Mobile Forensics: le nuove funzionalità di sicurezza integrate di Android e iOS rendono più difficoltoso l’accesso alla polizia giudiziaria

Date : 14 marzo 2018

Forse non tutti conoscono il significato di Mobile Forensics anche se sicuramente ne hanno sentito parlare.

La Mobile Forensics è la branca della Digital Forensics che si occupa di regolamentare le fasi di acquisizione, preservazione, analisi e reporting delle *evidenze digitali* contenute in un dispositivo mobile, quali telefoni, navigatori, tablet.

Per *evidenza digitale* viene intesa qualsiasi informazione avente valore probatorio che sia memorizzata o che sia stata trasmessa in forma digitale.

Attualmente la Mobile Forensics rappresenta un ausilio determinante nelle indagini investigative - specie in ambito penale - dato il sempre maggior rilievo probatorio assunto dalle evidenze digitali contenute all’interno dei dispositivi mobili.

I rapidi cambiamenti nella tecnologia dei dispositivi mobili forniscono grandi opportunità per attività criminali. I crimini commessi comprendono frodi, traffico di droga, terrorismo e pedopornografia solo per citarne alcuni. La rapida proliferazione dei dispositivi mobili sul mercato ha causato una richiesta enorme di acquisizione e analisi forense dei dispositivi, che non è stato possibile soddisfare con le tecniche forensi esistenti. Non vi sono modelli e tecnologie certificate per l’estrazione dei dati, a causa, tra le altre, della mancanza di standardizzazione degli stessi dispositivi.

Ma nonostante il successo che sembrerebbe derivarne pare che, l’epoca d’oro della Mobile Forensics, stia terminando.

Le ultime versione di iOS e Android rendono sempre più difficoltoso l’accesso ai dispositivi mobili anche alla polizia giudiziaria. Celato dall’attenzione per la privacy degli utenti, i maggiori produttori di dispositivi mobili stanno curando senza sosta la riservatezza dei dati e la loro protezione con tecniche sempre più raffinate. Google si è proposto per Android l’obiettivo di “piattaforma più sicura del mondo”.

Infatti, la nuova versione del sistema operativo Android, la versione 7 (Nougat)[1], dispone di tantissime novità in materia di sicurezza:

- procedure automatiche per l'installazione, in background, degli aggiornamenti di sicurezza;
- uno stack riprogettato per garantire una protezione avanzata contro gli attacchi più comuni e, nel contempo, meno sensibile ai contenuti di formato non valido;
- una crittografia basata su file;
- l'avvio diretto sicuro (Direct Boot) che consente, al dispositivo acceso ma non sbloccato, di ricevere telefonate, visualizzare le notifiche e accedere alle funzioni di accessibilità, mantenendo criptati i dati memorizzati.

Il sistema fornisce quindi due posizioni di archiviazione per i dati:

- Memoria crittografata delle credenziali, che è il percorso di archiviazione predefinito e disponibile solo dopo che l'utente ha sbloccato il dispositivo;
- Dispositivo di archiviazione crittografata, che è una posizione di archiviazione disponibile sia in modalità avvio diretto che dopo che l'utente ha sbloccato il dispositivo.

Android ha quindi funzionalità di sicurezza integrate che riducono significativamente la frequenza e l'impatto dei problemi di sicurezza delle applicazioni, rendendo sempre più difficoltosa l'analisi forense dei dispositivi equipaggiati con detta versione.

Il sistema è progettato in modo da poter creare in genere le App con le autorizzazioni predefinite per file e sistema ed evitare decisioni difficili in merito alla sicurezza.

Le funzionalità di sicurezza principali aiutano a creare App sicure:

- l'applicazione sandbox di Android, isola i dati dell'App e l'esecuzione del codice da altre App;
- un framework applicativo con robuste implementazioni di funzionalità di sicurezza comuni come crittografia, permessi e IPC[2] sicuro;
- tecnologie come ASLR[3], NX[4], ProPolice[5], safe_iop, OpenBSD dlmalloc, OpenBSD calloc e Linux mmap_min addr per ridurre i rischi associati agli errori di gestione della memoria più comuni;
- file system crittografato che può essere abilitato per proteggere i dati su dispositivi smarriti o rubati;
- autorizzazioni per limitare l'accesso alle funzionalità del sistema e ai dati dell'utente.

Quanto descritto è solo una parte delle misure di sicurezza implementate ed implementabili con Android. Sembra superfluo ricordare che, sin dalla versione 6, **Android cifra i dati utente tramite la sua password** e una seconda memorizzata all'interno del dispositivo. In mancanza di ambedue le credenziali, è **impossibile** accedere alla memoria del cellulare e, qualora ci si riuscisse, si verrebbe in possesso di informazioni impossibili da leggere.

