

RFID Security

Sicurezza dei Sistemi e delle Reti, A.A. 2021-2022
09/11/2022

emagon

Introduzione a RFID

Cos'è l'RFID?

- RFID significa **Radio Frequency Identification**.
- È una tecnologia utilizzata per trasmettere a brevi distanze (in genere pochi centimetri) piccole quantità di dati digitali.
- Si basa su due tipi di dispositivi: **trasmettitori/tag e lettori**.
- I trasmettitori possiedono al loro interno una **memoria non volatile** (read-only oppure riscrivibile) di pochi kB.
- I trasmettitori, quando alimentati dai lettori tramite induzione elettromagnetica, trasmettono il contenuto della loro memoria tramite **onde radio** (in genere con una frequenza che varia tra i 433 e 960 kHz).



Tipi di trasmettitori

- Esistono quattro tipologie di **trasmettitori RFID**:
 1. **Passivi**: i più comuni, vengono alimentati tramite induzione dai lettori;
 2. **Attivi**: possiedono una batteria con la quale alimentano l'apparato di trasmissione dei dati. Grazie ad essa riescono a trasmettere il loro segnale anche a diversi metri (per esempio il *Telepass* autostradale);
 3. **Semi-passivi**: possiedono una batteria che però non usano per alimentare il circuito di trasmissione ma solo il chip o apparati esterni. Il trasmettitore verrà alimentato tramite induzione dal lettore;
 4. **Semi-attivi**: possiedono una batteria con la quale alimentano l'apparato di trasmissione dei dati. In genere rimangono spenti o in stand-by e vengono attivati al passaggio di un lettore.

Utilizzi pratici dell'RFID

- L'RFID viene utilizzato nei più svariati campi:
 - Identificazione di animali da allevamento e domestici (*microchip* sottocutanei);
 - Etichette anti-taccheggio;
 - Chiavi e serrature smart;
 - *Immobilizer* dei veicoli;
 - Biglietti di viaggio;
 - Carte di riconoscimento e passaporti;
 - Carte di pagamento;
 - Monitoraggio di prodotti all'interno di edifici aziendali;
 - Riconoscimento di veicoli;
 - ... e molti altri.

L'NFC

- L'NFC significa **Near Field Communication** (standard ISO 18092).
- È lo standard RFID più conosciuto al mondo.
- Opera sulla frequenze radio 13,56 MHz e permette una velocità di comunicazione massima di 424 kB/s.
- L'NFC permette la comunicazione bi-direzionale: un dispositivo può essere sia lettore che trasmettitore. Per esempio gli smartphone moderni sono in grado sia di leggere che trasmettere dati via NFC e creare quindi una rete p2p temporanea.
- L'NFC supera il concetto di sola "**Identificazione**" dell'RFID e permette di trasmettere **qualsiasi tipo di dato**, per esempio foto (o altri file multimediali) tra due dispositivi.
- L'NFC viene anche utilizzato per le **carte di pagamento contactless** e per i **sistemi di pagamento digitali** (Apple Pay, Google Pay, Samsung Pay, ecc.).



Problemi di privacy dell'RFID

I rischi per la privacy

- L'utilizzo della tecnologia RFID (e NFC) presenta dei rischi per la privacy delle persone.
- Basta pensare a un tag contenente delle informazioni personali (per es. un passaporto): un malintenzionato potrebbe leggere il tag di nascosto ed entrare in possesso dei dati privati presenti nella memoria del trasmettitore.
- I rischi sulla privacy ci sono anche con i semplici tag RFID di identificazione. Un malintenzionato potrebbe tracciare gli spostamenti di un tag contenuto in oggetto appartenente alla vittima (anche un indumento) tramite una rete di lettori RFID sparsi in giro: in questo caso la vittima non si accorgerebbe di niente e, addirittura, potrebbe anche non essere a conoscenza del fatto che un suo oggetto o indumento abbia un tag RFID.

Soluzioni

- Per ridurre questi rischi esistono soluzioni sia **fisiche** che **legislative**.
 - Soluzioni **fisiche**:
 - **Bloccare** la trasmissione di un segnale RFID tramite una **schermatura metallica**. Questa soluzione è usata da alcuni portafogli "*RFID block*" e anche dai **passaporti**, che permettono la lettura del tag solo se fisicamente aperti;
 - Rimuovere o disattivare i tag RFID quando non sono più necessari (per es. rimuovere i tag utilizzati per gestire l'inventario dei capi di abbigliamento una volta che vengono venduti).

