UNIVERSITÀ DEGLI STUDI
DI GENOVA

Rapporto Tecnico

Analisi e Valutazione della Sicurezza delle Applicazioni per il Mobile Banking

Versione 1.0 - 12 ottobre 2017

TLP AMBER

In collaborazione con Talos s.r.l.s:

UNIVERSITÀ DEGLI STUDI
DI GENOVA

CERTFin
CERT Finanziario Italiano

Rapporto Tecnico

Analisi e Valutazione della Sicurezza delle Applicazioni per il Mobile Banking

Alessandro Armando[123], Gabriele Costa[13], Alessio Merlo[13],
Giorgio Orlandi[4], Monica Pellegrino[4], Romano Stasi[4], Luca Verderame[3]

Abstract

Le applicazioni mobili stanno diventando il canale preferenziale per l'accesso alle diverse tipologie di servizi, inclusi quelli bancari. Ciò spinge le banche a un continuo aggiornamento delle App prodotte e delle relative funzionalità in esse presenti, nell'ottica di garantire un'elevata user experience e rispondere alle esigenze della clientela. Al contempo, la criticità sotto il profilo della sicurezza delle operazioni che possono essere effettuate tramite le App di Mobile Banking, combinata con l'incessante evoluzione tecnologica dei dispositivi su cui vengono eseguite, impone un livello di attenzione particolarmente elevato.

Il presente documento, realizzato attraverso una collaborazione tra il laboratorio Computer Security Lab dell'Università degli Studi di Genova e il CERT Finanziario Italiano (CERTFin), con il contributo della società di cybersecurity Talos, descrive una metodologia open source per il *vulnerability assessment* e *penetration testing* dedicata alle applicazioni mobili e discute i risultati di una campagna di test effettuata sulle principali applicazioni per il Mobile Banking disponibili sui mercati italiano, tedesco e britannico. Oltre ad una descrizione dettagliata delle vulnerabilità scoperte dall'analisi rispetto ai controlli presi in esame nello studio condotto a maggio 2017, e dell'impatto conseguente al loro sfruttamento da parte di malintenzionati, il presente documento illustra le possibili contromisure per mitigare o eliminare il rischio di attacchi, con l'obiettivo di sensibilizzare gli stakeholder preposti allo sviluppo e alla verifica della sicurezza delle applicazioni mobili, favorendo la mitigazione e la prevenzione delle vulnerabilità presenti. Il presente studio può costituire il punto di partenza per sviluppare ulteriori analisi sulle applicazioni e valutare eventuali correlazioni con le previsioni normative in materia di sicurezza dei pagamenti che entreranno in vigore nei prossimi mesi.

[1] CSEC Lab, DIBRIS, Università degli Studi di Genova
[2] Security & Trust, Centro per le Tecnologie dell'Informazione, Fondazione Bruno Kessler
[3] Talos s.r.l.s
[4] ABI Lab - CERTFin (CERT Finanziario Italiano) – Direzione Operativa

Sommario

1. L'evoluzione dei servizi Mobile nel contesto bancario 3
1.1. Il livello di diffusione e di utilizzo del canale e dei servizi di Mobile Banking 3
1.2. Mobile Banking e Sicurezza 4
2. Metodologia di Analisi 7
2.1 Analisi di Sicurezza delle Applicazioni Mobili 7
2.2 Definizione della metodologia per il report 9
2.2.1. Descrizione del Campione scelto 9
2.2.2. Descrizione delle modalità di analisi 10
2.2.3. Focus Classi di Minaccia e Controlli 10
3. Risultati dell'Analisi 13
3.1 Controllo di Root Detection 13
3.2 Controllo di Protezione del Canale 14
3.3 Controllo di Confidenzialità del Canale 16
4. Conclusioni e prossimi passi 18
About Us 19

Indice delle Figure

Figura 1: Elenco delle principali categorie di verifica delle minacce di sicurezza definite dallo OWASP MASVS 8
Figura 2: Classifica OWASP delle principali categorie di rischi di sicurezza per dispositivi mobile 9
Figura 3: Presenza di controlli di integrità del dispositivo nelle App di Mobile Banking (Italia) .. 13
Figura 4: Presenza di controlli di integrità del dispositivo nelle App di Mobile Banking - comparazione tra Italia, Inghilterra e Germania 14
Figura 5: Protezione del canale - Presenza di SSL Pinning nelle App di Mobile Banking (Italia) 15
Figura 6: Protezione del canale - Presenza di SSL Pinning nelle App di Mobile Banking - comparazione tra Italia, Inghilterra e Germania 16
Figura 7: Confidenzialità del canale - Livelli di cifratura delle comunicazioni di rete nelle App di Mobile Banking (Italia) 17
Figura 8: Confidenzialità del canale - Livelli di cifratura delle comunicazioni di rete nelle App di Mobile Banking - comparazione tra Italia, Inghilterra e Germania 17

1. L'evoluzione dei servizi Mobile nel contesto bancario

I dispositivi mobili hanno cambiato profondamente le abitudini e gli stili di vita dei cittadini al punto che qualsiasi impresa e organizzazione che voglia avviare a consolidare una relazione con un target di utenti in modalità digitale non può prescindere dalla definizione di una specifica offerta Mobile.
L'attenzione del settore bancario su questa tematica è pertanto molto elevata, con l'obiettivo di costruire un'offerta evoluta di servizi sfruttando le potenzialità dei dispositivi mobili e secondo un percorso di innovazione che ha un ritmo particolarmente elevato.

1.1. Il livello di diffusione e di utilizzo del canale e dei servizi di Mobile Banking

Secondo le analisi[5] condotte dall'Osservatorio Mobile Banking di ABI Lab in collaborazione con la School of Management del Politecnico di Milano, nel mese di marzo 2017 sono stati 28,2 milioni gli utenti che si sono connessi ad Internet almeno una volta da un dispositivo mobile: un valore in crescita, se si considera che a marzo 2016 era pari a 25,3 milioni, mentre a marzo 2015 a 20,9 milioni, che corrisponde ad un incremento del 11.5 % rispetto al 2016 e del 34.9 % rispetto al 2015.

Per quanto riguarda la fruizione della specifica offerta bancaria, nel 2016 sono stati 5,6 milioni gli utenti attivi sul canale di Mobile Banking (su un campione di 18 banche/gruppi rispondenti), con un aumento dell'11% del numero di clienti da tablet e smartphone (questi ultimi guidano il trend con un +22% rispetto all'anno precedente). Interessante notare che gli utenti attivi da smartphone sono stati nel 2016 pari al 34% degli utenti da PC, con una crescita di 5 punti percentuali rispetto al 2015.

Dal punto di vista della frequenza di utilizzo, dalle analisi condotte emerge che un cliente attivo su canale Mobile accede in media nel corso di un anno 92 volte ai servizi (circa 7-8 volte al mese); anche in questo caso, tale valore è in crescita, in dettaglio, del 35% rispetto al 2015 (anno in cui sono stati registrati 68 accessi annuali per utente).

Tra gli utenti Mobile, la percentuale di coloro che effettuano disposizioni è pari al 71% del totale, con un aumento di 9 punti percentuali rispetto al 2015; inoltre l'86% svolge sia operazioni dispositive che informative, mentre il 12% del campione opera solo a livello informativo. Il 58% degli utenti operativi accede per fini informativi almeno una volta a settimana; tra questi, emerge un 13% di utenti particolarmente attivi che effettuano consultazioni una o più volte al giorno, mentre circa un fruitore di servizi dispositivi su tre esegue almeno una disposizione a settimana.

Con riferimento a 18 banche/gruppi rispondenti, il numero totale di operazioni dispositive registrate da smartphone nel 2016 è stato pari a 21,8 milioni, con una crescita del 125% a campione costante. In generale, l'utilizzo di tutte le tipologie di operazioni è aumentato nell'ultimo anno; rileva notare, in dettaglio, il numero di bonifici disposti, che nel 2016 è aumentato del 61% rispetto all'anno precedente.

