

SEMINARIO DI TEORIA
DELL'INFORMAZIONE

***NFC
AND
SECURITY***

STUDENTI:

Marta Luzi

Stefania Alcini

SOMMARIO

- 1. PREMESSA**
- 2. COS' E' LA TECNOLOGIA NFC (o Near Field Communication)?**
- 3. COME SI USA?**
- 4. PERCHÈ USARLA?**
- 5. MA È REALMENTE SICURO?**
 - 5.1 SNIFFING
 - 5.1.1 Clonazione
 - 5.2 TAMPERING E SPOOFING
 - 5.2.1 Data corruption
 - 5.2.2 Data modification
 - 5.2.3 Data inserction
 - 5.2.4 Man-in-the Middle-Attack
- 6. COME DIFENDERSI?**
 - 6.1 AUTENTICAZIONE
 - 6.1.1 Autenticazione passiva
 - 6.1.2 Autenticazione attiva (MSK e DK)
 - 6.2 CRIPTAZIONE DEI DATI-ALLESTIMENTO DI UN CANALE SICURO
 - 6.2.1 Una proposta per scambio chiavi
- 7. CONCLUSIONI**
- 8. BIBLIOGRAFIA**

1. PREMESSA

Pagare e ricevere denaro è un'esigenza che l'uomo ha fin dalla notte dei tempi e nei millenni abbiamo assistito a tutta una serie di metodi differenti per soddisfare questo bisogno. Siamo partiti dal baratto, abbiamo attraversato la fase delle monete di vari metalli fino a giungere all'invenzione della banconota, e poi ancora dell'assegno e per finire al denaro fatto di bits.

Se escludiamo gli ultimi decenni, abbiamo sempre avuto a che fare con metodi di pagamento basati sullo scambio materiale di "oggetti" di vario tipo, via via sempre più complessi anche in risposta al crescente numero di contraffattori. Negli ultimi anni però il denaro è divenuto digitale, grazie anche alla diffusione dei personal computer, dell'online banking e dei servizi come E-Bay et similia. Abbiamo così perso il contatto fisico con il denaro, anche se nella nostra società la banconota e tutte le sue declinazioni (assegni, carte di credito, bancomat..) rimane ancora il metodo di pagamento più utilizzato, nonostante l'esponenziale crescita che sta avendo lo shopping online.

2. COS' E' LA TECNOLOGIA NFC (o Near Field Communication)?

Si tratta di una tecnologia a radiofrequenza che consente di far dialogare due dispositivi a breve distanza, consentendo lo scambio di informazioni, o effettuare pagamenti sicuri. Gli ideatori sostengono che il NFC semplificherà estremamente il modo di interazione tra i dispositivi dei consumatori garantendo uno scambio di informazioni molto veloce ed in totale sicurezza.

La tecnologia NFC può essere vista come una sottocategoria all'interno dei sistemi RFID(Radio Frequency IDentification).

Con la tecnologia RFID l'identificazione avviene usando un'antenna per leggere un chip digitale (chiamato tag, o transponder) che è stato applicato sull'oggetto. Il tag contiene un certo numero di informazioni relative all'oggetto su cui è applicato (come il codice, la data di produzione, il produttore), che possono essere statiche, oppure cambiare nel corso del tempo.

I tag sono dispositivi molto semplici e compatti e si dividono in due categorie:attivi e passivi.

I tag passivi sono dei transponder a radiofrequenza costituiti da un circuito stampato sul quale trovano spazio una logica di controllo, un'antenna ed una piccola area di memoria, inoltre essi non hanno bisogno di elettricità per funzionare, grazie a un fenomeno chiamato "induzione magnetica". Quando i tag sono "stimolati" per induzione sono in grado di restituire un segnale radio contenente informazioni che si trovano nella memoria, prendendo l'energia necessaria al funzionamento del circuito dalle onde radio emesse dal reader.

Se invece è necessaria una potenza maggiore, per trasmettere a lunga distanza, il tag dev'essere alimentato da una sorgente di elettricità, come una batteria. In questo secondo caso il tag viene chiamato "attivo".

Il reader è un dispositivo più complesso, in quanto consiste a tutti gli effetti di una ricetrasmittente in grado di inviare e ricevere segnali radio su una determinata frequenza. Punto chiave della tecnologia RFID è il fatto di essere contactless, ossia i dispositivi parlano tra di loro senza contatto fisico: quando c'è un reader attivo, esso irradia lo spazio circostante con un segnale radio su una determinata frequenza e se c'è un tag nelle vicinanze, in grado di "vibrare" per risonanza a quella stessa frequenza, questo risponde, demodulando opportunamente l'onda per mezzo della sua antenna, inviando un segnale che tradotto in bits ha un significato per il ricevitore.