- Soluzioni **legislative**:
 - Provvedimento del **Garante della Privacy** (09 marzo 2005):
 1. **La consapevolezza** dell'utente della presenza dei tag RFID: è necessario informare gli utenti della presenza di lettori RFID (tramite simboli) e ridurre al più possibile l'utilizzo dei tag quando non più necessari, permettendone la rimozione o disattivazione;
 2. **Le informazioni** contenute nei tag: impone che i prodotti di largo consumo con tag RFID debbano contenere solo un identificativo seriale del tag stesso e non altre informazioni;
 3. **Dati personali**: il Garante ha indicato che nel caso di trattamento dei dati personali è necessario, come sempre, il consenso informato ed esplicito del diretto interessato.

Problemi di sicurezza dell'RFID

Problemi di sicurezza

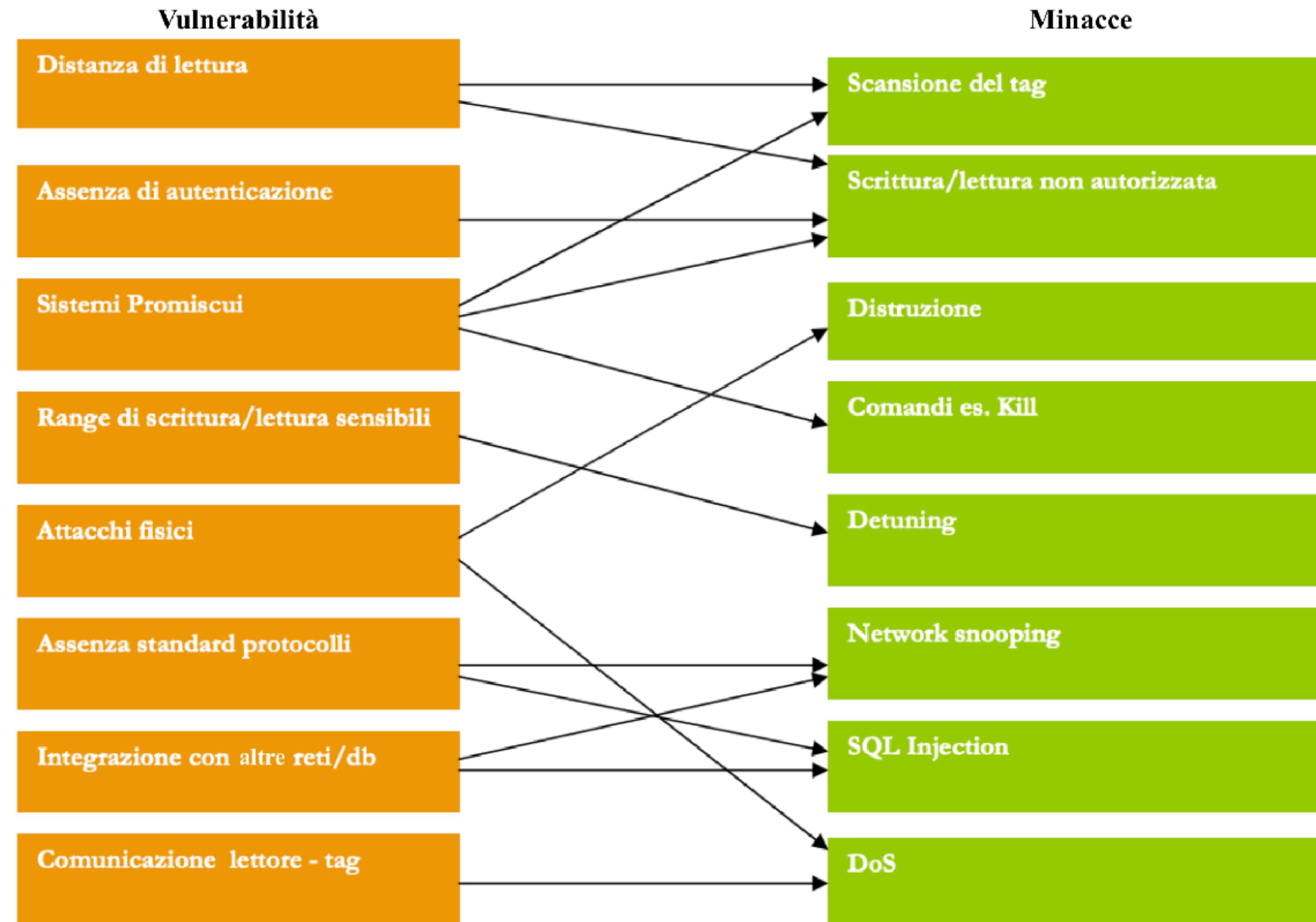
- La tecnologia RFID presenta diversi **problemi di sicurezza**.
- Oltre agli **attacchi fisici** dei lettori (rimozione, distruzione...), sono possibili attacchi all'**integrità, confidenzialità, autenticità e disponibilità** dei dati.
- È possibile infatti **leggere i dati senza autorizzazione** (attacco alla **confidenzialità**) oppure, nel caso di tag riscrivibili, **manomettere i tag** salvando dei **dati errati** (attacco all'**integrità, autenticità e disponibilità**).
- Sono possibili anche attacchi di **jaming**, anche se la maggior parte dei lettori (e anche alcuni trasmittitori) in commercio implementano delle tecniche di controllo dei dati.