La crescita del numero di utenti che ricorrono al canale Mobile è andata di pari passo con il percorso di evoluzione del canale stesso, in termini di funzionalità e servizi. In questo contesto, le

[5] ABI Lab, Politecnico di Milano – Osservatorio Mobile Banking – 2017, 20 rispondenti

banche italiane da tempo garantiscono una presenza completa e differenziata sul canale, attraverso un'offerta in grado di soddisfare le diverse aspettative del cliente. Le caratteristiche innovative e la continua evoluzione delle tecnologie utilizzate sono alcuni degli elementi che hanno contribuito alla veloce crescita di tale canale.
Dal punto di vista dei sistemi operativi supportati dai dispositivi in possesso della clientela, le analisi condotte dall'Osservatorio Mobile Banking di ABI Lab evidenziano che tutte le banche intervistate offrono servizi tramite App per smartphone con sistema operativo iOS e Android, e il 70% del campione rende utilizzabile la propria App anche da device con sistema operativo Windows. Se si considerano invece i tablet, le banche che hanno sviluppato una App per iOS e Android sono pari all'88% del campione, mentre il 44% dei rispondenti anche per Windows.
Inoltre, un terzo delle banche intervistate ha già predisposto servizi anche per dispositivi wearable, focalizzandosi quasi esclusivamente su smartwatch.
Per quanto riguarda i servizi offerti, oltre alle classiche funzionalità banking, emerge che per il 75% del campione è elevata l'attenzione su servizi di trading, mentre il 60% offre servizi di pagamento peer-to-peer e assistenza ai clienti.
Le diverse funzionalità possono essere offerte in un'unica App oppure attraverso App ad hoc per un determinato servizio: gli esempi più evidenti in questo senso sono il borsellino elettronico (wallet) e il Mobile POS (pagamenti elettronici con carte di credito o debito collegando il dispositivo mobile al POS), quasi sempre gestiti con un'App aggiuntiva rispetto a quella "classica" di Mobile Banking; anche i servizi di trading per una banca su tre sono gestiti con applicazione specifica.
Nell'evoluzione dei servizi tramite device mobile, l'ambito del mobile payment risulta essere una delle principali priorità ICT 2017 in termini di investimento (70%) e di ricerca (70%) per il settore bancario italiano[6].

1.2. Mobile Banking e Sicurezza

A fronte del crescente utilizzo del canale mobile da parte degli utenti, cambia lo scenario delle minacce informatiche cui può essere esposta la clientela nell'utilizzo dei servizi bancari e si evolve inevitabilmente anche la valutazione dei rischi di sicurezza da parte delle banche, che devono poter fronteggiare e prevenire i nuovi possibili meccanismi di attacco.
In particolare, il ricorso ai dispositivi mobili per accedere ai servizi bancari attraverso le App e per ricevere i codici OTP (One Time Password) autorizzativi delle transazioni online rende tali strumenti degli obiettivi sensibili sotto il profilo della sicurezza, anche perché non tutta la superficie di attacco è sotto il controllo diretto della banca: basti pensare, ad esempio, ai processi e alle tecnologie in carico ai produttori di telefonia, ai TelCo Provider, oltre che alle vulnerabilità umane legate ai comportamenti dell'utente e allo stesso dispositivo mobile, con l'insieme di App in esso presenti. La facilità d'uso dei servizi mobile deve quindi andare di pari passo con una crescente responsabilizzazione da parte del cliente nei confronti del servizio e delle sue funzionalità, affinché la semplicità di adozione non si trasformi in atteggiamenti poco diligenti e attenti sotto il profilo della sicurezza. Particolare attenzione deve essere rivolta alla sfera delle App per il loro crescente utilizzo, anche nel contesto bancario, che le rende un target appetibile per i frodatori, in grado di sfruttare eventuali vulnerabilità presenti.

L'analisi[7] condotta sull'anno 2016 da ABI Lab nell'ambito delle attività dell'Osservatorio Cyber Knowledge and Security Awareness del CERT Finanziario Italiano (CERTFin), cui hanno partecipato 28 organizzazioni rappresentative dell'89% del settore in termini di dipendenti, ha evidenziato che il fenomeno delle frodi informatiche specifiche per il contesto del Mobile Banking

[6] ABI Lab – Rilevazione sulle priorità ICT delle banche italiane, marzo 2017, 27 rispondenti
[7] CERTFin - Osservatorio Cyber Knowledge and Security Awareness – 2017, 28 rispondenti

è ancora molto contenuto. Solo nel 2016 si sono registrati, per le banche intervistate, i primi casi di frode ai danni della clientela su tale canale: in dettaglio, rispetto al campione complessivo solo una realtà ha indicato di aver rilevato frodi effettive (dimensionate in 50 accadimenti) ai danni della propria clientela e adducibile a servizi specifici mobile. II meccanismo di attacco associato ha visto in primo luogo la sottrazione delle credenziali statiche di accesso ai servizi bancari attraverso tecniche più o meno tradizionali di *social engineering* (quali *phishing* e *SMiShing*, che puntano sulle vulnerabilità umane) e, successivamente, la realizzazione delle transazioni dopo aver preso il controllo del telefono tramite la tecnica del *SIM Swap*. Tale tecnica consiste nella capacità da parte dei frodatori di prendere possesso del telefono della vittima attraverso la richiesta al provider di telefonica di bloccare la SIM del cliente – spacciandosi per il cliente stesso e motivando la richiesta con una denuncia falsa di furto/smarrimento o presentando falsi documenti di identità – per poi riattivarne una nuova con lo stesso numero. In questo modo, in poco tempo i criminali hanno il controllo del numero di telefono del cliente con cui poter disporre transazioni. Tale modalità di attacco mette in evidenza l'importanza del rafforzamento della cooperazione tra i diversi attori coinvolti (banche, utenti, TelCo Provider), per minimizzarne l'impatto e l'efficacia.

Le analisi, inoltre, hanno mostrato che solo due tra le realtà rispondenti hanno indicato di aver rilevato App clone, per un totale di 386 unità, e che nessuna banca intervistata ha registrato nel 2016 casi di frode associati a specifici servizi di mobile payment.

A protezione del canale di Mobile Banking, e in linea con quanto già fatto per il canale Internet, le banche hanno introdotto strumenti in grado di monitorare eventuali anomalie rispetto a operazioni effettuate attraverso il canale mobile (62,5% dei rispondenti alla survey) e di semplice accesso alle App (50%) o di rilevare la presenza di *malware* nei dispositivi mobili dell'utente (29,2%). Inoltre, azioni informative sui rischi cyber e sulle buone pratiche di utilizzo dei servizi mobile vengono distribuite su tutti i canali a disposizione della banca, nell'83,3% dei casi sull'interfaccia di Internet Banking e nel 37,5% dei casi anche attraverso le notifiche via App.

I risultati positivi registrati lo scorso anno non devono determinare un abbassamento dei livelli di attenzione e di guardia da parte delle banche nei confronti dei possibili attacchi che possono insistere sui servizi e sul canale Mobile. È noto come i rischi cyber siano particolarmente complessi da fronteggiare, per la loro crescente sofisticazione, complessità e persistenza, oltre che per la notevole capacità, da parte dei cybercriminali, di poter sfruttare in tempi sempre più rapidi una vulnerabilità (sia essa tecnologica, di processo, o umana) a proprio vantaggio, prima che possano essere individuate o messe in atto le specifiche contromisure. È importante dunque affiancare all'innovazione lato business e all'offerta di nuovi servizi anche una continua e approfondita conoscenza, da parte del settore, delle vulnerabilità e delle minacce specifiche per il contesto bancario, in modo da poter prevenire e contrastare adeguatamente i rischi emergenti, già a partire delle fasi di sviluppo di nuovi servizi/funzionalità tramite App.

Il crescente livello di diffusione dei servizi mobile, unito all'incremento costante dei pagamenti effettuati da remoto, ha fatto sì che anche a livello istituzionale sia sempre più diffusa la consapevolezza della necessità di garantire, da un lato, un contesto competitivo nel quale possano entrare sempre nuovi attori, purché opportunamente regolamentati, e, dall'altro, un ambiente sicuro all'interno del quale permettere alla clientela di usufruire dei servizi bancari, senza porre freno all'innovazione. Nello scenario appena descritto, sono numerose le normative nazionali e comunitarie che sono state emanate negli ultimi anni a tal fine. Si riporta di seguito un elenco non esaustivo delle principali iniziative regolamentari che affrontano i temi di cybersecurity e che hanno impatto sul settore bancario, in termini di investimenti e interventi di adeguamento.
In primo luogo la nuova PSD (Payment Service Directive), pubblicata a inizio 2016 e la cui entrata in vigore è prevista per il prossimo gennaio 2018, che prevede specifiche misure e controlli di sicurezza cui tutti i PSP (Payment Service Providers) devono necessariamente adeguarsi.