I tag passivi hanno una portata molto piccola, che varia in funzione della frequenza di lavoro e che generalmente è circoscritta in un intorno di spazio che va da pochi centimetri ad un massimo che non supera un paio di metri.

Inoltre come detto essi non possiedono un vero trasmettitore, ma solo un'antenna che rimodula un segnale in ingresso, quindi è lecito aspettarsi distanze operative così basse che però di norma sono più che sufficienti per gli scopi previsti.

Invece, i tag attivi poiché possiedono una batteria ed un trasmettitore vero e proprio, raggiungono distanze di lavoro che arrivano anche fino a 200 metri.

Esistono anche tag ibridi, che possono essere semi-passivi o semi-attivi. I primi hanno una batteria che generalmente alimenta alcuni sensori per scopi vari, ma in fase di trasmissione sono a tutti gli effetti dei tag passivi. Gli altri invece possiedono una batteria che alimenta un trasmettitore, ma per aumentarne la vita operativa esso è spento e si attiva, sempre per induzione, solamente quando c'è un reader nei paraggi per poi spegnersi di nuovo.

Sempre in funzione della frequenza, abbiamo differenti capacità di trasmissione, intesi come transfer rate al secondo, e nei tag più utilizzati (13,56 Mhz) siamo nell'ordine delle decine/centinaia di kbit/s. Può sembrare un valore molto piccolo, ma non dimentichiamo che ciò che il tag deve trasmettere è solamente un codice alfanumerico univoco dal quale poi il reader, appoggiandosi su servizi web e database, trae tutta una serie virtualmente infinita di informazioni.

E' molto importante anche il ruolo della memoria integrata nel tag: di solito essa è solo readonly ed è di pochi bits, giusto quel che serve a contenere un codice di qualche decina di caratteri, ma esistono applicazioni in cui abbiamo necessità di memorie read/write, come nel caso delle tecnologie di pagamento, che possono arrivare anche ad ordini di grandezza del megabyte e con transfer rate decisamente superiori.

La vita operativa di un tag è normalmente molto alta, specie per quelli passivi, in quanto sono a tutti gli effetti dei dispositivi che non consumano energia e che non si degradano quasi per nulla. C'è da dire però che spesso il tag ha una vita effettiva molto breve, in

quanto molto spesso esso “muore” nel momento in cui ciò che deve marcare raggiunge l’utente finale, e difficilmente si parla di rigenerazione o rottamazione.

Una tecnologia più evoluta ma sempre basata sul principio dell’RFID che è e sarà alla base dei sistemi di pagamento ed interfacciamento di vario tipo tra più dispositivi, come ad esempio il nostro smartphone e la cassa del supermercato è : l’ NFC.

I Near Field Communication sono dei dispositivi, solitamente embedded in altri apparecchi, che integrano le funzionalità di tag e reader nello stesso componente, permettendo a due apparati di dialogare ed interrogarsi vicendevolmente. La distanza operativa è solitamente di poche decine di centimetri, e la frequenza maggiormente utilizzata è ancora quella dei 13,56 Mhz.

Gli NFC di per sé costituiscono quindi semplicemente un meccanismo per instaurare una comunicazione sicura tra due dispositivi senza bisogno di contatto o di pin/password da digitare, sono poi le informazioni presenti altrove (sul telefono lato utente, e sui server della banca dalla parte della cassa) a permettere l’esecuzione di un pagamento piuttosto che il ritiro di denaro da un bancomat di prossima generazione.

Un cellulare dotato di tecnologia NFC (quindi di un controller NFC, un’antenna e un Secure Element) può operare in tre diverse modalità:

- Emulazione Carta Contactless
- comunicazione peer-to-peer
- comunicazione Reader/writer

Reader/writer mode

Questo modo fornisce la comunicazione di un NFC mobile con un NFC tag. Lo scopo della comunicazione è sia leggere o scrivere i dati da/o un tag dal cellulare. Noi possiamo ulteriormente classificarlo in due diversi modi: reader mode e writer mode. Nel primo il cellulare legge i dati da un NFC tag; mentre in writer mode il cellulare scrive i dati su un NFC tag.

Peer-to-peer mode

Due telefoni cellulari NFC utilizzano questa modalità di scambio dei dati tra di loro.

