laurea in Informatica

Autenticazione nei sistemi RFID

Studenti:

Marco Bizzarri

Andrea Lauri

Professore:

Stefano Bistarelli

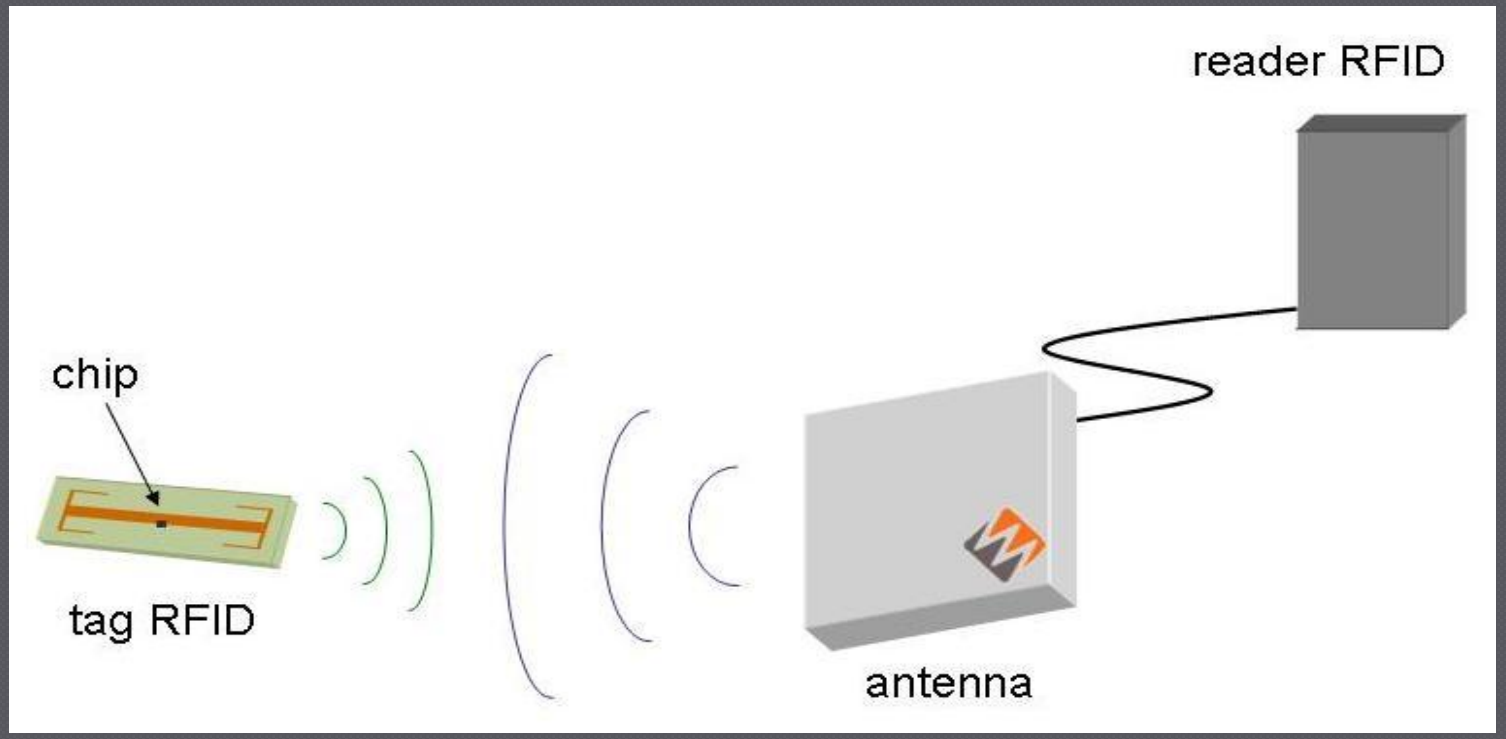
ANNO ACCADEMICO 2010/2011

Sommario

- Introduzione
- Struttura
- Campi di applicazione
- Problematiche di sicurezza
- Autenticazione

Introduzione: cos'è un RFID

RFID (Radio Frequency IDentification):
sistema di identificazione automatica a radiofrequenza