L'attuazione di tali misure è regolata inoltre dagli RTS (Regulatory Technical Standards)[8] in via di finalizzazione da parte dell'EBA (European Banking Authority), che identificano specifiche misure attraverso cui adeguarsi alla Direttiva, riferite in particolare alle procedure di autenticazione forte della clientela per l'accesso ai servizi e alla disposizione di operazioni da remoto e la comunicazione sicura con le cosiddette Terze Parti, che offrono servizi dispositivi e informativi pur non detenendo i conti della clientela.

A questo si aggiungono le iniziative della Banca Centrale Europea, e in particolare il nuovo processo di segnalazione da parte degli istituti significativi dei gravi incidenti cyber, attivo dal 10 luglio 2017, nonché la Direttiva UE 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. Direttiva NIS – Network & Information Security), da recepire a livello nazionale entro il 10 maggio 2018. La Direttiva NIS prevede, tra l'altro, la creazione di una rete di collaborazione tra le Autorità competenti degli Stati membri e forme di cooperazione pubblico-privato per lo scambio di informazioni sui rischi emergenti e su eventuali incidenti, in attuazione delle misure indicate dalla strategia di cybersecurity europea. La Direttiva ha impatti anche sugli operatori bancari e finanziari, in quanto annoverati tra gli operatori di servizi essenziali che sono nel perimetro di applicazione della normativa.

[8] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

2. Metodologia di Analisi

Questa sezione presenta la metodologia adottata nel presente studio per l'analisi di sicurezza delle applicazioni per dispositivi mobili, partendo da una descrizione generale fino alla definizione del sottoinsieme di controlli utilizzati.

2.1 Analisi di Sicurezza delle Applicazioni Mobili

La metodologia OSSTMM[9] definisce un insieme di processi volti all'analisi di sicurezza di un sistema informatico. Tali processi, declinati nel mondo dei dispositivi mobili, permettono di delineare una rigorosa metodologia di verifica della sicurezza delle applicazioni. La metodologia di assessment, integrata con le linee guida di sicurezza definite dall'Open Web Application Security Project (OWASP), può essere riassunta nelle seguenti macro-attività:

- **Definizione della superficie di attacco**. La definizione della superficie di attacco permette di specificare il perimetro dell'analisi, identificando tutti i componenti dell'applicazione potenzialmente esposti ad attacchi. In questa fase vengono definite anche le modalità di accesso alle informazioni (analisi white-box, grey-box oppure black-box) ed eventuali strumenti automatici o semiautomatici coinvolti nel processo.

- **Individuazione delle tipologie di minaccia**. Questa fase prevede l'individuazione e l'analisi di scenari d'azione costruiti attraverso lo studio del repertorio di minacce conosciute verso le applicazioni e le piattaforme mobile oggetto di analisi.

- **Esecuzione dei controlli**. Per ogni minaccia identificata nella fase precedente vengono eseguiti una serie di controlli di sicurezza basati sulla "OWASP Mobile Application Security Verification Standard" (MASVS[10]). Il MASVS è un framework che permette di definire il livello di sicurezza delle applicazioni per dispositivi mobili. Esso definisce due *security verification levels* (L1 e L2) e un insieme di requisiti di resilienza al *reverse engineering* (MASVS-R). Soddisfare il livello L1 significa possedere una applicazione che segue le principali best practice di sicurezza in termini di qualità del codice, gestione dei dati sensibili e interazione con il sistema operativo. Il livello L1 è consigliato per tutte le applicazioni mobile a prescindere dalla loro destinazione. Il livello L2 integra i requisiti del livello L1 con meccanismi di sicurezza avanzati che vanno oltre i requisiti standard, come ad esempio l'SSL Pinning, e garantisce che l'applicazione sia protetta anche contro attacchi sofisticati. Questo tipo di livello di sicurezza è consigliato dal MASVS per tutte quelle applicazioni che gestiscono dati sensibili. Il livello R definisce invece una serie di controlli di sicurezza volti a verificare la robustezza dell'applicazione rispetto agli attacchi "client-side", diretti ad alterare e a studiare l'applicazione (*reverse engineering*, *tampering* e *modding*). L'integrazione di tale livello con i requisiti L2 (L2+R) viene raccomandata dal MASVS per tutte le applicazioni del mondo finanziario, incluse le applicazioni di online banking. Il MASVS definisce otto categorie, raffigurate in Figura 1, che coprono le diverse aree di verifica. Tali categorie vengono tradotte in un elenco tecnico di verifiche di sicurezza, volto a definire in maniera rigorosa a quale di livello di sicurezza appartiene l'applicazione mobile oggetto di analisi. L'elenco di tali controlli è codificato nel "OWASP Mobile Security Testing Guide" (MSTG).

[9] http://www.isecom.org/research/
[10] https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide

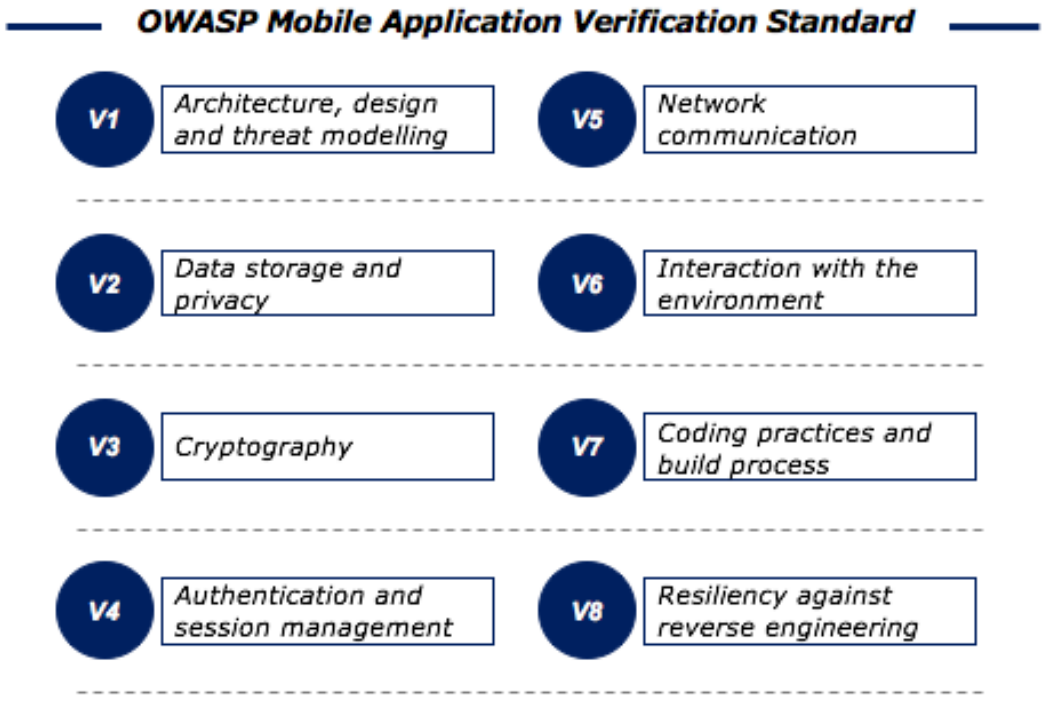

Figura 1: Elenco delle principali categorie di verifica delle minacce di sicurezza definite dallo OWASP MASVS

- **Identificazione delle vulnerabilità**. In base ai risultati della verifica dei controlli di sicurezza vengono identificate e analizzate le vulnerabilità che insistono sull'applicazione. Le vulnerabilità identificate vengono classificate secondo le categorie dell'OWASP Top 10 Mobile Risks 2016[11] (Figura 2) redatte dal consorzio OWASP, che racchiude i principali vettori di rischio per le applicazioni mobile, e valutate in ottica di esposizione al rischio, calcolando il potenziale impatto e la probabilità di accadimento secondo la "OWASP Risk Rating Methodology"[12].