Ogni cellulare usa la propria energia per essere in modalità attiva.

La comunicazione bidirezionale viene effettuata in questo modo :quando un dispositivo sta trasmettendo, l’altro sa di ascoltare e può iniziare la trasmissione dei dati dopo che il primo finisce.

Carta di emulazione

Questa modalità fornisce l’opportunità di un telefonino cellulare NFC di funzionare come un contactless smart card. Alcuni esempi sono le carte di credito, di debito, carte fedeltà e così via. Un cellulare NFC può anche memorizzare più applicazioni contactless smart card contemporaneamente. La modalità di emulazione carta è una modalità importante in quanto consente il pagamento e le applicazioni di bigliettazione ed è compatibile con smart card esistenti.

Chiaramente è assolutamente cruciale la sicurezza dei dati che transitano durante transazioni di questo tipo ed infatti sono state progettate varie tecniche di sicurezza e cifratura, al fine di combattere i più comuni tipi di attacco.

3. COME SI USA?

Ecco una versione semplificata del processo di un pagamento NFC.

Questo è il protocollo utilizzato per trasmettere dati da un cellulare con tecnologia NFC, attraverso un operatore telefonico fino a raggiungere il gestore dei servizi di fiducia e poi alla banca o all'emittente della carta. Si tratta di una forma sicura di trasmissione dei dati per i pagamenti.



I numeri sulla immagine qui sopra corrispondono con la lista qui sotto.

1. Con un gesto si possono pagare beni o servizi a un commerciante. I dati vengono criptati e preparati all'invio in sicurezza.
2. L'operatore di rete mobile instrada la transazione al gestore dei servizi di fiducia con un protocollo sicuro.
3. La transazione dei dati criptati viene passata dall'operatore telefonico al responsabile del servizio di fiducia che provvede alla transazione delle richieste, decripta i dati e li passa all'emittente della carta o alla banca.
4. L'emittente della carta o la banca controlla il bilancio ed alcuni particolari di sicurezza, come ad esempio la presenza di un ID di transazione deperibile e, se tutto va bene, emette il denaro.
5. Poi i dati vengono crittografati e inviati di nuovo all'operatore telefonico attraverso tutti gli stessi meccanismi descritti in precedenza.
5. Il pagamento viene accreditato al proprio account. La transazione è stata completata.

Come possiamo vedere la tecnologia NFC semplifica e velocizza il processo di pagamento.

4. PERCHÉ USARLA?

Con queste nuove tecnologie il denaro “sonante” sarà destinato a scomparire e diventerà digitale. Ma quali saranno i vantaggi di questa rivoluzione monetaria?

Un beneficio molto importante del passaggio dalla moneta “sonante” al bits è che la prima ha costi di produzione, gestione e distribuzione, ed inoltre è più facile da falsificare nonostante i complicati meccanismi di difesa in atto.

Inoltre se tutto il denaro fosse digitale, i governi avrebbero uno strumento infallibile per sconfiggere l'evasione fiscale, in quanto ogni singolo pagamento dovrebbe necessariamente passare per dispositivi connessi al sistema bancario di turno e sarebbe difficile eseguire e ricevere pagamenti senza essere tracciato in qualche modo, e quindi evadere le tasse.

Un altro vantaggio importante è la comodità che offre questo nuovo metodo. Ci basti pensare che nei prossimi anni con il nostro cellulare in tasca potremmo tranquillamente riempire il carrello della spesa e uscire dalla porta senza fare nulla: il denaro scompare automaticamente e vengono eliminate le noiose file alle casse.

Accertata l'idea che l'utilizzo di questa nuova tecnologia sia conveniente, il passo più grande sarà convincere la gente sulla sicurezza di questo nuovo metodo. Infatti certo è che la “perdita” materiale del soldo come lo conosciamo oggi potrebbe lasciarci un senso di incompiutezza, quasi di disarmante preoccupazione per le problematiche di sicurezza. Per questo motivo analizziamo ora in dettaglio se questa nuova tecnologia è sicura.

5. MA È REALMENTE SICURO?

Dopo aver esplorato la tecnologia che sarà alla base dei futuri sistemi di pagamento, è arrivato il momento di rispondere alla domanda fondamentale: mi posso fidare?

Prima di capire come difendersi però, è assolutamente necessario capire da chi e da cosa bisogna guardarsi: come abbiamo visto infatti, la comunicazione tra tag e reader avviene mediante un'onda radio che si diffonde nello spazio e che è potenzialmente “leggibile” da chiunque sia provvisto di una banale antenna soprattutto se non è stata prevista nessuna cifratura dei dati.