Problemi di sicurezza

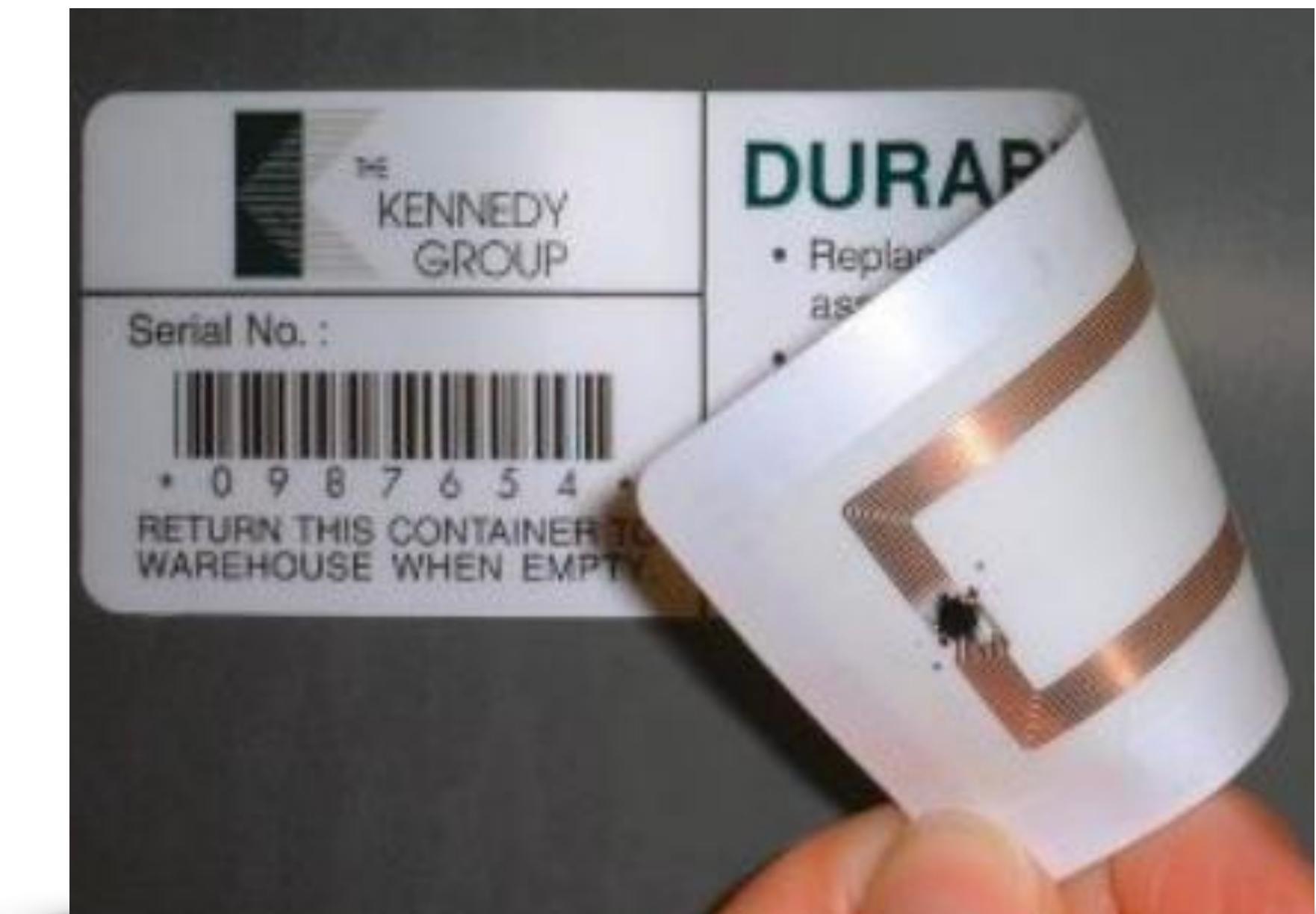
- In ambienti **business** è comune trovare dei **lettori** RFID/NFC che **comunicano** con i **sistemi backend/database** aziendali (per es. serrature smart che controllano il badge dell'impiegato).
- In questi casi l'**elaborazione** dei dati letti viene **effettuata dal sistema di backend** già esistente, mentre il lettore si occupa solamente di riportare il segnale letto dai tag RFID.
- Questo sistema, a prima vista, **appare sicuro**: dato che il controllo dei dati è affidato al backend aziendale è possibile implementare qualsiasi tipo di controllo senza doversi preoccupare delle capacità computazionali del lettore RFID.
- In realtà questo sistema espone una **superficie d'attacco** che potrebbe portare a grandi **rischi per la sicurezza**: un malintenzionato potrebbe avvicinare un **tag RFID** contenente dati che, una volta letti e inviati al backend aziendale, danneggierebbero il sistema: una classica **SQL injection**, **codice malevolo** ecc.