[11] https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
[12] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

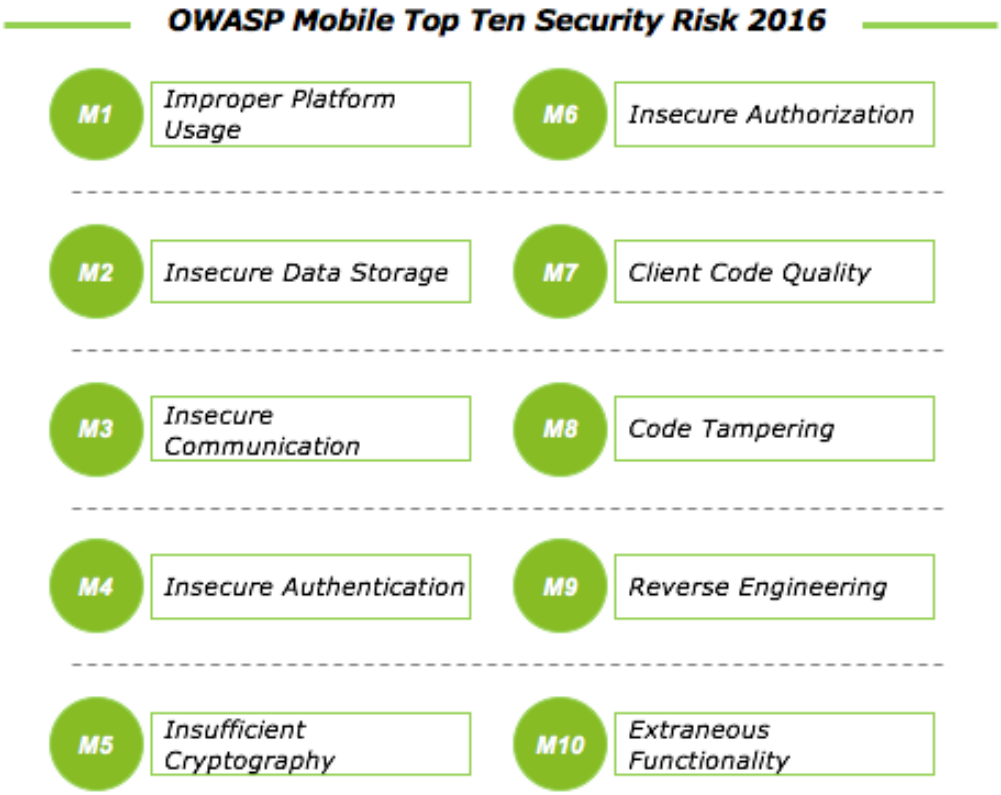

Figura 2: Classifica OWASP delle principali categorie di rischi di sicurezza per dispositivi mobile

2.2 Definizione della metodologia per il report

2.2.1. Descrizione del Campione scelto

Per il presente report è stato individuato un campione di applicazioni di Mobile Banking per la clientela retail e sviluppate per Android, sistema operativo mobile tra i più utilizzati (64,47% di market share mondiale[13]); in particolare sono state selezionate le prime quindici applicazioni di istituti bancari italiani ordinati secondo il parametro legato alla solidità finanziaria (CET1)[14].
Le applicazioni di Mobile Banking così selezionate sono state reperite mediante l'ultima versione disponibile sul Google Play Store a maggio del 2017.
La seconda fase di analisi ha visto l'estensione del campione analizzato anche a quindici istituti bancari tedeschi e quindici istituti bancari britannici (selezionati secondo la solidità finanziaria CET1), con l'obiettivo di confrontare le misure di sicurezza messe in campo da tali applicazioni.
Le 45 applicazioni così selezionate coinvolgono un vasto numero di clienti, vantando (nel loro complesso) più di 20 milioni di download distinti[15].

[13] NetMarketShare – Mobile/Tablet Operating System Market Share
[14] Elaborazione Università Bocconi da dati pubblici per Corriere Economia, III trimestre 2015
http://www.corriere.it/economia/16_gennaio_25/piu-solide-convenienti-classifica-istituti-italiani-040c424c-c348-11e5-b326-365a9a1e3b10.shtml
[15] Google Play Store, Maggio 2017

2.2.2. Descrizione delle modalità di analisi

Le analisi, realizzate dal laboratorio CSEC Lab e dalla società Talos, sono state effettuate in modalità black-box, ovvero senza alcuna informazione specifica sull'applicazione (ad esempio eventuale documentazione tecnica), salvo quelle reperibili pubblicamente dal Google Play Store. Poiché i controlli definiti dalla MSTG sono "*app-centric*" e indipendenti dall'ambiente di esecuzione, la superficie di attacco considerata nel presente studio è limitata all'applicazione e alle sue interazioni con il sistema operativo e con i servizi di backend; vengono esclusi problemi di sicurezza specifici del sistema operativo (Android) o del canale di comunicazione (Internet), che potrebbero compromettere la sicurezza generale del sistema e quindi anche delle applicazioni stesse.
Le analisi sono stata effettuate in due fasi: la prima fase è stata condotta con l'ausilio di strumenti automatici (Approver, Androguard, Dex2Jar, JD-Gui, Charles Proxy) che hanno consentito una preliminare rilevazione delle potenziali aree di attacco, mentre la seconda ha previsto verifiche e approfondimenti condotti manualmente sulle singole vulnerabilità identificate, al fine di validare i risultati ottenuti. Le attività di verifica manuale sono state limitate alla sola superficie pubblica delle applicazioni di Mobile Banking, senza quindi poter accedere alle aree riservate alla clientela dotata di credenziali di accesso.

2.2.3. Focus Classi di Minaccia e Controlli

Il presente report si focalizza su una serie di controlli estratti dall'OWASP MSTG descritti nei precedenti paragrafi, volti a valutare il livello di protezione e confidenzialità del canale di comunicazione tra l'applicazione di Mobile Banking e i servizi di backend, nonché la possibilità da parte dell'applicazione di verificare lo stato di integrità del dispositivo in cui è in esecuzione. I controlli considerati, descritti nel dettaglio nel prosieguo di questo capitolo, sono accomunati da un impatto tecnico molto elevato nonché da una particolare facilità di sfruttamento da parte degli attaccanti.

2.2.3.1. Controllo di Root Detection

Il controllo di Root Detection viene definito all'interno della OWASP MSTG 6.10 come la capacità da parte dell'applicazione mobile di identificare se l'ambiente in cui è in esecuzione è stato modificato per avere privilegi di root ("rooted"). In funzione poi dei requisiti di business l'applicazione può decidere di avvisare l'utente, chiedendo il suo esplicito consenso a continuare l'esecuzione, oppure auto-terminarsi.
La mancanza del controllo sui permessi di root è classificata nelle categorie M9-*Reverse Engineering*[16] e M8-*Code Tampering*[17] dell'OWASP top 10 risks, ed è associata ad un impatto tecnico giudicato tra il moderato e il severo ed una possibilità di sfruttamento classificata come facile.

Implicazioni per la Sicurezza

Di default, su Android, solo il kernel Linux e un ristretto sottoinsieme di servizi core possono funzionare con i privilegi di root. Le applicazioni invece, ciascuna associata a un utente distinto e senza privilegi specifici, vengono eseguite in "ambiente utente" e non esiste la possibilità di fare "*Priviledge Escalation*".

[16] OWASP M9 - Reverse Engineering https://www.owasp.org/index.php/Mobile_Top_10_2016-M9-Reverse_Engineering
[17] OWASP M8 - Code Tampering https://www.owasp.org/index.php/Mobile_Top_10_2016-M8-Code_Tampering

Un utente (e quindi una applicazione) con i permessi di root potrebbe modificare il sistema operativo, il kernel o qualsiasi altra applicazione. In generale, l'utente root ha il completo accesso a tutte le applicazioni e a tutti i dati delle applicazioni presenti sul dispositivo.

In particolare, l'utente root può:

- avere accesso completo al file system (cartelle private delle applicazioni, impostazioni del dispositivo, database, keystore, shared preferences, etc);
- eseguire qualsiasi operazione security relevant senza aver bisogno di alcun permesso;
- accedere direttamente al sistema operativo e al kernel sottostante;
- installare in maniera silente altre applicazioni all'interno del dispositivo;
- avere un controllo completo di tutte le interfacce di rete (es Wi-fi, Bluetooth, NFC).

Avere dunque un dispositivo con i permessi di root significa essere in grado di aggirare i principali meccanismi di sicurezza del Sistema Operativo Android, come ad esempio l'*Application Sandbox*[18] e il *Permission Enforcement*[19].

Le applicazioni installate su un dispositivo Android rooted sono esposte ad una serie di rischi dal punto di vista della sicurezza molto più ampia rispetto alle normali condizioni di un sistema operativo stock. Di seguito vengono elencati i principali punti di attenzione.

Utilizzo del File System. Un attaccante può creare un'applicazione malevola per accedere direttamente alla cartella privata di una applicazione bersaglio rubando tutti i file di configurazione, i database e le chiavi memorizzate nell'Android Keystore.