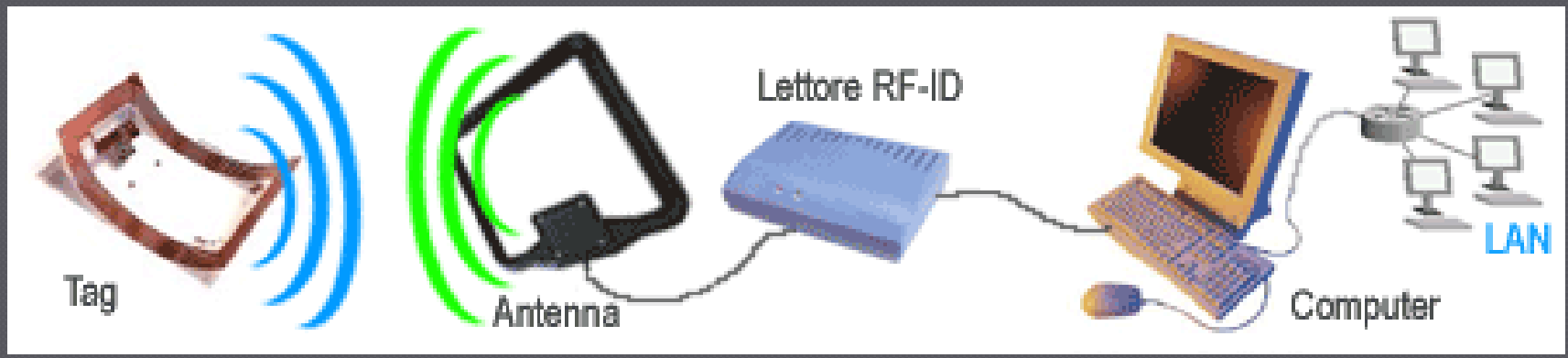


Struttura

Tag (Transponder)