Problemi di sicurezza



Soluzioni

- In alcuni casi è possibile **crittografare** i dati presenti sui tag RFID (anche se spesso si usano protocolli **ECB**, vulnerabili ad attacchi **known-plaintext**) oppure adottare tecniche di **hashing** e quindi scrivere, oltre al messaggio stesso, il relativo *message digest*. Queste tecniche possono aiutare contro gli attacchi alla confidenzialità e autenticità, senza però impedire i *replay attack*.
- Infatti, la maggior parte dei tag RFID è composta da dispositivi "*dumb*", che non sono quindi in grado di effettuare elaborazioni e non possono adottare le classiche tecniche di protezione contro gli attacchi di tipo **replay** (per esempio l'utilizzo di autenticazione, nonce, challenge-response, ecc.).



Soluzioni

- Esistono alcuni **trasmettitori attivi** composti da componenti come **chip di controllo** e memorie aggiuntive in grado di **implementare** ulteriori tecniche di **protezione**.
- Nei casi di sistemi dove il lettore RFID si interfaccia con un sistema di backend aziendale è necessario fare un'analisi dei rischi sull'**intero sistema informatico** aziendale e implementare le **opportune soluzioni** (in genere direttamente nel sistema di backend).



Demo

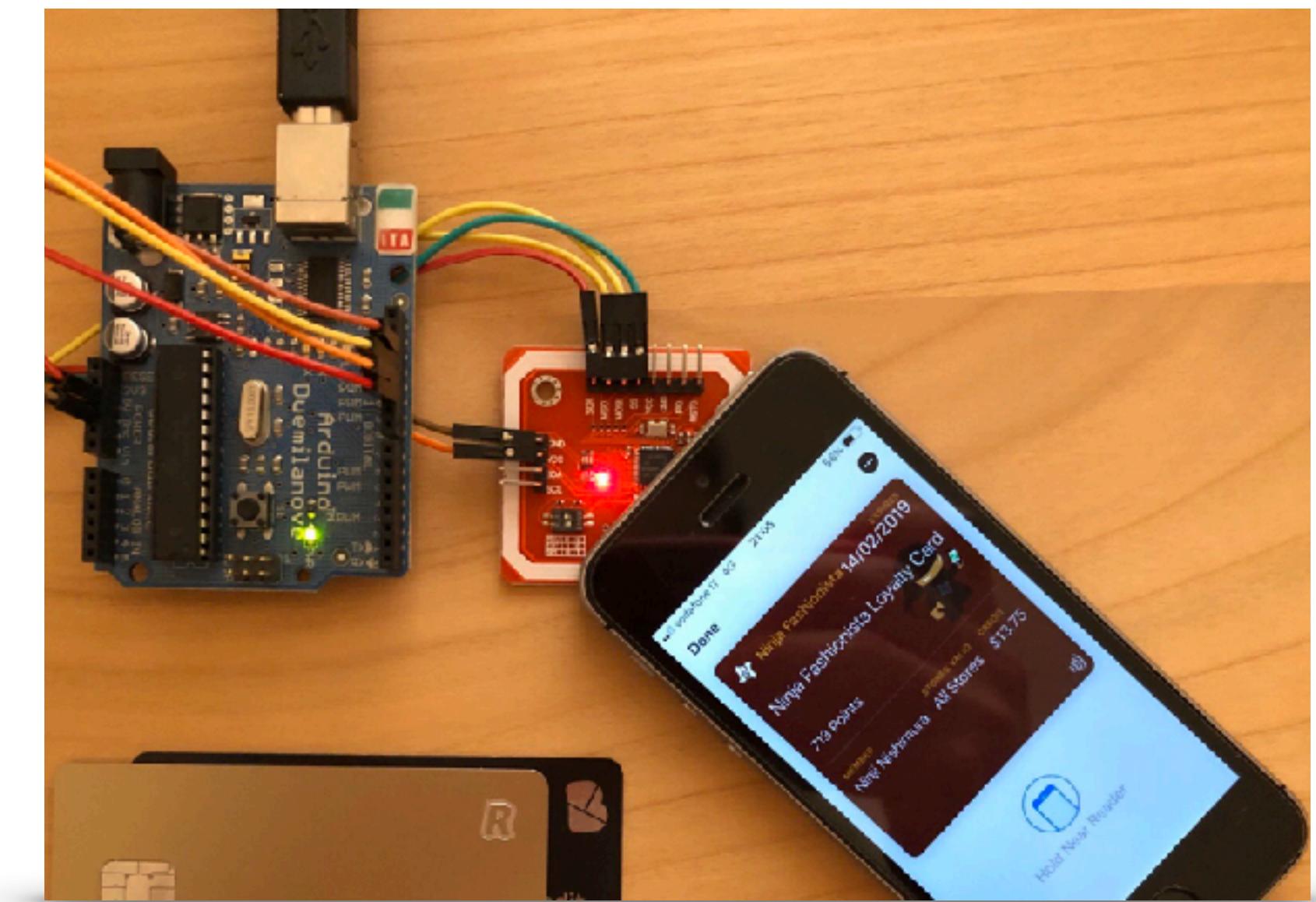
Un esempio di attacco

- Tramite un **lettore/scrittore RFID**, una **tessera RFID** e un **semplice circuito** collegato ad una scheda programmabile **Arduino** è possibile **simulare un attacco** di tipo *replay* ad un sistema RFID.
- Il **circuito e l'Arduino** vengono utilizzati per **implementare** un sistema tipo **serratura** smart: avvicinando al lettore una tessera RFID, l'Arduino controlla i dati rilevati e, se corrispondenti ad una determinata sequenza di byte, **approva la tessera** e apre una serratura (in questo esempio riproduce un suono e accende un led verde).