Utilizzo delle interfacce di Rete. Un utente con permessi di root può accedere, ad esempio, alle impostazioni di rete del dispositivo, nonché intercettare il traffico (Wi-Fi, Bluetooth, NFC, Rete Mobile) che vi passa attraverso.

Utilizzo delle interfacce di I/O. Le applicazioni per dispositivi mobili utilizzano tipicamente una serie di input, sia dall'utente (tramite l'inserimento di informazioni con tastiera), sia tramite sensori presenti nel dispositivo (giroscopio, GPS, fotocamera, sensore di impronta digitale). In condizioni di dispositivo stock le periferiche di I/O sono sotto il controllo del sistema operativo, ma dal momento che l'utente di root è in grado di superare le restrizioni di sicurezza imposte dal sistema operativo, non è possibile considerare affidabili tali interfacce.

2.2.3.2. Protezione del Canale (SSL Pinning)

Il controllo sulla protezione del canale che viene definito all'interno della OWASP MSTG 5.4 è volto a verificare se l'applicazione utilizzi un proprio certificate store o se includa al suo interno il certificato o la chiave pubblica dell'endpoint (SSL Pinning); in questo modo si impedisce che vengano stabilite connessioni TLS con endpoint che offrono un certificato diverso, anche se firmato da una Trusted Certificate Authority.
L'insufficiente protezione del canale di comunicazione viene classificata nei rischi legati alla comunicazione insicura (M3-*Insecure Communication*[20] dell'OWASP top 10 risks) ed è associata ad un impatto tecnico severo ed una possibilità di sfruttamento classificata come facile.

[18] Meccanismo di sicurezza che associa ad ogni applicazione installata sul dispositivo un diverso Linux User ID, una area di memoria e un processo di esecuzione dedicato. Questo meccanismo è volto a incrementare il livello di isolamento tra le applicazioni, le cui comunicazioni sono regolate dal sistema operativo.
[19] Meccanismo di sicurezza che permette di associare a certi servizi e dati, un token di accesso, chiamato permesso, che deve essere esplicitamente accordato alle applicazioni per poter garantire l'utilizzo di tali risorse.
[20] OWASP M3-Insecure Communication https://www.owasp.org/index.php/Mobile_Top_10_2016-M3-Insecure_Communication

Implicazioni per la Sicurezza

La prima fase delle comunicazioni TLS tra un'applicazione e il backend prevede la costituzione di un canale sicuro (HTTPS) attraverso cui comunicare. Tale fase prevede un'attività di scambio e verifica reciproca dei certificati, al termine del quale viene instaurata la comunicazione.
Tuttavia, tale verifica può essere bypassata, esponendo un certificato SSL valido in grado di soddisfare la procedura di verifica SSL. Questo può essere ottenuto installando un nuovo certificato all'interno di quelli attendibili presenti nel sistema operativo. L'installazione può essere fatta inducendo l'utente stesso a effettuarla (es. certificato per accedere in maniera gratuita ad un hotspot Wi-Fi) oppure, nel caso di sistemi con permessi di root, senza alcuna necessità di interazione.
Questa debolezza può essere sfruttata per eseguire, ad esempio, un attacco di tipo *Man In the Middle* tra l'applicazione e il backend tramite l'utilizzo di un web proxy oppure tramite la connessione del dispositivo ad un access point Wi-Fi malevolo.
Un attaccante infatti può ridirigere le comunicazioni dell'applicazione ad un server proxy esterno che può leggere e modificare tutte le comunicazioni da/per l'applicazione (a meno che non siano ulteriormente cifrate a livello applicativo), incluse le richieste di autenticazione e le transazioni finanziarie.
La procedura di SSL Pinning permette di prevenire questo rischio di sicurezza, manlevando l'applicazione dal doversi affidare ai certificati presenti sul dispositivo e includendo al suo interno il certificato atteso del backend. Ogni volta che l'App intende stabilire una comunicazione sicura con un'entità esterna andrà a verificare non solo che tale certificato sia valido ma anche che sia effettivamente quello atteso.

2.2.3.3. Confidenzialità del Canale

Il controllo sulla confidenzialità del canale, definito all'interno della OWASP MSTG 5.1, è volto a verificare se l'applicazione utilizzi per le comunicazioni una connessione cifrata in maniera consistente attraverso tutta l'applicazione.
Una confidenzialità assente o parziale del canale di comunicazione viene classificata nella categoria dei rischi di comunicazione (M3-*Insecure Communication*) ed è associata ad un impatto tecnico severo e ad una possibilità di sfruttamento classificata come facile.

Implicazioni per la Sicurezza

Le comunicazioni che avvengono tra l'applicazione e il backend possono avvenire in contesti in cui non si ha la certezza che il canale sia fidato, come ad esempio attraverso connessioni a hotspot Wi-Fi gratuiti e non protetti (circa il 24.7% della totalità secondo Kaspersky[21]) o comunque non adeguatamente protetti. Un canale non fidato implica la possibilità che un attaccante possa intercettare e/o modificare il traffico che passa attraverso tali connessioni, con un rischio sostanziale per la sicurezza sia dell'utente che dei servizi di backend.
Usare comunicazioni non protette da meccanismi TLS comporterebbe quindi la possibilità, ad esempio, da parte di un malintenzionato di intercettare i dati sensibili del cliente o modificare i contenuti dei dati trasmessi.
Questo tipo di scenario di attacco ha recentemente raggiunto livelli di attenzione, tanto che il GCHQ National Cybersecurity Centre ha segnalato nei suoi threat report[22] come gruppi di hacker organizzati stiano prendendo di mira gli hotspot Wi-Fi delle strutture ricettive europee per diffondere *malware* sui dispositivi ad esso connessi.

[21] https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/
[22] https://www.ncsc.gov.uk/report/weekly-threat-report-18th-august-2017

3. Risultati dell'Analisi

I risultati delle analisi svolte sui campioni di applicazioni di Mobile Banking mostrano diversi punti di attenzione. Da una valutazione generale, approfondita nel prosieguo di questo capitolo, si evince come numerose tra le applicazioni analizzate presentino alcuni livelli di vulnerabilità relativamente ai controlli individuati dal presente report.

3.1 Controllo di Root Detection

Il controllo di Root Detection del dispositivo mobile è volto a verificare se l'applicazione di home banking sia in possesso di meccanismi in grado di valutare se l'ambiente di esecuzione disponga o meno dei privilegi di root.
Secondo la definizione data nell'OWASP MSTG, tale controllo deve essere effettuato ad ogni avvio dell'applicazione e, qualora venisse rilevato un sistema non integro, fornire un avviso all'utente o, a seconda dei requisiti di business, inibire il funzionamento (totale o parziale) dell'applicazione stessa.
In relazione al campione italiano, la Figura 3 evidenzia come l'86,7% delle applicazioni mobile non implementi efficacemente tale controllo, rispetto ad un 13,3% in cui tale controllo viene effettuato. Raffrontando il dato con i campioni estratti dal mondo anglosassone e quello tedesco (Figura 4), è possibile notare come la situazione differisca in maniera minima rispetto al campione tedesco (66,7%) e nulla rispetto a quello anglosassone.

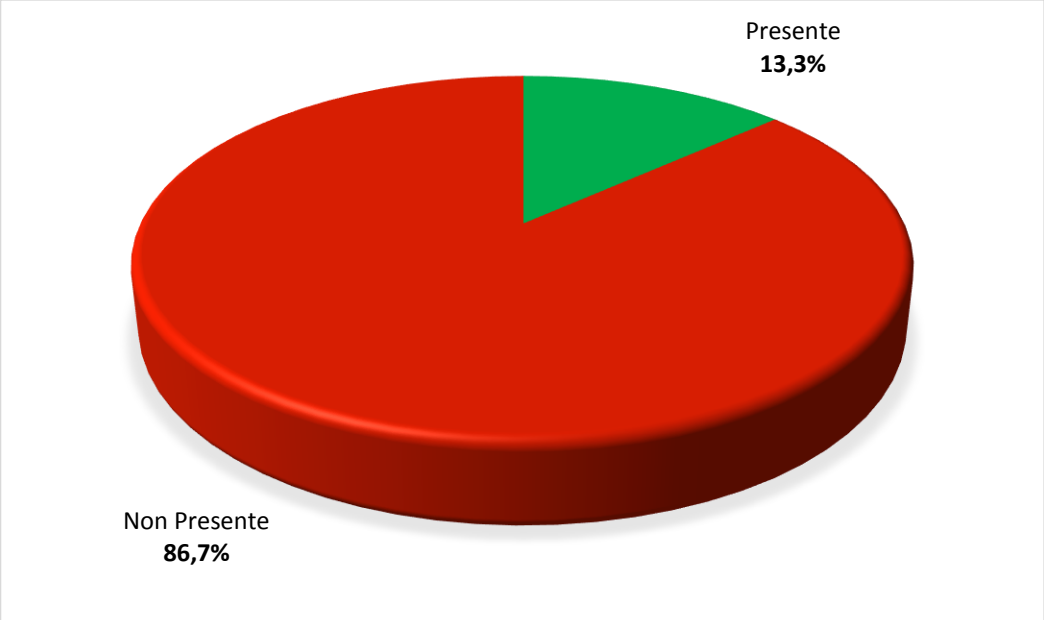

Figura 3: Presenza di controlli di integrità del dispositivo nelle App di Mobile Banking (Italia)