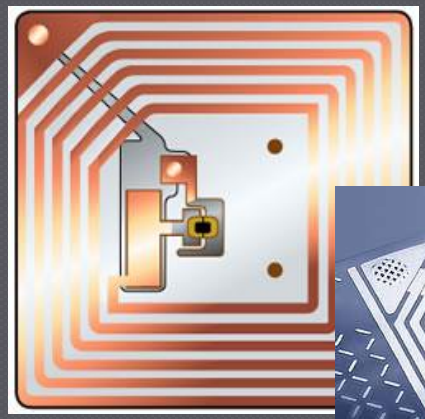
Reader

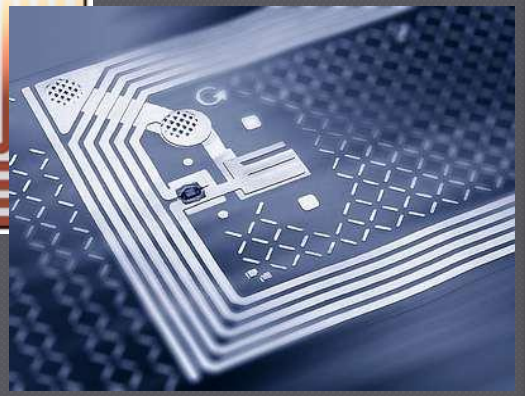
Sistema informatico

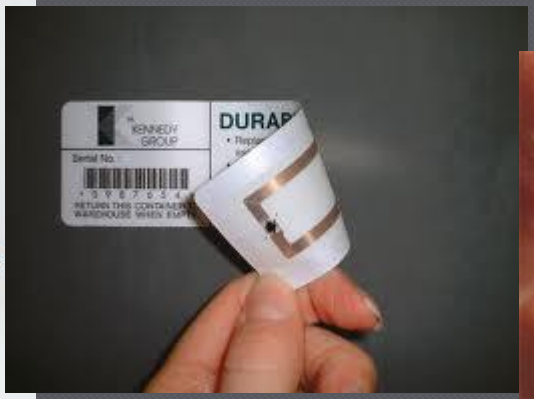


Struttura: tipologie di Tag

- Passivi
- Attivi
- Semi-passivi







Struttura: tipologie di Tag

Struttura: modalità di utilizzo

- Read-Only

  solo lettura, di solito passivi

- Write-Once e Read-Many

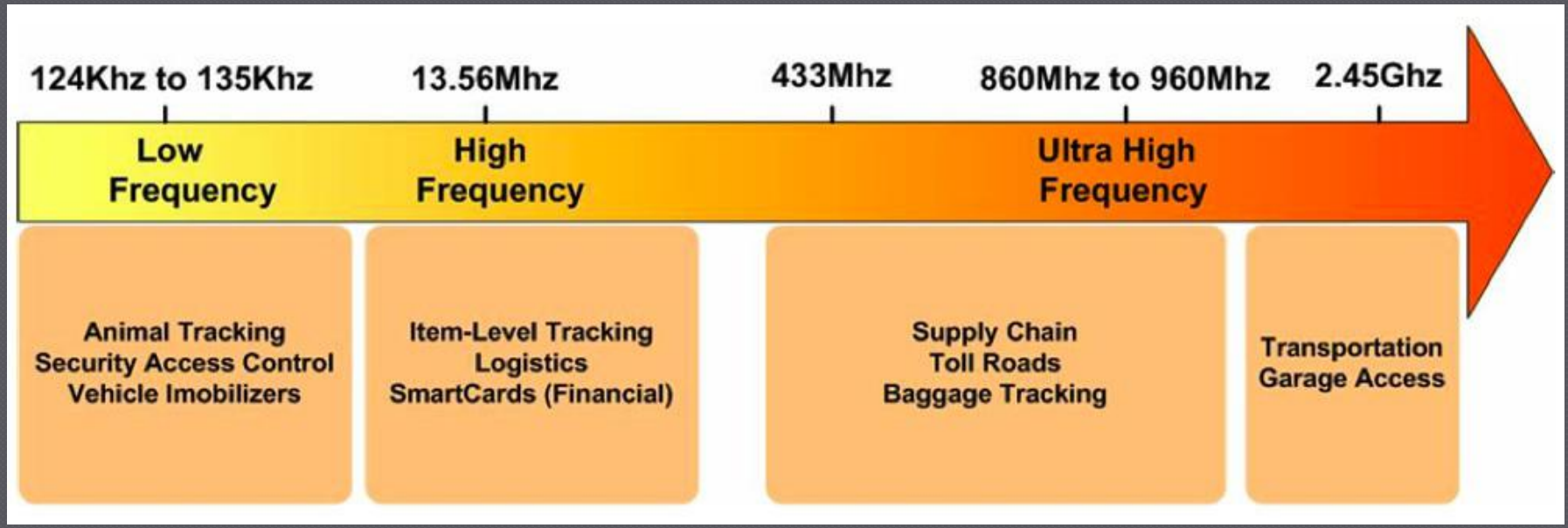
  scrivibili una sola volta

- Read and Write

  accessibili in R/W, memoria di maggiore dimensione, di solito attivi

Struttura: frequenze di utilizzo

In base alle frequenze varia il campo di applicazione



Struttura: reader

Struttura: applicazioni

Pagamenti e biglietteria elettronica

- Carte di credito
- Parcheggi
- Biglietti mezzi di trasporto
- Telepass
- Sky-lift

Struttura: applicazioni

Trasporti e viaggi

- Identificazione merce
- Inventario real-time
- Tracciamento bagagli
- Associazione bagaglio-passeggero