I tipi di attacchi a cui siamo esposti sono di diverso tipo, e possono essere più o meno efficaci a seconda che il target sia un tag passivo, attivo od in base alla tipologia di memoria adottata. Alcuni sono più pericolosi ed altri meno, e possiamo individuare certe categorie più ricorrenti che vale la pena analizzare più nel dettaglio.

5.1 SNIFFING

5.1.1 Intercettazione

Il più rischioso degli attacchi in cui possiamo incappare, specialmente se stiamo trattando con degli NFC che servono ad eseguire pagamenti, è quello che mette un “attaccante” in grado di intercettare le nostre comunicazioni e/o clonarle.

Per operare le intercettazioni, l'aggressore usa un'antenna e un ricevitore . Quest'ultimo può operare sia ad alta sensibilità e lungo raggio sia occultando un Reader lungo la linea di produzione, sia utilizzando un dispositivo portatile. Il primo problema da risolvere sarà quindi la ricezione dei segnali, mentre il secondo problema sarà interpretare (decodificare) il significato dei segnali medesimi. La decodifica sarà un problema se la trasmissione è cifrata, altrimenti la domanda principale sarà quanto deve essere vicino l'aggressore per ricevere un segnale utilizzabile, visto che gli apparati operano generalmente in prossimità. Naturalmente non è possibile fornire una risposta univoca, ma solo un elenco di fattori da tenere in conto. Ad esempio:

- Rapporti potenza/sensibilità,
- Fattori ambientali (Caratteristiche dell'ambiente come la presenza di muri o masse metalliche, livello di rumore di fondo, ecc)
- Caratteristiche dell'antenna dell'aggressore (geometria dell'antenna, libertà di movimento della medesima, ecc.).

Un primo vantaggio però, specialmente nei tag passivi, è proprio quella della ridotta distanza operativa, per cui una lettura non autorizzata può essere possibile solamente se si è abbastanza vicini (nel raggio di pochi centimetri) al dispositivo. Questo basta già di per sé a considerarne sicuro l'uso in alcuni ambiti (ad esempio nei badge aziendali), ma di certo non sufficiente nelle transazioni bancarie di prossimità, dove le distanze operative sono anche superiori e c'è in gioco qualcosa di più importante.

Il problema nasce nei sistemi **anti-collisione**, dove il Reader trasmette con una potenza molto più alta di quella dei TAG e cio' permette di ovviare la necessità di essere molti vicini a quest'ultimo. Infatti i sistemi anti-collisione hanno lo scopo di permettere ad un reader di elaborare più tag contemporaneamente senza problemi di sovraccarichi.

Questo viene fatto mediante un procedimento, denominato binary tree, che prevede un'interrogazione del reader verso i tags un bit dopo l'altro: prima viene chiesto di rispondere a tutti i tag il cui ID inizia per 0, poi quelli per 1 e così via, ed in base alle risposte ricevute si procederà con l'interrogazione di tutti i restanti bits.

Il problema è che il reader emette un campo elettromagnetico che ha un'intensità notevolmente superiore al tag e quindi un potenziale cracker può "ascoltare" tutte queste interrogazioni ad una distanza maggiore. In altri termini: attraverso la comunicazione Reader => TAG ad alta potenza e facilmente intercettabile, si scoprono le informazioni della comunicazione TAG => Reader a bassapotenza e difficilmente intercettabile. L'aggressore quindi non vede le risposte del TAG, ma le interrogazioni del Reader svelano lo stato della ricerca binaria anche a lunga distanza

Pertanto, anche TAG che operano a cortissimo raggio potrebbero essere invece vulnerabili sfruttando l'algoritmo anticollisione, ma soprattutto potrà dedurre la risposta dei tags semplicemente sapendo che cosa sta chiedendo il reader, anche se la distanza operativa è di pochi centimetri, ricostruendo per intero i messaggi originali.

I tag attivi invece, sono naturalmente ben più esposti a letture fraudolente a causa proprio della loro elevata distanza di trasmissione, ragion per cui i dati vengono cifrati con varie tecniche che esploreremo in seguito.