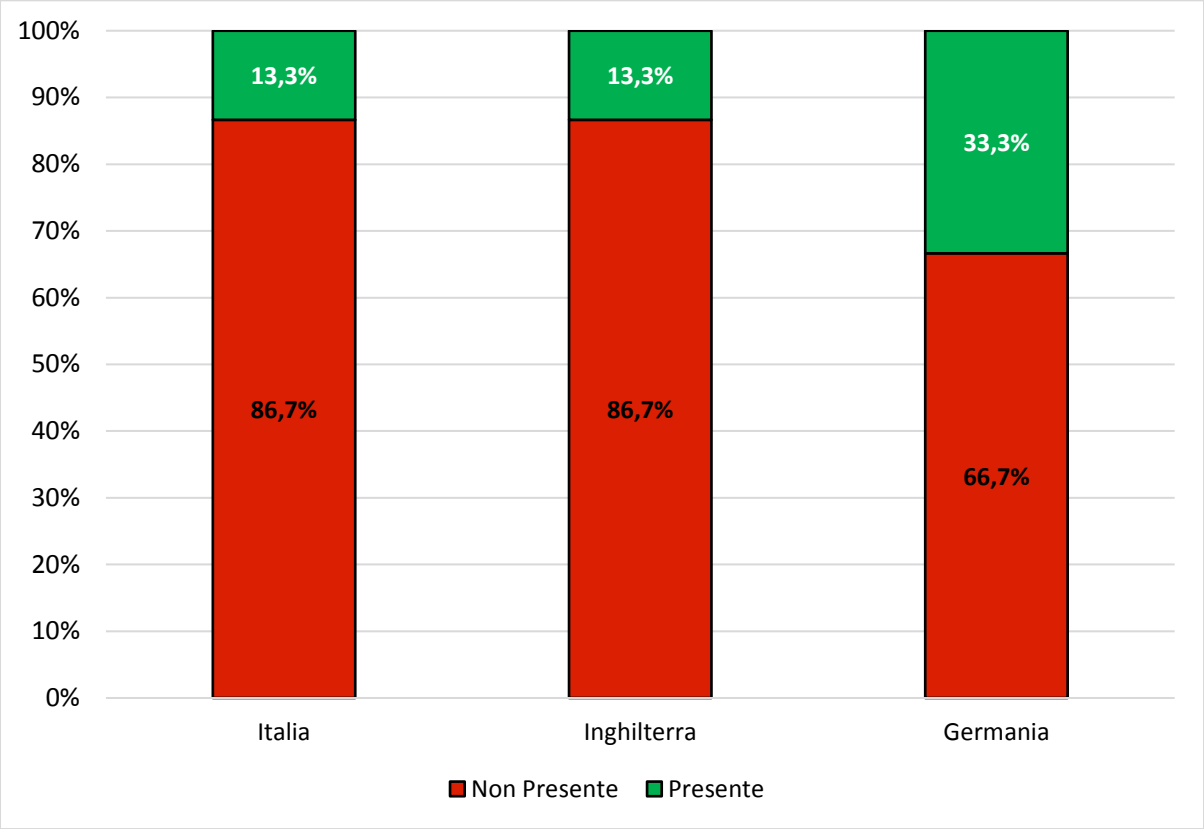

Figura 4: Presenza di controlli di integrità del dispositivo nelle App di Mobile Banking - comparazione tra Italia, Inghilterra e Germania

L'uniformità dei risultati elaborati sul campione di App di Mobile Banking nei tre Paesi suggerisce come la scelta di non ricorrere a questo tipo di controlli possa essere legata a vincoli operativi e procedurali da parte delle banche (come ad esempio l'adozione di diverse linee guida o policy aziendali), o all'esigenza di non voler modificare la customer experience nell'utilizzo dell'applicazione bancaria.
Al contempo, è importante notare come questa scelta possa rappresentare un fattore di rischio, dato che non è possibile fare assunzioni sul livello di sicurezza di un dispositivo non integro, che non è sotto il diretto controllo della banca; pertanto, occorre valutare con attenzione le tipologie di dati che vengono salvati in locale, proteggere la comunicazione di rete secondo i più moderni standard di crittografia, appoggiarsi a tecniche di validazione dell'interlocutore nonché prevedere procedure ad hoc per mitigare il rischio di alterazione/intercettazione delle informazioni date in input all'applicazione. Il controllo sull'integrità del dispositivo può inoltre essere un'utile informazione per tutti i sistemi di monitoraggio e fraud-detection, che andranno a valutare in maniera più approfondita tutte quelle transazioni che vengono effettuate da dispositivi non integri.
È importante rimarcare come la scelta di introdurre specifiche misure di sicurezza risponda alla necessità di bilanciare diverse esigenze e requisiti (compliance, sicurezza, tecniche di business) ed è funzione, oltre che delle indicazioni riportate da normative, standard e best practice, anche del livello di esposizione al rischio cyber, valutato periodicamente in merito allo specifico servizio offerto.

3.2 Controllo di Protezione del Canale

Il controllo sulla protezione del canale prevede la verifica dell'utilizzo da parte dell'applicazione di tecniche di SSL Pinning.

Le analisi svolte sul campione italiano analizzato (Figura 5) evidenziano come l'86,7% delle applicazioni di Mobile Banking non implementi tali tecniche, facendo emergere alcune vulnerabilità rispetto alla possibilità per un attaccante di esporre un certificato valido ma diverso da quello atteso ed effettuare, ad esempio, un attacco di tipo *Man in the Middle*.
Questo dato, confrontato con il mondo anglosassone e quello tedesco (Figura 6) mostra una grossa disparità: le applicazioni che non effettuano adeguati controlli di protezione del canale sono infatti solo il 26,7% nel mondo inglese, fino a salire al 53,3% nel mondo tedesco, discostato comunque dal panorama italiano di più di 30 punti percentuali.
Come ricordato nei precedenti capitoli, un'adeguata protezione del canale, unita ad un'identificazione dell'interlocutore mediante SSL Pinning, consente di ridurre considerevolmente il rischio di essere intercettati da parte di un potenziale attaccante.
Il grado di protezione può essere incrementato introducendo, come consigliabile, un layer di cifratura applicativa (il contenuto della trasmissione) in aggiunta alla protezione fornita dal protocollo TLS/SSL. Questa misura, pur non essendo risolutiva di per sé, consentirebbe di ridurre il rischio che i messaggi, anche qualora intercettati, vengano decifrati da un attaccante. Anche in questo caso è importante rimarcare che il livello di gravità degli impatti derivanti dallo sfruttamento della vulnerabilità in oggetto varia in base alle condizioni in cui l'utente si trova a operare (integrità del dispositivo, protezione delle connessioni, etc.)

