RFID
Identificazione automatica a radiofrequenza: tecnologia e impatto sulla privacy

Gianni Bianchini
giannibi@firenze.linux.it

Metro Olografix Camp
Pescara, Agosto 2004

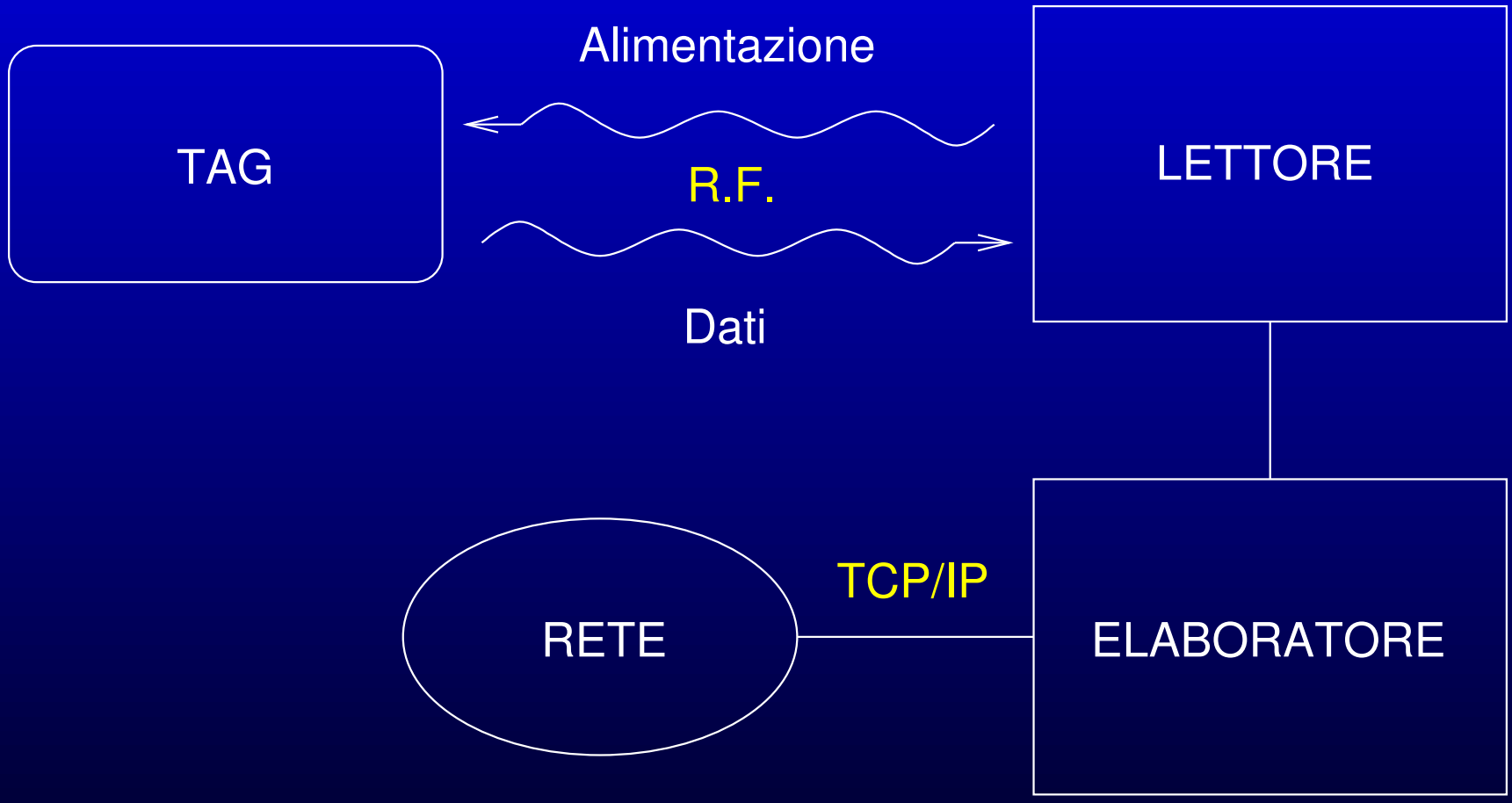
Sommario

- La tecnologia RFID
  - Tag o transponder (“etichetta intelligente”)
  - Dispositivi di lettura e trasmissione
- I contesti applicativi
- Il lato oscuro: rischi per la privacy del consumatore
  - Identificabilità
  - Tracciabilità
  - Profilabilità
- Le soluzioni tecnologiche
- Gli orientamenti normativi