Struttura: applicazioni

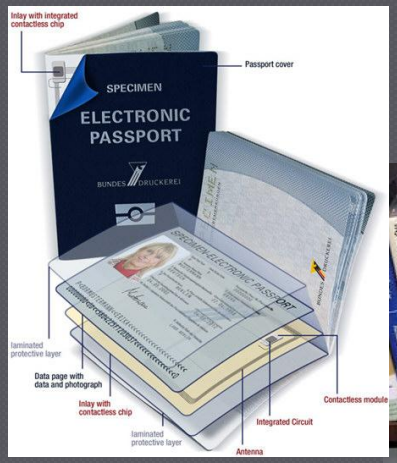
Aziende

- Gestione degli accessi
- Sicurezza sul lavoro

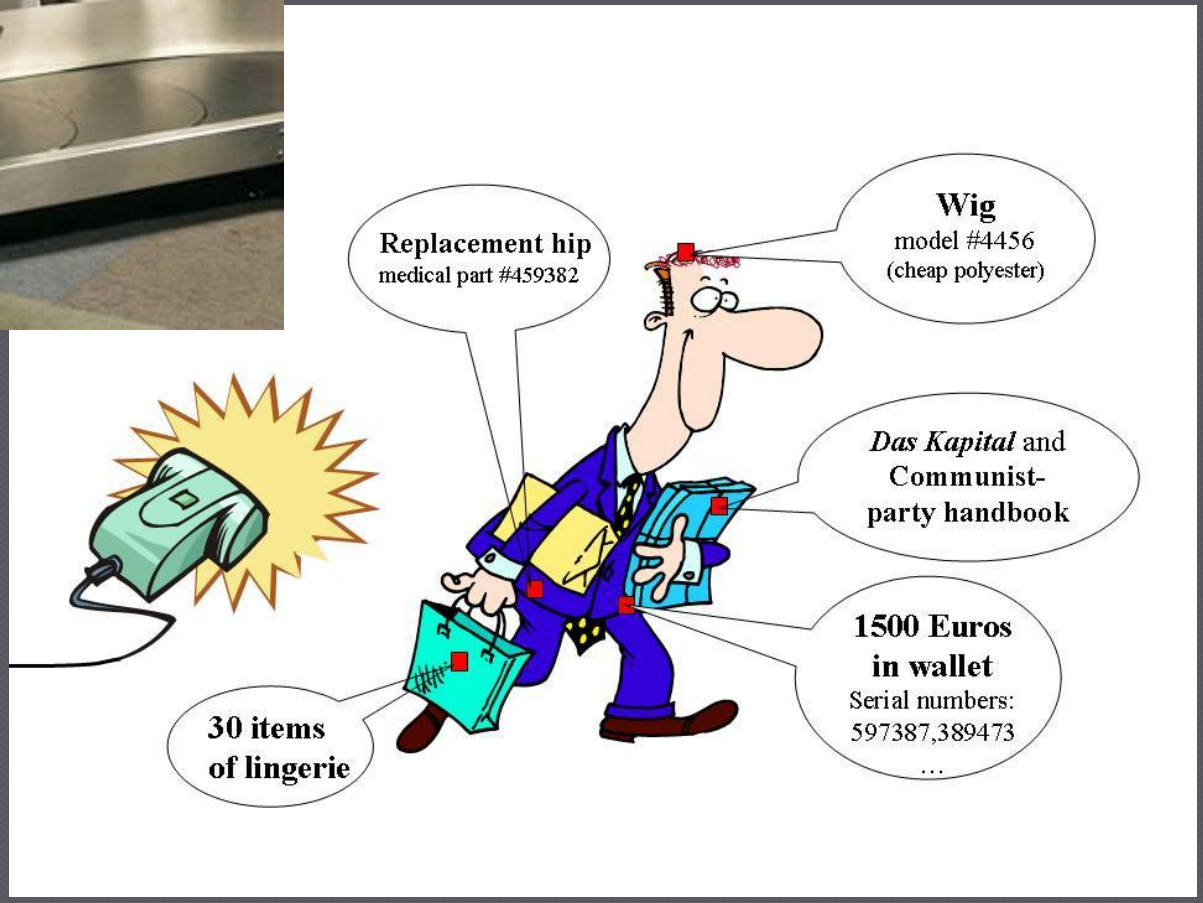
Struttura: applicazioni

Altro

- Documenti
- Biblioteche
- Medicina
- Ambito agro-alimentare
- Sostituzione chiavi
- Esercizi commerciali
- ...



Sicurezza e privacy



Sicurezza e privacy

Scenari di attacco

- Riservatezza e privacy
- Spoofing e clonazione
- Denial of service
- Malware

Sicurezza e privacy

Contromisure

- Software antivirus
- Crittografia
- Proxying
- Distanza di sicurezza
- Autenticazione

Autenticazione

Processo tramite il quale tag e reader dimostrano di essere dispositivi legittimi

Esitono diversi protocolli standard ma la maggior parte delle aziende preferisce utilizzare metodi proprietari

Principali metodi di autenticazione

- Password based (debole)
- Zero-knowledge (ISO 9798-5)
- Challenge-response (ISO 9798-2)

Autenticazione

Challenge-response (ISO 9798-2)

Protocolli di autenticazione basati sulla comunicazione reciproca di informazioni, spesso abbinati a tecniche di crittografia (simmetrica o asimmetrica).