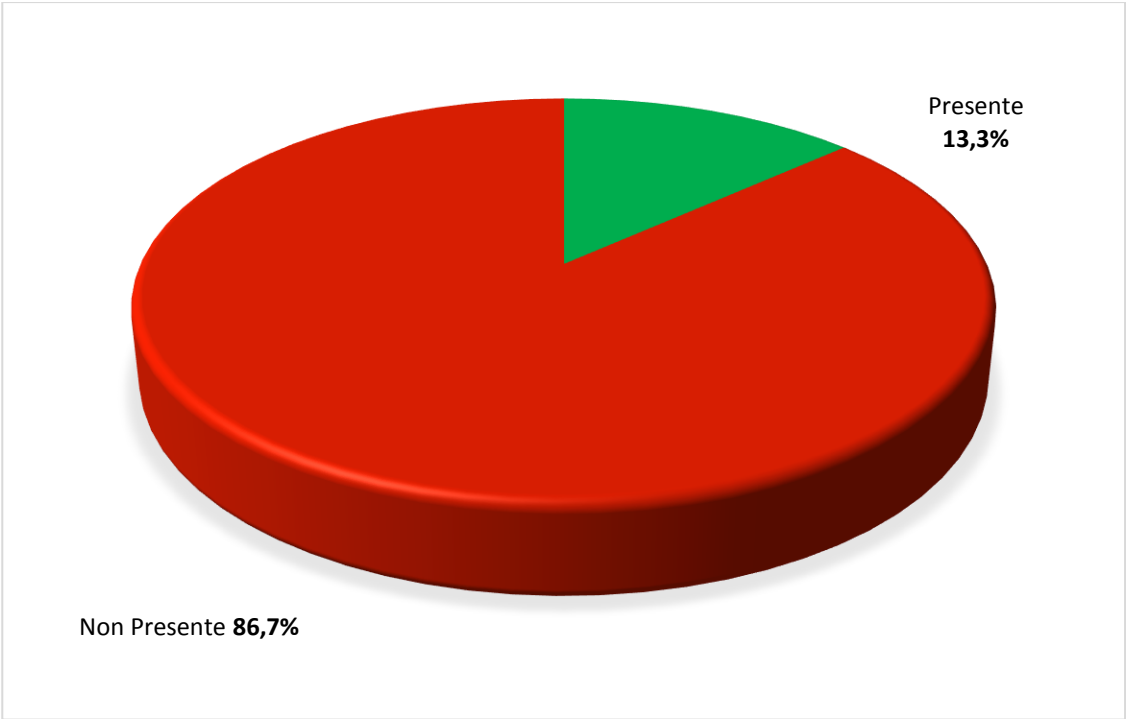

Figura 5: Protezione del canale - Presenza di SSL Pinning nelle App di Mobile Banking (Italia)

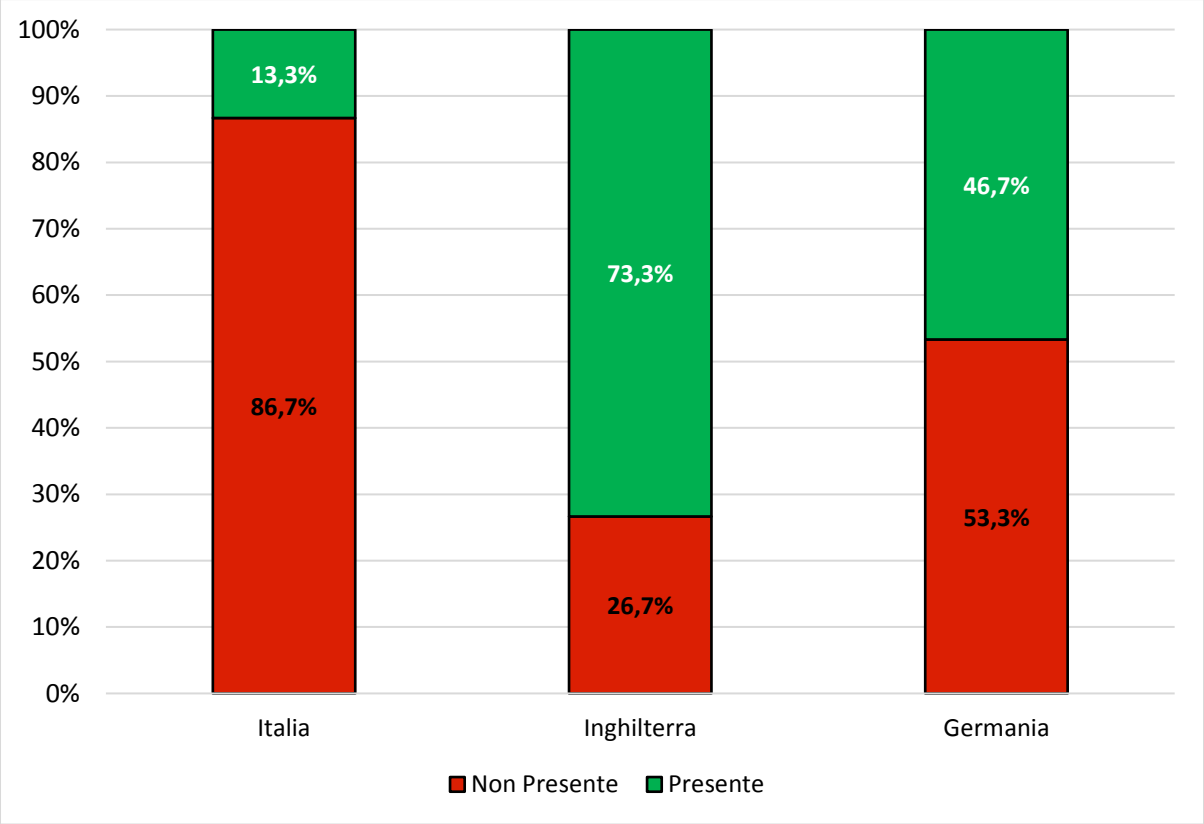

Figura 6: Protezione del canale - Presenza di SSL Pinning nelle App di Mobile Banking - comparazione tra Italia, Inghilterra e Germania

3.3 Controllo di Confidenzialità del Canale

Il controllo di confidenzialità del canale prevede la verifica dell'utilizzo da parte dell'applicazione di connessioni adeguatamente cifrate, per evitare che gli attaccanti possano alterare o intercettare il flusso di comunicazione.
Il campione italiano analizzato (Figura 7) mostra che il 60% delle applicazioni di Mobile Banking non adotta una modalità di cifratura estesa a tutte le comunicazioni.
La situazione del campione inglese e tedesco (Figura 8), pur essendo migliore, non si discosta molto da tale risultato (53,3% per l'Inghilterra e 46,7% per la Germania) e ciò rappresenta dunque un importante punto di attenzione sotto il profilo della sicurezza.
È bene notare come durante l'attività di analisi non ci si sia focalizzati esclusivamente sulla comunicazione tra l'applicazione e il backend finanziario, bensì su tutte le comunicazioni effettuate dall'applicazione bancaria tramite le sue funzionalità accessorie (ad esempio la mappa delle filiali tramite Google Maps). Tali comunicazioni, pur non avendo lo stesso livello di criticità di quelle dirette al backend, rappresentano comunque un fattore di rischio rilevante dato che costituiscono un punto di accesso diretto all'applicazione e che consentirebbero all'attaccante di intercettare e modificare il traffico da e per l'applicazione, con conseguenze non trascurabili per la sicurezza dell'intero servizio.

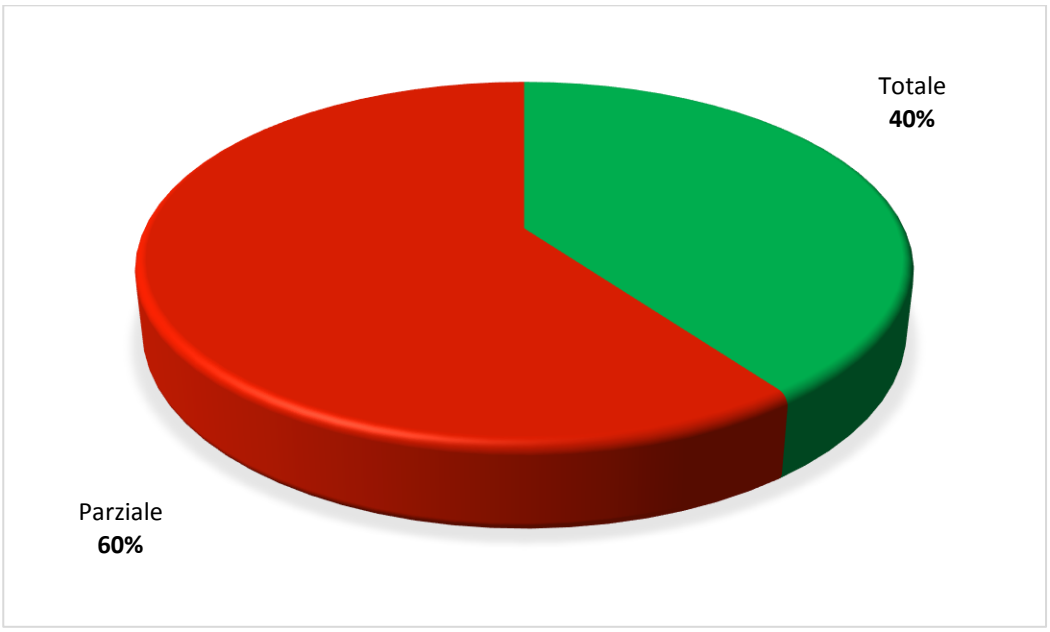

Figura 7: Confidenzialità del canale - Livelli di cifratura delle comunicazioni di rete nelle App di Mobile Banking (Italia)