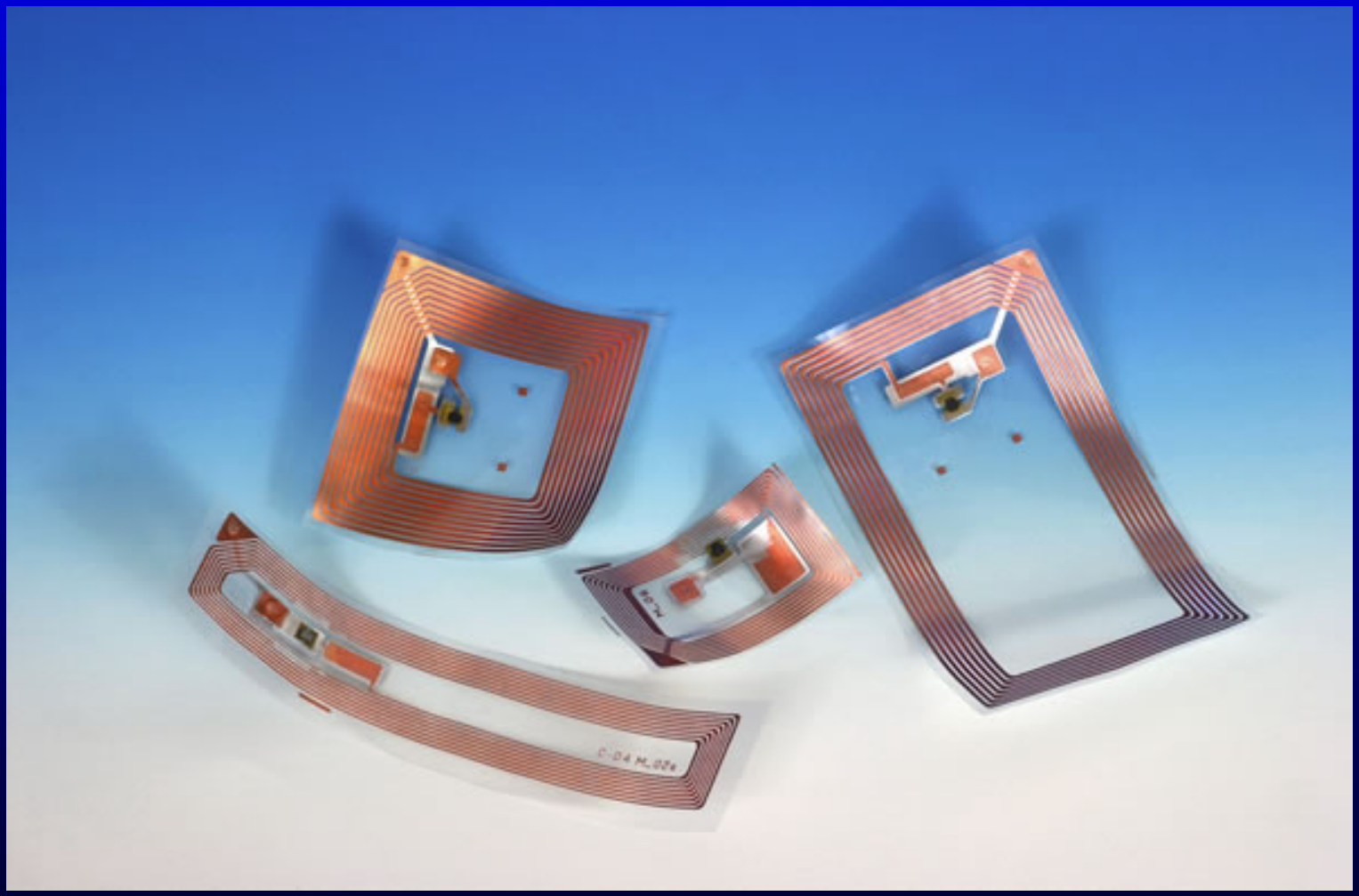
La tecnologia RFID

Un sistema di identificazione automatica a radiofrequenza (*RFID* = Radio Frequency Identification) è costituito da microchip dotati di antenna, detti *tag* o *transponder*, e da un dispositivo di lettura a radiofrequenza che riceve e decodifica le informazioni in essi contenute. Le informazioni lette sono successivamente trasmesse attraverso una rete ed elaborate.