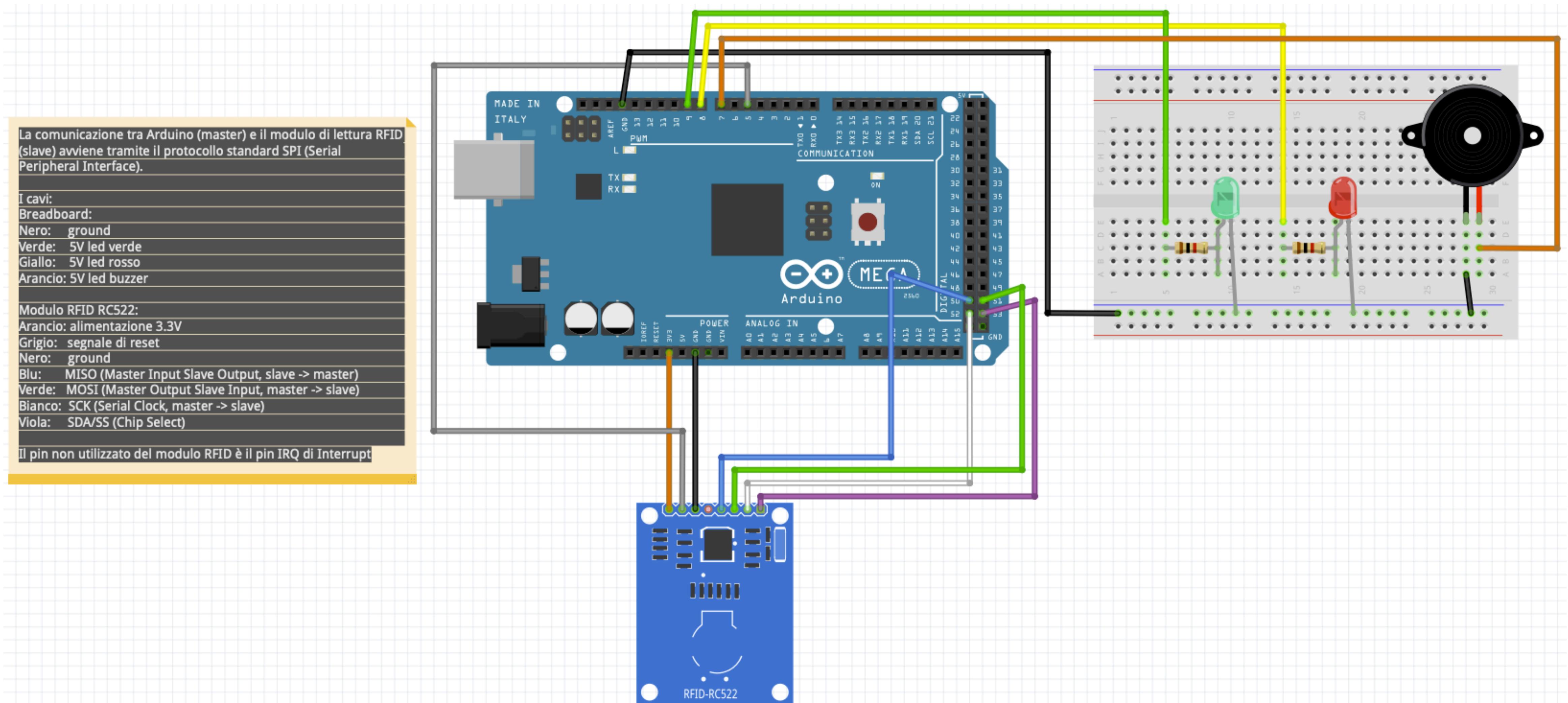


Un esempio di attacco

- Utilizzando un **lettore/scrittore** RFID è possibile **leggere** e salvare il contenuto della **tessera** quando non è in uso (per es. mentre si trova in una tasca del proprietario).
- Successivamente è possibile **scrivere** i dati in un'**altra tessera** riscrivibile in modo da creare a tutti gli effetti un **clone** della scheda originale.
- Nel caso di sistemi basati su **NFC** è addirittura possibile utilizzare uno **smartphone** come lettore, scrittore e anche trasmettitore dei dati letti dalla tessera originale. In questo modo non è necessaria nessuna tessera riscrivibile.

