Sempre più spesso online si trovano articoli o post che mettono fortemente in dubbio la sicurezza del Mobile Payment tramite tecnologia NFC, rilanciando notizie e spunti provenienti dall'estero e presentando in modo acritico ipotetici scenari di furto delle credenziali di pagamento che saranno scambiate via Mobile NFC.

Come Osservatorio NFC & Payment della School of Management del Politecnico di Milano abbiamo lavorato su questi e altri temi da oltre 4 anni, in stretta cooperazione con i colleghi del Dipartimento di Elettronica, Informazione e Bioingegneria del Politecnico di Milano; vogliamo dunque dare il nostro punto di vista e fare chiarezza sui "falsi miti" che leggiamo troppo spesso, affinché siano veicolati i messaggi corretti che possano porre ogni utente nella migliore condizione di conoscere questi nascenti servizi.

In primis definiamo cosa è il Mobile Proximity Payment tramite NFC: è un servizio di disposizione di pagamento attivato avvicinando un telefono cellulare dotato di tecnologia NFC ad un POS contactless. Al telefono cellulare deve essere associato uno strumento di pagamento elettronico (ovvero una carta di credito o di debito o una carta prepagata) legato ai circuiti di pagamento comunemente utilizzati (Mastercard o Visa). Le credenziali di pagamento sono memorizzate in un "posto sicuro", il cosiddetto Secure Element, dunque un hardware fisicamente separato (che può trovarsi nel telefono o sulla SIM) a cui possono accedere solo applicazioni certificate e dotate di specifici privilegi.

Dal punto di vista del mercato, a fine 2012 in Italia abbiamo stimato ci siano 2,5 milioni di utenti (meno del 5% degli utenti che in Italia hanno un telefonino) con un telefonino dotato di tecnologia NFC e circa 30.000 POS contactless attivi (meno del 2,5% del totale dei POS attivi in Italia): questi numeri cresceranno, secondo le nostre previsioni, in modo esplosivo nei prossimi anni, creando quella infrastruttura (lato domanda e lato offerta di servizi) indispensabile per portare alla piena circolarità questa nuova generazione di strumenti di pagamento.

Proviamo ora a dare qualche risposta, volutamente semplificata, ai dubbi che più volte sono stati sollevati.

Un malintenzionato dotato di un'antenna direttiva con un alto guadagno, un amplificatore di segnale e un ricevitore di qualità è in grado di intercettare i dati di pagamento NFC in un raggio di 10 metri?
Considerando la frequenza e la potenza operativa dello standard NFC, la distanza massima che consente di effettuare l'eavesdropping (termine tecnico di intercettazione dei segnali radio e decodifica dei dati trasmessi) è di **10m** (con l'ausilio di antenne direttive con alto guadagno, amplificatore di segnale, ecc.) **solo** se entrambi i dispositivi NFC funzionano in **modalità attiva**, ovvero trasmettono dati (come nel caso del pairing effettuato attraverso l'NFC tra due dispositivi). Nel caso in cui uno dei dispositivi NFC funzioni in modalità passiva (ovvero si ponga in ascolto della comunicazione iniziata da un altro dispositivo, e risponda di conseguenza), la distanza massima che consente l'eavesdropping crolla a **1m**.
Questo punto è essenziale, dal momento che nei pagamenti NFC, solo il POS lavora in modalità attiva, mentre il dispositivo mobile lavora in modalità card-emulation, che corrisponde ad una modalità di comunicazione passiva. In altri termini, il telefono opera come una qualsiasi carta di pagamento contactless (a fine 2012, ne circolavano in Italia circa 2 milioni) e risponde con la sola energia raccolta dalla comunicazione del dispositivo interrogante (il POS).
Un malintenzionato potrebbe dunque "origliare" i dati veicolati dal POS fino a 10m, ma i dati veicolati dal telefonino NFC possono essere colti solo fino ad un massimo di 1m. Quindi, per poter ascoltare l'intera "conversazione" tra i due dispositivi, cosa necessaria per carpire le credenziali scambiate, dovrebbe posizionare il suo sistema di eavesdropping (ingombrante e visibilissimo, per

via delle antenne ad alto guadagno) a meno di 1m dal POS, situazione del tutto inverosimile in un scenario reale. Questa precisazione, indispensabile per una reale comprensione dello scenario di attacco, è regolarmente omessa dalla descrizione data nei media.