La tecnologia RFID: schema di base



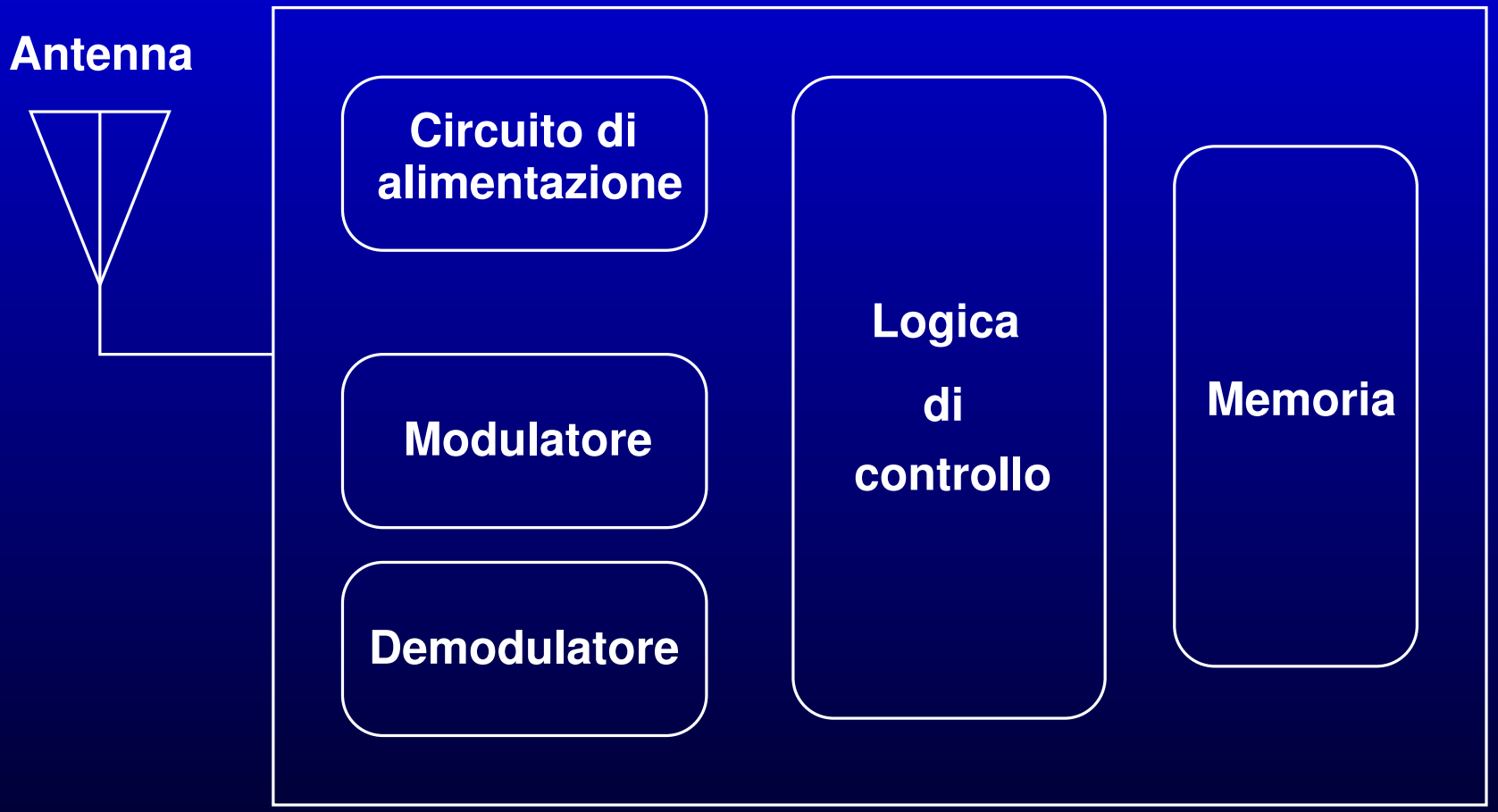
RFID tag



Antenna + microchip + involucro

Metro Olografix Camp, Pescara, Agosto 04

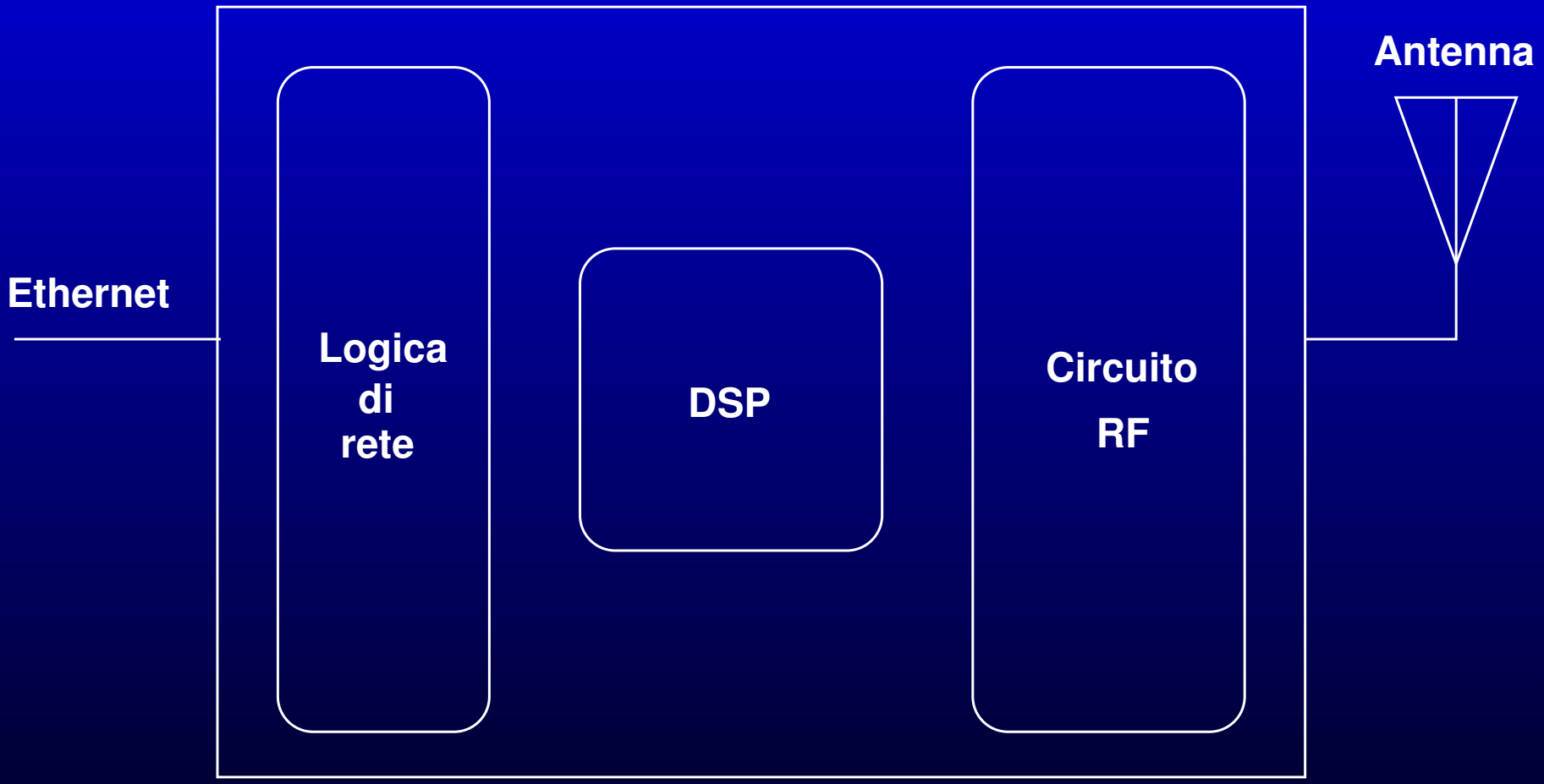
RFID tag: schema a blocchi



RFID tag: funzionamento

- In genere il dispositivo è *passivo*
  - Capta la RF inviata dal lettore e ne ricava l'energia necessaria per il funzionamento
- Esistono dispositivi *attivi*, autoalimentati
- Funzionalità di base
  - Modulazione a RF e trasmissione di un codice identificativo (es. 128 bit) contenuto nella memoria
- Alcune funzionalità avanzate
  - Aggiornamento dei dati in memoria e riprogrammazione della logica
  - Crittografia elementare
  - Lettura di sensori

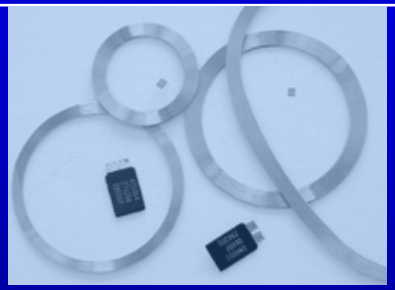
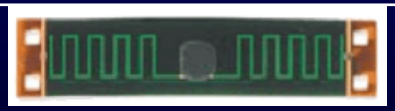
Lettore: schema a blocchi



Lettore: funzionamento

- Alimentazione a radiofrequenza dei tag
- Creazione del link dati
- Riconoscimento di tag multipli
- Demodulazione e decodifica delle letture