5.1.2 Clonazione

La clonazione è invece una tecnica che prevede la copiatura bit a bit dei dati contenuti nel tag, in modo da poterne costruire di fasulli che “impersonano” quello originale. In questi casi, anche le tecniche di cifratura più avanzate falliscono miseramente, in quanto è sufficiente avere a disposizione un tag “vergine” simile a quello che vogliamo emulare, intercettare l'intero contenuto dell'originale e copiarlo integralmente. Cifratura o no, i due tag saranno indistinguibili e potrei tranquillamente pagare gli acquisti utilizzando il conto di un altro. Saranno necessarie tecniche più avanzate di mutua autenticazione, ed anche queste saranno trattate più dettagliatamente insieme a quelle di cifratura.

5.2 TAMPERING E SPOOFING

Nel gruppo degli attacchi che alterano i dati originali, troviamo principalmente due tipologie di attacco: quelle mirate a sovrascrivere la memoria del tag con dati fasulli (tampering), e quelle indirizzate verso la falsificazione delle informazioni trasmesse (spoofing). Ci sono delle necessità per cui il tag deve avere una memoria riscrivibile, possibilità che espone a sovrascritture non autorizzate e certamente pericolose.

TAG TAMPERING

Tampering assume il significato di “modifica non autorizzata delle informazioni (in memoria)”. Questo tipo di attacco mira a modificare i dati che sono presenti nella memoria del tag. La possibilità di riuscire a compiere questo attacco dipende dalle caratteristiche di protezione con cui le informazioni vengono scritte nel tag. Il tampering è infatti favorito se il tag non ha protezioni (password) che ne inibiscono la scrittura oppure se nel tag ci siano informazioni articolate sul prodotto (ad es. data di scadenza o composizioni), è tutto in chiaro. I possibili effetti di questo attacco dipendono dalla tipologia delle informazioni riportate sui tag e dal grado di integrazione dei sistemi, potendo tali informazioni essere costituite da codici di accesso a banche dati riservate ed anch'esse protette.

Un modo per proteggersi dal tampering è l'applicazione delle più idonee tecniche crittografiche e di sicurezza per proteggere i dati scritti.

DATA SPOOFING

Spoofing significa “attacco mirato a far credere il falso, in particolare alla contraffazione di identità per mezzo della falsificazione dei dati trasmessi (del tag o del reader)”.

Questo tipo di attacchi modificano i dati in transito, generalmente nella comunicazione tag→reader e vi sono diverse modalità:

5.2.1 Data corruption

In questo attacco l'aggressore cerca di disturbare la comunicazione, poiché in questo caso non è in grado di interpretare i dati ed alterarli.

Il disturbo viene in genere realizzato trasmettendo a tempo debito e nelle frequenze corrette.

Il tempo debito può essere calcolato dall'aggressore attraverso lo studio del sistema di modulazione e codifica del sistema sotto attacco. Con questo tipo di attacco in realtà vi è solamente un disturbo del servizio attuabile per breve tempo e funzionale ad azioni di altro tipo.

Una possibile contromisura consiste nell'ascolto da parte di un sistema indipendente di controllo, attrezzato meglio di un reader commerciale, per percepire la situazione e dare l'allarme.

5.2.2 Data modification

L'aggressore cerca di modificare i dati in transito in modo che vengano ricevuti alterati.

In questo caso i dati vengono ricevuti come validi (anche se manipolati).

Questo attacco dipende dall'indice di modulazione utilizzato da chi trasmette e dalla tecnica di decodifica. Per questo attacco la contromisura consiste nell'allestimento di un canale sicuro oppure con l'utilizzo di un altro dispositivo NFC che controlla il campo di radiofrequenza durante l'invio e se percepisce un attacco lo interrompe.

5.2.3 Data inserction

In questo tipo di attacco vengono inseriti messaggi apparentemente corretti tra i dati scambiati tra i due apparati.

L'aggressore in questo caso inserisce il proprio messaggio prima della risposta dell'apparato giusto.

L'attacco è riuscito solo se il messaggio verrà trasmesso prima che l'apparato interrogato inizia a rispondere. Se i due flussi di dati si sovrapponevano i dati verrebbero ricevuti come non validi e l'attacco fallirebbe.

Per questo tipo di attacco ci sono tre contromisure:

1. La prima consiste nel ridurre il ritardo della risposta dell'apparato interrogato sino a rendere impossibile l'attacco.
2. La seconda consiste nell'ascolto del canale da parte di un terzo dispositivo per un tempo considerevole. Se per una interrogazione ci sono più risposte l'attacco viene scoperto.
3. La terza consiste nell'allestimento di un canale sicuro.