- Kill-pin con crittografia minimalista
- Metodo delle matrici
- Autenticazione con AES

Autenticazione

Kill-pin con crittografia minimalista

Applicata su tag low-cost
Tecnica di crittografia molto semplice (XOR)
Utilizza pseudonimi come chiave di autenticazione

Il protocollo è basato su una mutua autenticazione. Vi sono tre liste di pseudonimi, che hanno dei compiti ben definiti:

- { α } avvia la procedura
- { β } autentica il reader al tag
- { γ } autentica il tag al reader

Autenticazione

Kill-pin con crittografia minimalista

Tag		Reader
$d \leftarrow (c \bmod k) + 1$ $c \leftarrow c + 1$ $\alpha' \leftarrow \alpha_d$	α' →	Se α' 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 $\gamma' = \gamma_d$	← β' γ' →	Se $\gamma' \neq \gamma$ o $\gamma' = \perp$ allora Autenticazione fallita Altrimenti Genera il nuovo insieme di pad $\tilde{\Delta}_k$ **Autenticazione Riuscita**
Aggiorna $(\Delta_k, \tilde{\Delta}_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$ $\kappa \leftarrow \kappa \oplus livepad(\Delta_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$	← $\tilde{\Delta}_k$	Aggiorna $(\Delta_k, \tilde{\Delta}_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$ $\kappa \leftarrow \kappa \oplus livepad(\Delta_k)$ $\forall \kappa \in \{\alpha\}\{\beta\}\{\gamma\}$

Autenticazione

Kill-pin con crittografia minimalista

Il sistema è efficiente ma ha alcuni svantaggi

- Quantità di informazioni da trasmettere elevata
- Un attaccante capace di inserirsi nell'ultima fase del protocollo e di inviare falsi one-time pad al tag, potrebbe causare un Denial of service
- Uno pseudonimo α_i è utilizzabile una sola volta per sessione

Autenticazione

Metodo delle matrici

Il processo di autenticazione in questo protocollo non usa algoritmi o sistemi crittografici, ma semplici operazioni di prodotti tra matrici

Il tag ha in memoria una coppia di matrici:

$$M_1 , M_2^{-1} \text{ di dimensione } p \text{ x } p$$

Il reader memorizza le loro inverse:

$$M_2 , M_1^{-1}$$

Tag e reader condividono una chiave *K* di dimensione *rp*
K deve essere scelta in modo che il prodotto $X = K_i * M_1$ sia unico per ogni $1 < i < r$.

Autenticazione

Metodo delle matrici

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: $K_{new} \leftarrow ZM_2^{-1}$

Autenticazione

Metodo delle matrici

• La sicurezza del metodo sta nel riuscire a mantenere segrete le matrici e le loro inverse visto che non vengono mai trasmesse

• Protocollo sicuro ad attacchi *known-ciphertext*

Svantaggi:

- Quantità di memoria utilizzata
- Aggiornamento delle matrici

Autenticazione

Autenticazione con AES

Metodo basato sul protocollo di crittografia

AES (Advanced Encryption Standard)

Possibilità di mutua identificazione o autenticazione unilaterale

L'unica informazione di cui hanno bisogno tag e reader è la chiave simmetrica K

Autenticazione

Autenticazione con AES

Unilaterale

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

Autenticazione

Autenticazione con AES

Mutua identificazione

Reader -> Tag	:	C_1
Tag -> Reader	:	$R_1=e_K(C_1,C_2)$
Reader	:	If $d_K(R_1) = (C_1, C_2)$ Identità tag verificata
Reader -> Tag	:	$R_2=e_K(C_2,C_1)$
Tag	:	$d_K(R_2) = (C_2, C_1)$ Autenticazione riuscita

Autenticazione

Autenticazione con AES

Metodo particolarmente adatto a sistemi chiusi dove il controllo dei dispositivi è centralizzato

(Es: gestione bagagli in aeroporto, spedizioni)

Svantaggi:

Aggiornamento della chiave

Fine

Domande?