- Eventuale aggiornamento dei dati sul tag
- Interfacciamento con un elaboratore o con la rete

Tipologie

Frequenza di lavoro	Raggio di lettura	
100-500 kHz [125]	Corto	
10-15 MHz [13.56]	Corto/Medio	
850-950 MHz [915]	Medio	
2.4-5.8 GHz [2.4]	Lungo	

- Standard ISO/IEC 15963 (”logico”), ISO 18000-x (”fisico”)

Applicazioni

- Sostituzione del codice a barre
  - Identificazione dei prodotti
  - Automatizzazione dell'inventario
  - Operazioni di cassa
- Logistica avanzata
  - Tracciamento del percorso del prodotto attraverso le fasi di produzione e distribuzione, fino alle procedure di smaltimento
  - Sistemi di stoccaggio
  - "Scaffali intelligenti" (Auto-ID / Gillette / Wal-Mart)
  - Gestione della manutenzione
- Sistemi di pagamento automatico (Telepass)
- Controllo di accesso ad edifici e mezzi di trasporto
- Identificazione volumi nelle biblioteche

Un codice a barre di nuova generazione

- Codice a barre
  - Deve essere in vista rispetto al lettore
  - Indica solo la tipologia e la provenienza dell'oggetto a cui si riferisce
  - Standard UPC, EAN
- RFID
  - L'interazione a radiofrequenza permette l'identificazione "da remoto"
  - È possibile leggere più di un'etichetta allo stesso tempo
  - L'etichetta è in grado di memorizzare un'informazione che contraddistingua univocamente il *singolo* oggetto, ovvero un puntatore al record relativo all'oggetto all'interno di un opportuno database
  - EPC (Electronic Product Code): standard per l'assegnazione di identificativi univoci
- Costo attuale di un tag passivo: circa €0.13

Applicazioni avanzate e future

- Tracciamento del bagaglio aereo (British Airways)
- Alcuni tag di nuova generazione possono alimentare ed interfacciarsi con sensori
  - Misura di temperatura e pressione dei pneumatici (Michelin)
  - Monitoraggio di strutture come ponti o tralicci
  - Monitoraggio di grandezze in ambienti critici
- Banconote (BCE, 2005)
  - Anti-contraffazione
  - Tracciamento di denaro proveniente da attività illecite