Si stanno diffondendo soluzioni come "NFCproxy" che consentono di intercettare i segnali radio; i pagamenti NFC sono davvero al sicuro da attacchi con queste soluzioni?
Facciamo una premessa: un altro possibile scenario di attacco è quello cosiddetto di tipo *Man in The Middle*, in cui un hacker che si interpone nella conversazione tra un client e un server, inganna il server facendo da "passaparola" delle informazioni trasmesse dal client e nel frattempo carpendo l'informazione di interesse.
E' stato ampiamente dimostrato che questi attacchi sono impraticabili nel caso di pagamenti NFC, grazie alle scelte tecniche e protocollari fatte dai progettisti della soluzione. Un attacco di questo tipo funziona infatti solo se si soddisfano contemporaneamente i seguenti requisiti:

- il dispositivo "malintenzionato" dovrebbe essere posto tra il POS e il telefonino NFC, assicurandosi che **il POS e il telefonino non riescano a comunicare direttamente**, altrimenti si accorgerebbero dalla presenza di un terzo che "ripete la conversazione". Dal momento che la tecnologia NFC ha una distanza massima di funzionamento di pochi cm (basti pensare all'esperienza comune, ad esempio alle tessere del trasporto pubblico urbano) è impensabile che si interponga fisicamente un dispositivo maligno tra i due, senza che esso sia visto;
- il dispositivo maligno, in ogni caso, dovrebbe rispondere al POS in modo tempestivo in modo che la transazione non vada in timeout, e al tempo stesso schermare la comunicazione diretta telefono - POS. Già la prima di queste due condizioni è poco realizzabile, dal momento che se i dati vengono veicolati attraverso un link wireless (WiFi), come nel caso di NFCProxy, i tempi di risposta del dispositivo maligno sarebbero incompatibili con i tempi di risposta imposti dal protocollo, che sono tenuti strettissimi proprio per avere la certezza che la comunicazione sia interamente avvenuta attraverso il canale NFC, che è un canale di prossimità (come dice l'acronimo stesso, Near Field Communication).

Se un malintenzionato tenesse attivo il proprio ricevitore NFC in posti affollati dove ci si ritrova molto vicini, come in bus, metrò, etc., potrebbe impossessarsi di informazioni di telefoni NFC?
La possibilità di appropriarsi dei dati di una carta di pagamento (il cosiddetto skimming) semplicemente avvicinando un lettore al telefonino è del tutto inverosimile per molti motivi. In primo luogo, l'applicazione di pagamento che ha i privilegi per accedere al SE deve essere attivata dall'utente (come una normale applicazione) e mantiene i diritti di accesso al SE entro un certo time-out, generalmente posto in 60 secondi, trascorsi i quali essa va riattivata con un click. Infine, la piramide di sicurezza prevede che solo transazioni molto piccole (generalmente inferiori a 25€) e per cumulati di spesa molto contenuti (generalmente fino ad un massimo cumulato di 50€) possano avvenire senza l'inserimento di un PIN, così da replicare la praticità d'uso del contante, ma controllando comunque l'accumulo di transazioni. Questi parametri possono anche essere personalizzati dall'utente (in senso più restrittivo) impostando che la propria applicazione richieda un PIN per soglie più basse.
Il complesso di questi elementi porta facilmente a capire come il pagamento via Mobile NFC sia molto sicuro, perché tale sicurezza è costruita attraverso una serie di elementi di controllo che sono radicati nelle scelte hardware, protocollari e applicative che sono state fatte.

Se ci sono interferenze/intercettazioni nella rete cellulare è possibile che un malintenzionato possa rubare i dati dello strumento di pagamento di un utente di un servizio di Mobile Payment? E se durante una transazione di Mobile Payment il pagante riceve un Sms o una chiamata è possibile che si generino errori o problemi?

Durante un pagamento NFC, le informazioni vengono scambiate non attraverso la rete cellulare, ma, per l'appunto, attraverso una comunicazione NFC tra il POS e il cellulare, quindi non si possono generare interferenze tra i due canali di comunicazione (quello GSM e quello NFC), mentre il conflitto tra applicazioni (di chiamata o messaging vs. di pagamento) è del tutto inverosimile. Inoltre, il "Single Wire Protocol", ovvero il protocollo fisico di comunicazione tra la SIM e il cellulare, permette che la SIM possa essere utilizzata contemporaneamente per chiamare (ad esempio conversando con un auricolare bluetooth) e per effettuare un pagamento.