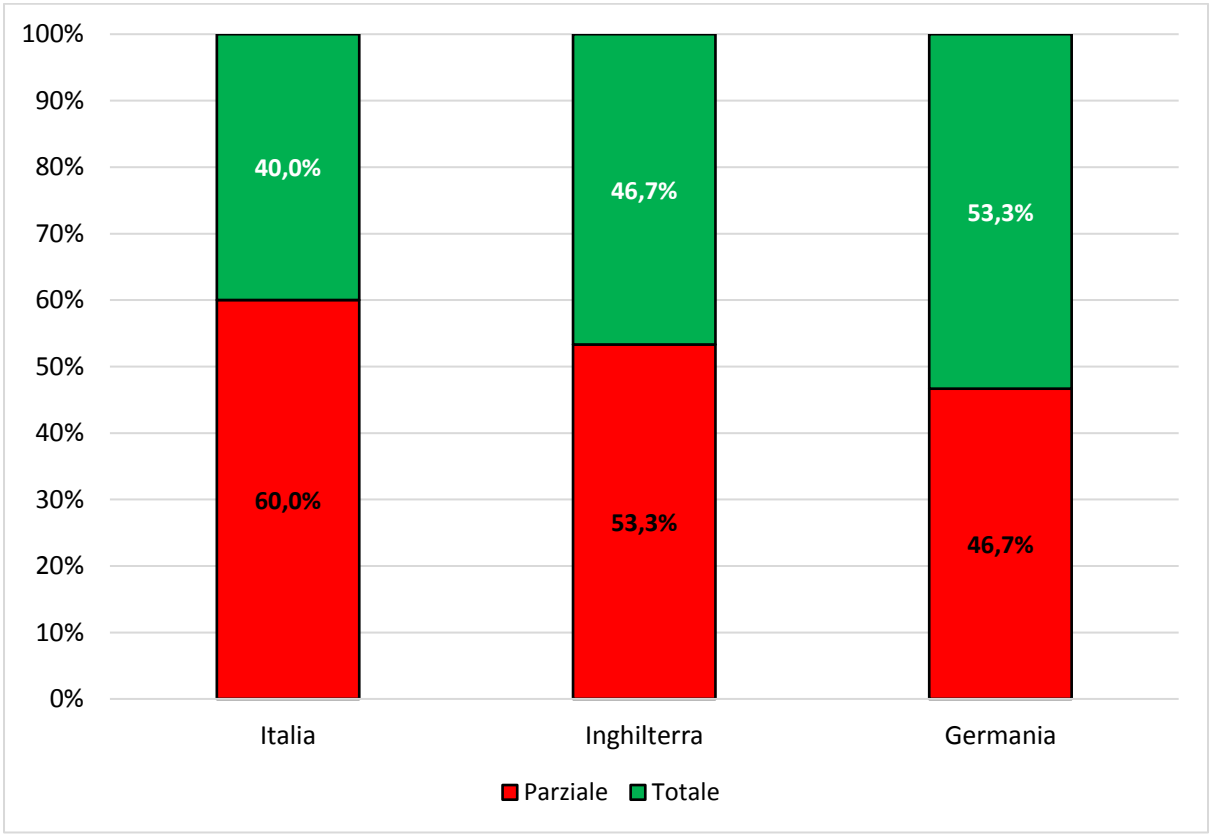

Figura 8: Confidenzialità del canale - Livelli di cifratura delle comunicazioni di rete nelle App di Mobile Banking - comparazione tra Italia, Inghilterra e Germania

4. Conclusioni e prossimi passi

Lo studio condotto ha rappresentato una prima occasione per applicare una metodologia di analisi delle App basata sul framework OWASP al mondo delle App per il Mobile Banking.

In sintesi, dall'analisi emerge come, rispetto ai controlli presi in esame, le applicazioni di Mobile Banking analizzate - con riferimento alle porzioni di accesso non protette da credenziali personalizzate - presentino vulnerabilità che potrebbero esporre maggiormente le App a minacce di severità anche elevata.

Se, come evidenziato nel Capitolo 1, i processi e i controlli antifrode hanno consentito sinora di contrastare efficacemente i fenomeni fraudolenti, i risultati del presente studio suggeriscono, in relazione alle tipologie di vulnerabilità e di controlli presi in esame nel presente studio, di mantenere sempre elevati i livelli di sicurezza delle applicazioni di Mobile Banking, attraverso processi di *vulnerability assessment* e *penetration testing,* secondo le migliori pratiche e in coerenza con le misure già in essere oltre che con le attività di risk assessment adottate. Particolare attenzione potrà essere rivolta anche alla fase di sviluppo delle App, tenendo conto delle diverse e possibili superfici di attacco cyber, in modo da ridurre i relativi livelli di rischio.

È importante notare come l'impostazione adottata abbia consentito di effettuare controlli dettagliati sotto il profilo tecnico, che potranno essere estesi in una seconda fase dello studio ad altre tipologie definite dall'MSTG. La selezione dei controlli da prendere in esame potrà essere effettuata con il supporto dei referenti delle banche che partecipano ai tavoli di lavoro del CERTFin.

Inoltre, alla luce della normativa di attuazione della PSD2 in materia di sicurezza dei pagamenti, in corso di finalizzazione da parte di EBA e citata nel Capitolo 1 del presente report[23], potrà essere sviluppato un ulteriore filone di analisi per comprendere come la metodologia adottata possa eventualmente supportare le banche nel valutare la conformità ai requisiti definiti dal regolatore. Ci si riferisce, in particolare, alla capacità di garantire che i dati del pagamento impostato e autorizzato dall'utente, anche tramite l'area riservata della App, arrivino integri e senza alterazioni al backend della banca per poter essere processati.

Infine, sulla base delle esigenze definite dalle singole banche, potranno essere condotte:

- Analisi più estese sulle App già monitorate nel presente studio, prendendo in considerazione eventuali versioni aggiornate e/o eseguendo i controlli anche sull'area riservata al cliente, accessibile con le credenziali di sicurezza personalizzate fornite dalla banca
- Analisi su altre App non considerate in questa prima fase dello studio

[23] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

About Us

CERTFin

Il CERTFin – CERT Finanziario Italiano – è un'iniziativa cooperativa pubblico-privata finalizzata a innalzare la capacità di gestione dei rischi cyber degli operatori bancari e finanziari e la cyber resilience del sistema finanziario italiano attraverso il supporto operativo e strategico alle attività di prevenzione, preparazione e risposta agli attacchi informatici e agli incidenti di sicurezza.
Il CERTFin è governato dall'Associazione Bancaria Italiana (ABI) e dalla Banca d'Italia, che ne condividono la Presidenza, ed è operato dal Consorzio ABI Lab. I servizi sono messi a disposizione dei partecipanti su base cooperativa, grazie al coinvolgimento degli operatori finanziari italiani.

Per info: http://www.certfin.it

CSEC Lab

Il Laboratorio di Computer Security (CSEC Lab) è il laboratorio di ricerca dedicato ai temi della Cybersecurity del Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS) dell'Università degli Studi di Genova. Il CSEC Lab, fondato da Alessandro Armando, Gabriele Costa e Alessio Merlo nel 2014, è attualmente diretto dal Prof. Alessandro Armando. Le principali attività di ricerca del CSEC Lab includono l'analisi della sicurezza delle applicazioni mobili, lo studio delle tecniche di penetration testing e la verifica dei protocolli di sicurezza.

Maggiori informazioni sono disponibili sul sito web http://csec.it/

Talos

Talos srls è una startup innovativa, nata a inizio 2016, che opera nel campo della cybersecurity e che è stata riconosciuta Spin Off dell'Università degli Studi di Genova.
L'attività principale di Talos è fornire soluzioni ad alto contenuto tecnologico per problemi di sicurezza relativi agli ambienti mobili per ambito business e consumer, tramite strumenti automatizzati per la valutazione dei rischi di sicurezza delle mobile App e tramite servizi di consulenza di sicurezza specializzati.
Talos vanta collaborazioni con importanti realtà aziendali e organizzazioni internazionali.

Maggiori informazioni sono disponibili sul sito web: https://www.talos-sec.com