Il lato oscuro

- L'individuazione di tag e lettori può essere resa difficile
- Se non rimosse o disattivate, le etichette RFID rendono identificabili gli oggetti, e quindi potenzialmente palesi i dati ad essi collegati, anche fuori dall'ambito nel quale il sistema è stato concepito per funzionare
  - ⋆ L'etichetta funziona da "faro", anche indipendentemente dal collegamento con i dati relativi al prodotto
- I dati relativi ai prodotti vengono spesso associati all'identità dell'acquirente
  - ⋆ Acquisto al dettaglio in catene di distribuzione
  - ⋆ Acquisto in rete
- L'identità dell'acquirente può a sua volta essere usata come indice in database di natura diversa, quindi l'identificativo dell'etichetta individua potenzialmente dati personali anche sensibili

I tag possono essere difficili da individuare

- Integrati nell'imballaggio delle merci
- Posti in luoghi inaccessibili all'interno dei prodotti
- Cuciti nelle stoffe
- Inseriti fra strati di carta
- "Fusi" nella plastica
- Stampati su supporti eterogenei
- Chipless tags
  - ⋆ Sottili fibre metalliche incorporate nelle fibre della carta, che riflettono l'onda e.m. verso il lettore risuonando a determinate frequenze ("resonant signature")

Anche i lettori possono essere molto ben nascosti

- Mura di edifici
- Pavimenti
- Tappeti
- Mobili
- Veicoli in movimento
- Strade
- . . .

Identificativi globali

- Lo standard di identificazione globale EPC è già pronto
- Potenzialmente ogni oggetto prodotto al mondo può venire identificato univocamente
- Una lattina trovata per terra reca di fatto informazioni su
  - quando, dove e da chi è stata prodotta
  - dove è stata comprata,
  - quando è stata comprata,
  - chi l'ha comprata
- . . .e facendo due più due...
  - <inserire qui lo scenario peggiore che la paranoia vi suggerisce>

Altri amplificatori del problema

- Raccolta sistematica dei dati
- Creazione di insiemi di dati commerciali aggregati in database centralizzati
- Incrocio ed associazione dei dati
  - ⋆ Già con i codici a barre è prassi collegare i dati del prodotto con l'identità dell'acquirente
  - ⋆ È vantaggioso per i commercianti identificare il consumatore per condurre campagne pubblicitarie mirate
- Norme (o loro mancanza) di conservazione e cancellazione dei dati
- Cessione e vendita (legale o meno) dei dati
- Analisi dei dati, *data mining*

Il risultato

- Identificabilità
  - Ogni oggetto acquistato può essere ricondotto all'identità (e non solo) dell'acquirente
- Tracciabilità
  - Le etichette possono essere lette da dispositivi più o meno "rogue"
  - Tracciamento degli spostamenti all'interno del centro commerciale...
  - ...ed all'esterno. "Dove sei andato oggi?"
  - Comunicazione inconsapevole di dati relativi agli oggetti posseduti
  - Le etichette inserite nelle banconote ne rivelano indubbiamente la presenza (con immaginabile soddisfazione dei borseggiatori)
- Profilabilità
  - Poternziale collegamento con dati personali (es. profilo sanitario)

In sostanza...

...l'impiego indiscriminato ed in assenza di opportuni accorgimenti (tecnologici e non) di dispositivi RFID all'interno di oggetti di uso comune rappresenta una seria minaccia per la privacy del consumatore e le libertà civili del cittadino.

"Non mi interessa ciò che quelli di Wal-Mart fanno per portare un prodotto nel supermercato, ma a loro non deve interessare ciò che faccio io quando esco dal supermercato" (K. Albrecht, CASPIAN)

- Consapevolezza?
  - Circa il 40% delle hit di Google sul termine "RFID" include la parola "privacy".

Ma no, dai!

- Le etichette non possono essere lette alle distanze necessarie per realizzare un'efficace azione di sorveglianza
  - Tag attivi possono essere letti a grandi distanze
  - Si può avere interesse a sorvegliare aree anche molto circoscritte
  - Distanze brevi rendono il sistema più efficace: minimizzazione dell'interferenza tra tag diversi
- Sarebbe necessaria una distribuzione eccessivamente capillare di dispositivi lettori
  - Per tracciare un'auto sull'autostrada basta un dispositivo ad ogni casello
  - Per tracciare i movimenti di una persona in città basta sorvegliare gli accessi agli edifici
- L'informazione contenuta nei tag è insufficiente
  - I dati contenuti sono puntatori a record in una o più basi di dati distribuite e interconnesse, contenenti potenzialmente grandi quantità informazioni eterogenee anche sensibili