È possibile che il telefono cellulare venga clonato?
L'elemento di sicurezza che contiene le credenziali è, come già detto, il Secure Element, ovvero un elemento fisico separato e sicuro. Esiste sempre la possibilità che i dati del SE possano essere estratti, o il SE clonato, così come anche le carte tradizionali con chip possono essere (con difficoltà) clonate. La domanda è: quanto è difficile farlo? Quanto è probabile che ciò avvenga senza che i sistemi di sicurezza che sono parte stessa del protocollo di pagamento (e.g. il PIN) vengano violati? O senza che i servizi di sicurezza accessori avvertano l'utente (ad esempio i servizi di SMS alerting)? Ancora una volta, è evidente a un qualsiasi soggetto che approcci obiettivamente la materia, che un telefonino, essendo un oggetto più intelligente di una carta di plastica, può solo innalzare il livello complessivo di sicurezza; se dunque vi è fiducia nell'utilizzo dei tradizionali sistemi di pagamento, a maggior ragione dovrebbe esservene nel nuovo strumento.

È possibile che ad essere compromesso sia il POS di un esercente, generando un pagamento verso terzi senza il consenso di acquirente e venditore?
E' teoricamente possibile, benché di difficile implementazione, proprio perché i POS per funzionare devono essere allacciati ad un circuito, che li identifica, censisce, ed autorizza ad operare. In ogni caso, ammesso che ciò possa avvenire, il rischio a cui è soggetto l'utente con telefono NFC è ancora una volta pari a quello di un utente che usi uno strumento di pagamento elettronico (bancomat o con carta di credito) tradizionale. La tecnologia NFC non comporta alcun cambiamento, rispetto a questo livello di rischio sottostante.

In conclusione il Mobile Proximity Payment ha livelli di sicurezza pari o superiori a quelli degli altri strumenti di pagamenti elettronici Card Present (quindi non pagamenti online) garantiti dai circuiti Visa e Mastercard.
Ovviamente la sicurezza assoluta è intrinsecamente irraggiungibile, e potranno sempre verificarsi truffe che riguardano strumenti elettronici di pagamento (che avvengono anche e in misura maggiore utilizzando il contante). Rispetto al contante, la moneta elettronica ha maggiori strumenti di tutela, e le banche o altri soggetti emettitori si assumono spesso in prima persona il rischio di possibili frodi, risarcendo (completamente o quasi) i clienti vittime di frodi.

I dati pubblicati dal Dipartimento del Tesoro nel "Rapporto statistico sulle frodi con le carte di pagamento" mostrano chiaramente che pagare con bancomat, carte di credito e carte prepagate in Italia sta diventando sempre più sicuro: le frodi infatti con carte di pagamento sono in netta diminuzione e nel 2011 si sono registrate 284.339 "transazioni non riconosciute" per un valore di soli 52 milioni di euro, contro le 319.818 registrate nel 2010 corrispondenti a circa 60 milioni di euro di valore. Il tasso di frode per l'Italia nel 2011 (valore del frodato sul totale delle transazioni effettuate) risulta quindi pari a 0,0196% (in diminuzione, rispetto al tasso del 2010), molto inferiore all'analogo valore di UK (0,061%), Francia (0,061%) e Australia (0,051%). Oltre che rispetto al valore, anche rispetto al numero delle transazioni fraudolente il fenomeno risulta in calo, essendo la percentuale di operazioni non riconosciute nel 2011 sul totale delle transazioni effettuate scesa allo 0,0121%, circa il 14% in meno sul 2010, segno che le ultime innovazioni (carte con chip rispetto

alla banda magnetica, utilizzo di PIN e ulteriori conferme per acquisti online, servizi di alerting etc.) stanno lavorando efficacemente.

In tutto questo, forse sarebbe bene richiamare l'attenzione generale sulla sensibilità che ogni utente dovrebbe mostrare rispetto all'uso che fa del proprio smartphone, che diventa un crocevia delle nostre relazioni e delle nostre informazioni personali, anche riservate. È esperienza di tutti, in tal senso, come molti utenti continuino ad utilizzare il proprio smartphone senza proteggere con password lo sblocco e l'uscita dalla condizione di stand-by. Forse, accanto agli articoli che paventano il furto delle credenziali di pagamento, sarebbe importante aggiungere un vademecum per l'uso accorto di questo dispositivo, che è altrettanto importante, personale e sensibile, del nostro PC.

Osservatorio NFC & Mobile Payment:
Giovanni Miragliotta
Valeria Portale

Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB):
Antonio Capone
Stefano Zanero