5.2.4 Man-in-the Middle-Attack

In questo attacco due apparati (A,B), che si stanno scambiando i dati, sono ingannati da un terzo estraneo attraverso una conversazione a tre. Durante l'attacco A e B pensano di parlare tra loro poiché l'aggressore simula, alterandoli, i dati di entrambi. In questo caso l'allestimento di un canale sicuro non basta. Infatti i due apparati dovrebbero concordare una chiave segreta che useranno per cifrare i dati. Tuttavia l'aggressore può decidere una chiave con A e un'altra con B e può tranquillamente continuare a comunicare e alterare i dati con i due dispositivi.

Nel caso però della tecnologia NFC la comunicazione avviene tra due apparati attivi oppure tra uno attivo e uno passivo.

Nel primo caso il campo di radiofrequenza è generato dall'apparato che sta inviando i dati, nel secondo viene generato dall'apparato attivo.

Assumendo che l'apparato A si comporti come attivo e l'apparato B come passivo, si genera la seguente situazione:

- L'apparato A genera un campo RF (Radiofrequenza) per inviare i dati a B.
- L'aggressore intercetta i dati e disturba la trasmissione in modo che l'apparato B non la decodifichi.
- Se l'apparato A si accorge del disturbo, interrompe la trasmissione della chiave segreta e l'attacco non può continuare.
- Se l'apparato A non si accorge del disturbo, lo scambio di chiavi continua con l'aggressore.
- Nel prossimo passo, l'aggressore deve inviare i dati a B, questo costituisce un problema perché, comportandosi B come passivo, A continua a trasmettere il campo RF e l'aggressore, che deve emettere i propri (falsi) dati, ha difficoltà ad allineare le due emissioni .

In questo modo è difficile che B decodifichi i (falsi) dati dell'aggressore.

L'altra situazione possibile è che entrambi gli apparati A e B si comportino come attivi, si genera la seguente situazione:

- Anche in questo caso l'apparato A genera un campo RF per inviare i dati a B e l'aggressore intercetta i dati e disturba la trasmissione in modo che l'apparato B non la decodifichi.
- Se l'apparato A si accorge del disturbo, interrompe la trasmissione della chiave segreta e l'attacco non può continuare.
- Se l'apparato A non si accorge del disturbo lo scambio di chiavi continua con l'aggressore.
- A prima vista sembra che l'inganno possa funzionare perché (in una comunicazione tra due apparati attivi) ora l'apparato A ha spento il RF. Quando però l'aggressore accende il proprio campo RF per inviare i dati a B, A che si aspetta la risposta di B, si può accorgere dell'inganno e bloccare il protocollo.

Le raccomandazioni, in questo caso, sono di preferire la comunicazione attivo/passivo.

Inoltre l'apparato attivo dovrebbe restare in ascolto per rilevare eventuali anomalie generate da eventuali aggressori e bloccare lo scambio delle chiavi.

6. COME DIFENDERSI?

Arrivati a questo punto si può pensare che questa nuova tecnologia NFC sia molto insicura e soggetta ad attacchi. La situazione è in realtà più rosea, in quanto oltre alla già citata cifratura è sufficiente instaurare dei solidi meccanismi di mutua autenticazione, per mettersi al riparo da tentativi di sniffing, di clonazione e di tutte le altre problematiche. Uno dei problemi fondamentali quando si parla di integrare policy di sicurezza negli NFC, è sempre l'estrema difficoltà tecnica di trovare un buon compromesso tra costi, robustezza e richieste energetiche. Più un sistema è sicuro e più sarà certamente costoso, senza contare che sarà necessario avere circuiti con più potenza elaborativa e quindi richieste energetiche da supplire con batterie più grandi quando si hanno tag attivi, con molti più compromessi invece nei tag passivi.

Sottolineiamo anche come in molti casi non sia necessario avere protocolli di sicurezza avanzati, e pertanto ci si può accontentare di piccoli accorgimenti od addirittura di lasciare tutto "aperto", ma nella nostra analisi abbiamo contestualizzato il caso dei pagamenti tramite NFC dove certamente è necessario avere un livello di sicurezza elevatissimo. Come anticipato, questo livello di sicurezza si ottiene solamente usando all'unisono tecniche avanzate di autenticazione e di cifratura mediante l'allestimento di un canale sicuro.

6.1 AUTENTICAZIONE

Esistono due tipi di autenticazione: quella passiva e quella attiva.

6.1.1 Autenticazione passiva

Consiste nell'apposizione della firma digitale sui dati che sono nel tag.