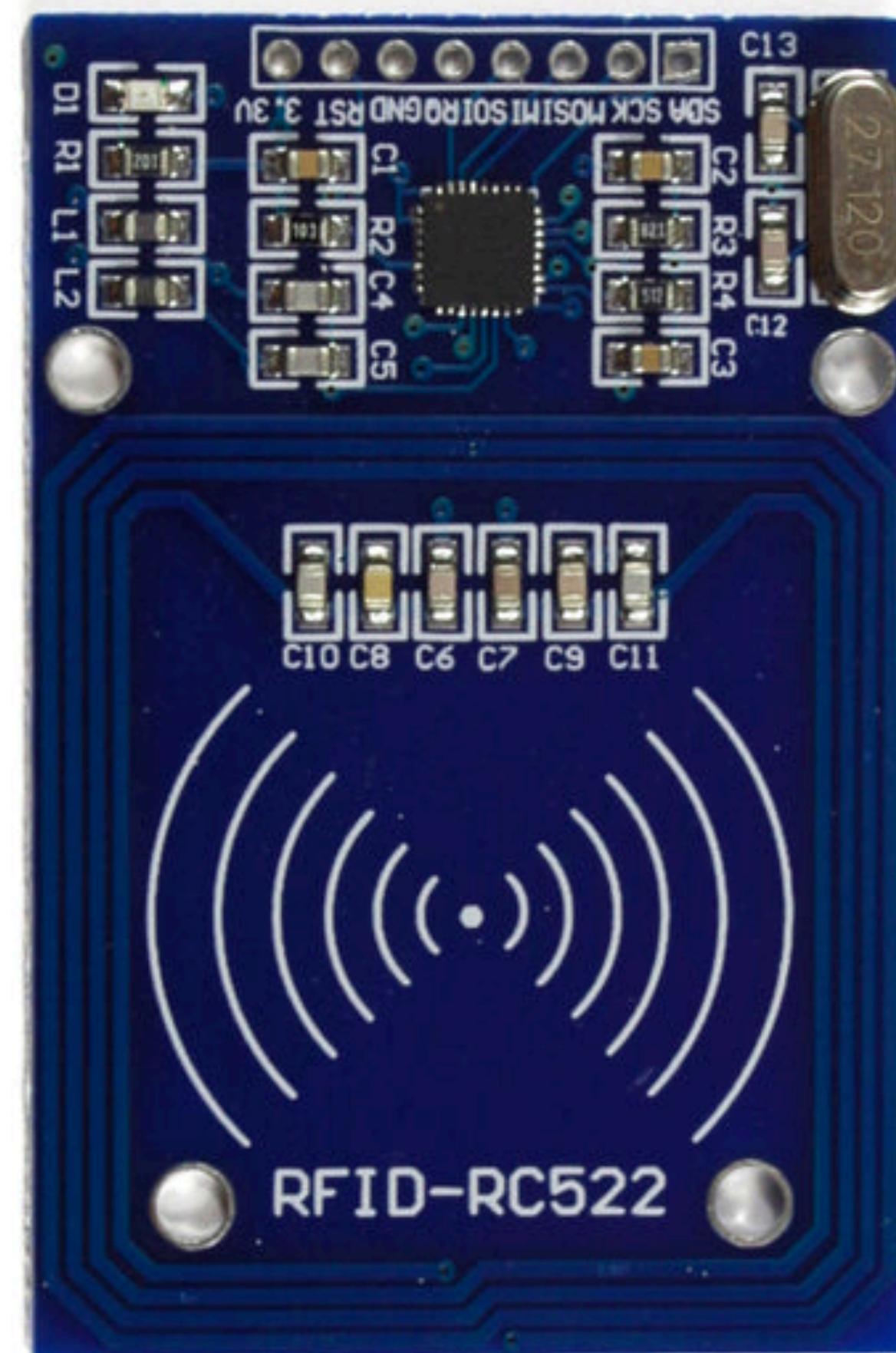


Schema del circuito



Descrizione della demo

- Per motivi pratici, in questa dimostrazione il **circuito** composto dall'Arduino e dal lettore/scrittore RFID fungerà sia da serratura smart "**vittima**" che da dispositivo "**clonatore**" di carte RFID.
- Il modulo di lettura/scrittura dei tag RFID utilizzato è un RFID-RC522, che lavora su frequenza 13,56 MHz e supporta lo standard ISO/IEC 14443 A/**MIFARE**. Comunica con l'Arduino attraverso lo standard **SPI** (Serial Peripheral Interface).