Sono necessarie regole precise

- Valutazione formale della tecnologia da parte di tutte le categorie interessate
- Uso improntato a principi di *Fair Information Practice*
  - Trasparenza: specifiche tecniche aperte, politiche di utilizzo aperte, l'utente dovrebbe conoscere quali prodotti recano tag RFID e dove e come questi vengono letti
  - Limitazione della raccolta dati allo stretto necessario
  - Definizione delle responsabilità
  - Sicurezza ed integrità nella trasmissione e conservazione dei dati
- Definizione di usi e comportamenti non ammissibili
  - Rendere difficile l'individuazione ed impedire la disattivazione dei dispositivi da parte del consumatore
  - Utilizzare la tecnologia RFID per ridurre il grado di anonimato nelle transazioni (uso nelle banconote)

Soluzioni

- Disabilitazione (es. all'uscita del punto vendita)
  - Quasi tutti i tag possono essere disabilitati a comando
  - Non elimina la tracciabilità all'interno del punto di vendita (interazione RFID-videosorveglianza in sistemi di "scaffale intelligente")
  - Alcuni tag possono essere resi solo semplicemente "dormienti"
  - La procedura può essere più o meno consapevolmente scoraggiata (gestione dei resi)
  - Uso a discrezione del consumatore
    - Creazione di due classi di consumatori

- I tag RFID possono essere molto difficili da rilevare o impossibili da rimuovere
  - Avremo ognuno il proprio scanner personale?
  - Avremo cura di avvolgere il nostro portafogli nella pellicola metallica?

Soluzioni tecnologiche

- Blocker tags [Juels, Rivest, Szydlo, 2003]
  - Disposti sopra un tag RFID, o comunque interposti tra il tag e il lettore, impediscono la comunicazione con il lettore “floodandolo”, ovvero simulando la presenza di molteplici tag (tecnologia RSA Labs)
  - Possibilità di attacco: blocco di tag di oggetti non ancora acquistati
    - Blocco selettivo: al momento dell’acquisto il tag passa da non bloccabile a bloccabile
    - Il tag bloccato “consiglia gentilmente” al lettore di non tentare di leggerlo
  - Incoraggia l’uso diffuso di RFID. E se per esigenze di sicurezza i blocker tags venissero un giorno banditi in alcune circostanze (aeroporti, edifici pubblici...)?
  - Uso a discrezione del consumatore

Soluzioni tecnologiche

- Crittografia minimale (tag in grado di realizzare funzioni di crittografia forte sono costosi)
  - ⋆ Cifratura dell'ID in modo che questo sia interpretabile solo dal lettore designato
  - ⋆ Re-encryption periodica dell'ID da parte di un lettore
  - ⋆ Hashing dell'ID da parte del tag (anche in catena)
- Pseudonym throttling
  - ⋆ Generazione off-line di una serie di pseudonimi crittograficamente non collegabili tra loro
  - ⋆ Ad ogni lettura l'etichetta emette uno degli pseudonimi
  - ⋆ Gli pseudonimi possono essere rinfrescati dal lettore
- Approcci energetici (vicinanza del lettore)

Alcuni casi recenti

- Il caso Metro AG Extra Future Store (D)
  - RFID tag non dichiarato nelle carte fedeltà
  - Il dispositivo di disattivazione rimuove l'ID del prodotto ma non l'ID univoco del tag
- Il caso Gillette Smart Shelf (UK)
  - Tracciamento clienti con telecamere pilotate tramite RFID
- Il caso Benetton
  - Sperimentazione RFID sulle etichette di una linea di abbigliamento ritirata a seguito di mobilitazione di consumatori
- Il caso WSIS (Ginevra, 2003)
  - Gli spostamenti dei delegati erano tracciati mediante tag inseriti all'interno dei badge, in apparente violazione della direttiva europea sulla privacy, delle linee guida ONU sui file personali e della legge svizzera