Nella firma digitale l'"impronta", generata con la funzione hash, viene cifrata con la chiave privata del firmatario per produrre quella che si definisce la firma digitale associata alla stringa (documento), nei casi in questione memorizzata nel TAG.

All'atto della lettura del TAG, per verificare la firma, questa viene decifrata con la chiave pubblica, ottenendo l'impronta della stringa originaria; quindi la verifica si completa ricalcolando l'impronta della stringa sotto verifica e riscontrando l'uguaglianza delle due impronte.

Il metodo è adatto ai tag passivi a basso costo poiché richiede solamente la presenza uno spazio in memoria per la firma. Infatti l'elaborazione dei dati è interamente a carico del Reader sia in fase di scrittura che in fase di lettura.

Con questo modo i dati contenuti nel tag dovrebbero risultare immuni da alterazioni.

Purtroppo però questo tipo di autenticazione non contrasta la clonazione poiché si possono copiare i dati assieme alla firma.

6.1.2 Autenticazione attiva

È una caratteristica dei sistemi ad elevato grado di sicurezza nei quali, oltre alla validazione dei dati, devono essere evitate letture fraudolente dei tag per evitare clonazioni. Esistono due particolari tecniche di autenticazione: Mutual Symmetrical Keys (MSK) e Derived Keys (DK)

Mutual Symmetrical Keys

il protocollo prevede che entrambi i soggetti (tag e Reader) verifichino reciprocamente la conoscenza di una chiave segreta.

Questo protocollo fa parte di quelli del tipo “challenge-response”, che definiscono lo scambio di uno o più messaggi tra l’entità che vuole dimostrare la sua identità (claimant) e l’entità che deve verificarla (verifier).

In uno scenario tipico il verifier invia al claimant un messaggio contenente un valore imprevedibile (pseudocasuale) ed il claimant è richiesto di inviare un messaggio di risposta che dipende dal suddetto valore e dal segreto condiviso (chiave segreta di cui entrambe le entità sono a conoscenza).

Dopo tale fase di mutua autenticazione le comunicazioni tra le due entità avvengono in modalità criptata (con l’impiego della chiave segreta di cui sono entrambe a conoscenza).

Derived Keys

Questa tecnica è molto usata per la sua semplicità e consiste nel derivare una chiave personalizzata per ogni coppia di apparati che comunicano, senza una vera e propria procedura di autenticazione.

In questo caso la chiave personalizzata viene creata a partire da un parametro non segreto (ovvero il numero di serie del tag che è unico nel mondo), che viene richiesto e trasmesso pubblicamente e da un segreto condiviso che non viene mai trasmesso poiché è contenuto nel firmware in tutti gli apparati. Poiché il tag conosce il proprio numero di serie e il segreto condiviso può risalire alla chiave personalizzata.

Un aggressore in ascolto intercetterebbe l’identificativo del tag ma non potrebbe risalire alla chiave personalizzata non conoscendo il segreto condiviso.

Questa tecnica ha il vantaggio di richiedere scarsa elaborazione da parte del tag.

6.2 CRIPTAZIONE DEI DATI-ALLESTIMENTO DI UN CANALE SICURO

In generale una volta conclusa l’operazione di autenticazione avviene la cifratura, che è la misura principale per potersi difendere dagli attacchi esterni.

Infatti i dati che non vengono protetti possono essere intercettati e modificati.

Spesso, inoltre, la cifratura viene effettuata con le chiavi oggetto della precedente procedura di autenticazione.

La differenza fondamentale tra il canale sicuro e la semplice applicazione di una funzione hash (anche con firma elettronica) ai dati del TAG consiste nel fatto che, nel canale sicuro viene effettuato, volta per volta uno scambio di chiavi e la cifratura dei dati si opera on line. Prima della trasmissione i dati sono cifrati usando la chiave segreta K; il ricevitore successivamente decifra i dati cifrati usando la chiave K'. Se le chiavi K e K' sono identiche (o in relazione reciproca) l'algoritmo si dice simmetrico, altrimenti la procedura è definita asimmetrica.