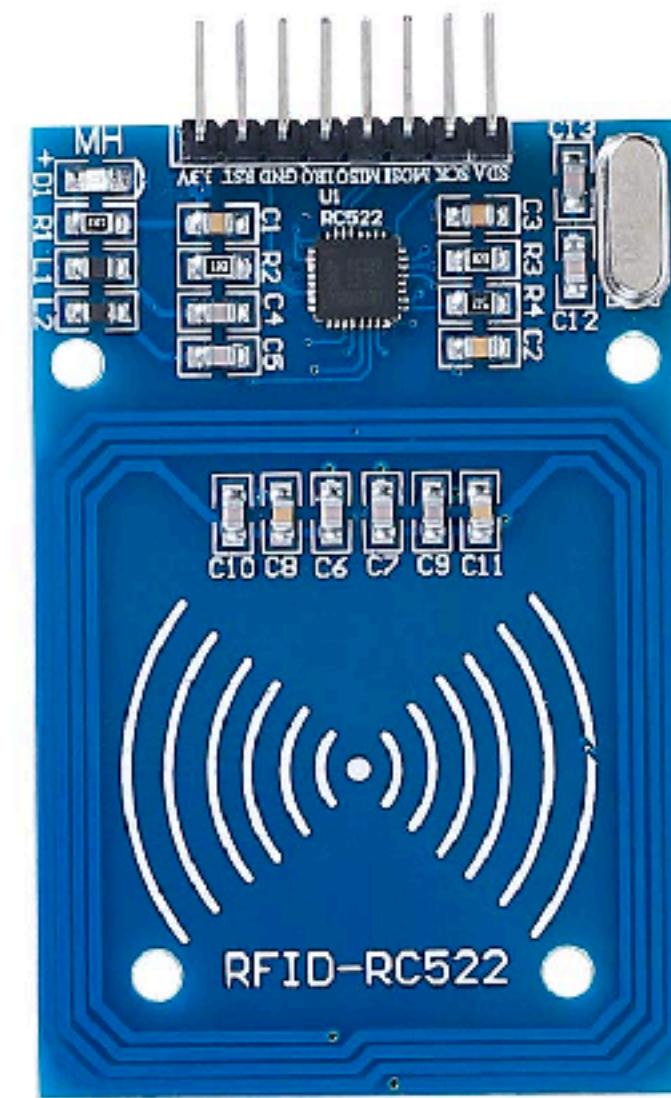


Descrizione della demo

- Il circuito è formato da una scheda programmabile **Arduino**, un modulo **lettore/scrittore RFID MIFARE** **RFID-RC522**, un **LED verde**, un **LED rosso** e un **cicalino** attivo.
- Il circuito può operare in due modi: modalità "**serratura smart**" e modalità "**clonatore**":
 - in modalità "**serratura smart**" simula una serratura che si **apre** avvicinando un **tag RFID autorizzato** (in questo caso l'apertura della serratura è simulata dall'accensione di un **LED verde** e da un **singolo suono** emesso dal cicalino. In caso di lettura di un **tag non autorizzato**, si accende il **LED rosso** e vengono emessi **tre suoni** distinti);
 - in modalità "**clonatore**" simula il dispositivo dell'attaccante che è in grado di **leggere** un tag RFID e **clonare** il contenuto su un altro tag.

Descrizione della demo

- I **tag RFID** (chiamati anche **PICC**, *Proximity Integrated Circuit Card*, in MIFARE) utilizzati sono due:
 - una **tessera bianca** che rappresenta un **tag autorizzato** all'apertura simulata della serratura;
 - un **portachiavi blu** che rappresenta il **tag dell'attaccante** sul quale verrà clonato il segreto letto dalla tessera legittima.



I PICC MIFARE Classic 1K

- I tag **PICC MIFARE** contengono una memoria non volatile EEPROM.
- Questa memoria può contenere in totale 1kB di dati (16 settori da 4 blocchi, dove 1 blocco è composto da 16 byte).
- In ogni settore l'ultimo blocco è chiamato *trailer* che contiene due chiavi segrete e dei bit di accessibilità per il blocco stesso.