Il Garante sull'uso della RFID nelle biblioteche

- Fornire agli utenti un'informativa sull'impiego dei dispositivi (quali articoli rechino etichette RFID, dove siano ubicati i lettori), escludendo forme occulte di lettura di tali dispositivi e specificando le finalità del loro utilizzo
- Limitare i dati raccolti a quelli indispensabili per le finalità in questione
- Evitare l'inserimento di dati personali nelle etichette RFID
- Garantire idonee misure di sicurezza (trasmissione dei dati, accesso ai relativi database, cifratura) (Bollettino n. 196, 11/1/2004)

"L'impiego di sistemi biblioteconomici automatizzati che utilizzino etichette basate sulla tecnologia in radiofrequenza comporta rischi potenziali che devono essere valutati attentamente per evitare di compromettere, nel lungo periodo, la libertà di pensiero." (Privacy Rights Clearinghouse, Electronic Frontier Foundation, USA)

Il Garante sulla RFID nella Relazione 2003

- ”Sostituendo i codici a barre, [le etichette RFID] permetteranno di seguire i prodotti nei loro spostamenti, creando cos le condizioni per controllare anche chi ha acquistato ed usa quel prodotto”.

- ”Molti impieghi RFID sono sicuramente utili e benefici: migliore gestione delle merci, possibilità di rintracciare l’origine di prodotti particolarmente delicati, come i medicinali, rapidità di operazioni commerciali, come la lettura istantanea dei prezzi di tutti gli oggetti posti nel carrello di un supermercato. Se, tuttavia, le etichette intelligenti non vengono disattivate nel momento in cui il prodotto passa nelle mani dell’acquirente, diventa reale il rischio di una sorveglianza generalizzata di persone e comportamenti”

(Relazione annuale 2003, 28/4/2004).

E questo è solo l'inizio

- La privacy del consumatore è solo uno dei molteplici aspetti di sicurezza legati all'uso su larga scala della tecnologia RFID
- Sicurezza intrinseca di una tecnologia giovane ("caso" RFDump)
- Informatizzazione pervasiva: "Extended internet"
  - La tecnologia RFID estende di fatto il "perimetro di sicurezza" di una rete
- I chip RFID impiantabili sugli esseri umani sono già una realtà.
  - Informazioni di localizzazione di persone in libertà provvisoria (VeriChip)
  - VeriPay: chip sottopelle progettato per prendere il posto della comune carta di credito
- ...d'altra parte 128 bit sono molto più che sufficienti per indicizzare l'intera popolazione mondiale (ne bastano 33!)

Questa invece è la fine

Grazie per l’attenzione!

/giannibi

Riferimenti

- K. Finkenzeller, *The RFID Handbook*, J. Wiley & Sons, 2003
- M. Reynolds, *Physics of RFID*, RFID Privacy Workshop @ MIT, Nov. 2003, http://www.rfidprivacy.org/papers/physicsofrfid.pdf
- R. Want, *RFID: a key to automating everything*, Scientific American, Gen. 2004.
- EPC Global, http://www.epcglobalinc.org
- Auto-ID Labs, http://www.autoidlabs.org

Riferimenti

- K. Zetter, *Jamming Tags Block RFID Scanners*, Wired, Marzo 2004
- A. Juels, *RFID Tags: Privacy and Security without Cryptography*, RFID Privacy Workshop @ MIT, Nov. 2003, http://www.rfidprivacy.org/papers/juels.pdf
- K. Fishkin, S. Roy, *Enhancing RFID Privacy through Antenna Energy Analysis*, RFID Privacy Workshop @ MIT, Nov. 2003, http://www.rfidprivacy.org/papers/fishkin-slides-2003-11-15.pdf
- Privacy Rights Clearinghouse, http://www.privacyrights.org
- Consumers against supermarket privacy invasion and numbering (CASPIAN), http://www.spychips.com

Riferimenti

- Electronic Frontier Foundation, http://www.eff.org
- K. Albrecht, *RFID: Privacy and Societal Implications*, RFID Privacy Workshop @ MIT, Nov. 2003 http://www.rfidprivacy.org/papers/albrecht.pdf
- Garante per la protezione dei dati personali, Relazione 2003, http://www.garanteprivacy.it
- RFID Privacy Workshop @ MIT, Nov. 2003 http://www.rfidprivacy.org
- RFDump, http://www.rf-dump.org