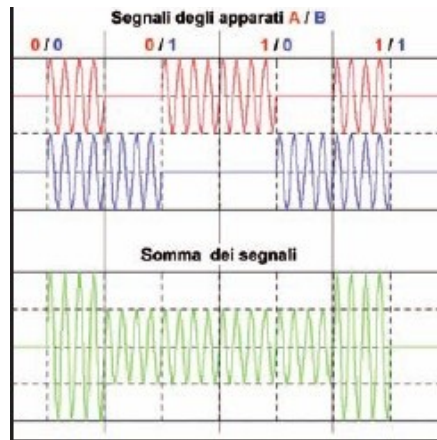
La creazione di un canale sicuro è certamente la migliore procedura per proteggere i dati dell'intercettazione, dall'alterazione degli stessi o dall'inserimento di falsi messaggi. Per fare ciò si possono usare algoritmi a chiave simmetrica come il DES, il 3DES o l'AES oppure si può la cifratura asimmetrica che può far uso degli algoritmi come l'RSA, le Curve Ellittiche od il Diffie Helmann. Per tutti questi casi rientriamo nelle consuete casistiche di sicurezze proprie di tutti gli altri sistemi informatici, dall'online banking ai vari servizi della PA, pertanto non ci soffermeremo sui punti di forza o le debolezze di questi già diffusissimi sistemi di cifratura.

6.2.1 Una proposta per scambio chiavi

Sempre a proposito dell'allestimento di un canale sicuro è apparsa di recente una proposta originale di scambio di chiavi per la tecnologia NFC, anche se non è contemplata nello standard ISO sugli NFC medesimi.

L'idea di base è che gli apparecchi che comunicano (tag e reader) si mandino contemporaneamente dati casuali. Nella fase di setup iniziale i due apparati sincronizzano ampiezza e fase dei segnali così come l'esatta temporizzazione dei bit trasmessi. Dopo la sincronizzazione i due apparati possono inviare dati esattamente nello stesso istante e con la medesima ampiezza e fase.

Questo è estremamente vantaggioso perché d'ora in poi, ogni volta che i due attori inviano lo stesso bit, ad esempio 0, l'onda risultante è data dalla somma dei due segnali cioè sempre 0, nel caso invece di 1 si ottiene un segnale con intensità doppia. Nel caso di segnali discordanti invece, quando ad esempio il tag invia uno 0 ed il reader un 1, si ottiene sempre un segnale di intensità pari ad uno. Se ci mettiamo nei panni di un cracker che ascolta la nostra comunicazione otteniamo qualcosa come quello mostrato in figura:



In pratica senza sapere chi ha inviato che cosa, non è possibile ricostruire il messaggio che risulterà sempre uguale “all'esterno” indipendentemente da quale dei due apparecchi abbia inviato lo 0 e l'1. Solo i veri tag e reader, sapendo cosa hanno inviato loro stessi, lavorando per “differenza”, potranno ricostruire il messaggio originale e potranno dialogare in tutta sicurezza.

Con questo metodo ogni tentativo di clonazione o contraffazione fallisce miseramente!

A questo punto, qualunque metodo sia stato scelto, abbiamo reso tag e reader consapevoli di essere autentici e siamo pronti ad instaurare una comunicazione cifrata.

7. CONCLUSIONI

Ora che sappiamo quale sarà la tecnologia che muoverà i sistemi di pagamento del prossimo futuro (e non solo visto che gli usi di tale tecnologia sono vastissimi) ed abbiamo anche cercato di capire quanto siano sicuri utilizzando le migliori tecniche fin qui esposte e molte altre ancora, possiamo concludere che la sicurezza si può ottenere e il denaro digitale rimarrà ben protetto forse ancor di più di quello di “carta”. In futuro rubarci il portafoglio non servirà a nulla, in quanto la tecnologia NFC funzionerà solo con i nostri parametri biometrici ed i dati in essa contenuti saranno ben cifrati ed al sicuro.

L'intercettazione a distanza sarà complessa grazie alla mutua autenticazione, cosicché potremmo andare in giro sereni con il nostro cellulare NFC senza alcuna paura.

Certamente la sicurezza al 100% non esiste, e tutto può essere sempre bypassato al pari di quanto lo sia già oggi con i sistemi tradizionali. Ma la scienza va sempre avanti, i sistemi di pagamento cambieranno e diventeranno completamente elettronici, ed è bello sapere come di pari passo avanzino anche le tecniche di sicurezza, rendendoci felici e tranquilli utilizzatori dei mezzi digitali del futuro.

8. BIBLIOGRAFIA

- **RFID Fondamenti di una tecnologia silenziosamente pervasiva** di Paolo Talone e Giuseppe Russo
- **Near Field Communication: From Theory to Practice** di Vedat Coskun, Kerem Ok and Busra Ozdenizci
- **www.nfcrumors.com**
- **www.stolpan.com**
- **La tecnologia NFC** (Seminario) del Prof. Carlo Maria Medaglia