- Le chiavi segrete vengono utilizzate per l'implementazione di **CRYPTO1**: una tecnica di crittografia e autenticazione (ormai non più sicura) che permette al lettore RFID (**PCD**, Proximity Coupling Device, in MIFARE) di leggere e scrivere i dati **solo se a conoscenza** della chiave simmetrica.

Demo

Codice e schema elettrico: <https://github.com/e-magon/demo-rfid-arduino>

Conclusioni

Conclusioni

- Dalla dimostrazione pratica si capisce che le tecnologie classiche RFID non sono sicure.
- È sempre importante effettuare uno studio di sicurezza e valutare i reali benefici derivanti dall'utilizzo di un sistema RFID:
 - Per un semplice sistema di gestione inventario, per esempio, un sistema classico RFID può essere una buona soluzione;
 - Dove invece è richiesto un alto livello di sicurezza (per es. un sistema di autenticazione) è necessario utilizzare tag e lettori RFID di ultima generazione che implementano algoritmi moderni e robusti in termini di crittografia e hashing, ovviamente dopo aver effettuato un'analisi completa e delineato un piano di sicurezza generale per il sistema informatico.

Bibliografia

- [https://www.dmi.unipg.it/~bista/didattica/sicurezza-pg/seminari2009-10/
sic_rfid/relazione_stage_Alfano.pdf](https://www.dmi.unipg.it/~bista/didattica/sicurezza-pg/seminari2009-10/sic_rfid/relazione_stage_Alfano.pdf)
- https://it.wikipedia.org/wiki/Identificazione_a_radiofrequenza#RFID_tag_o_transponder_o_etichetta
- https://it.wikipedia.org/wiki/Near_Field_Communication
- <https://www.mouser.com/datasheet/2/302/MF1S503x-89574.pdf>
- <https://github.com/miguelbalboa/rfid>

Codice e schema elettrico della demo:

- <https://github.com/e-magon/demo-rfid-arduino>