Risulta di lampante evidenza l'importanza rivestita dal PIN o dalla password per l'accesso al

contenuto dei dispositivi.

Dal punto di vista investigativo è comprensibile la non rosea situazione: gli indagati spesso e volentieri non forniscono le credenziali - per svariati motivi - rendendo blindato il sistema a cui è necessario accedere (si pensi alle evidenze digitali estraibili che potrebbero essere di ausilio nell'individuazione di terroristi, di bambini scomparsi, di pedopornografia) .

Anche se l'utilizzo del lettore biometrico (impronte digitali) sembra possa agevolare le richieste degli inquirenti - essendo elementi fisici che possono essere carpiti -, è bene tener a mente che, passate alcune ore dall'ultimo sblocco, sarà sempre e comunque necessario inserire il PIN.

Anche dal punto di vista di Apple, le notizie non sono certamente rassicuranti. La nuova versione del sistema operativo installato sui suoi smartphone e tablet, iOS 11, giunto attualmente alla release 11.2.6, contiene nuove misure di sicurezza che hanno un impatto rilevante sulle indagini, rendendole più ostiche.

Fino alla versione 7 di iOS la sincronizzazione tra un iPhone e un pc/mac non richiedeva conferme di nessun genere da parte dell'utente. Dalla versione 8 alla 10, è diventato obbligatorio confermare il "*trust*" sulla finestra che compariva subito dopo lo sblocco dell'iPhone; oggi **è necessario** inserire il Pin o la password solo per attivare la sincronizzazione o avviare un backup.

Palesemente, per avviare l'acquisizione forense di una periferica Apple è necessario disporre del PIN, non essendo utile l'impronta digitale. Pochi giorni fa, sul sito web di Cydia https://www.ios9cydia.com/ , è stata rilasciata la release che consente la funzionalità di *jailbreak* per la versione 11.2.6 di iOS e che dovrebbe consentire, - non ho ancora avuto modo di testarlo in laboratorio -, un'agevole acquisizione fisica del dispositivo in esame (va ricordato che, essendo la tecnica di *jailbreaking* altamente invasiva, è bene utilizzarla come *extrema ratio*).

Se il dispositivo è bloccato e non si conosce il PIN, è possibile accedere a parte del suo contenuto mediante un file particolare denominato "***lockdown***", reperibile sul computer in cui è stata effettuata la sincronizzazione, senza in realtà sbloccarlo. Ma anche in questo vi sono dei limiti: la versione 11 di iOS non consente l'utilizzo dei file di *lockdown* eventualmente ritrovati se questi non rispecchino alcune caratteristiche:

- blocco per meno di 48 ore del dispositivo mobile;
- 8 ore se negli ultimi 6 giorni è stata utilizzata solo l'impronta digitale e non è stata mai inserita la password di sblocco.

Ma vi è di più:

la Apple ha deciso di spingere i possessori di dispositivi muniti di iOS 11 ad abilitare **l'autenticazione a due fattori.** Detta procedura prevede l'inoltro di un SMS con un codice di verifica da indicare negli accessi con l'AppleID o all'area cloud. Tutto ciò implica un'ulteriore difficoltà per gli investigatori che debbono acquisire il backup in cloud: non possono farlo senza

che l’utente se ne accorga.

Resta comunque la possibilità di accedere ai dati online degli utenti Apple se si riesce a venire in possesso di un computer che abbia accesso a iCloud; l’acquisizione del cosiddetto “***token***” permetterebbe il bypass del nome utente e della password.

Anche gli Apple Watch - sistema operativo WatchOS derivato da iOS - contribuiscono non poco alla difficoltà di estrazione ed analisi. L’ **Apple Watch Series 3**, presentato nel **keynote** insieme ai nuovi **iPhone 8 e X è infatti divenuto autonomo dall’iPhone grazie alla connettività LTE che ne permette l’utilizzo anche a distanza dal telefono. Quindi: niente SIM, niente analisi.**

Ma non solo: non è più possibile per gli investigatori, almeno momentaneamente distinguere quale dispositivo è stato utilizzato per effettuare una chiamata: sia l'Apple Watch che l'iPhone usano lo stesso numero di telefono. Non è chiaro al momento se i database della cronologia delle chiamate possano avere dei flag per distinguere il dispositivo dal quale sia partita o ricevuta la chiamata.

L’analisi dell’Apple Watch potrebbe rivelare dati importanti riguardo l'utilizzo delle App dell'utente e potrebbe essere in grado di rivelare informazioni su determinate attività fisiche dello stesso che non potrebbero essere trovate con la sola analisi dell’iPhone.

Infatti, mentre gran parte dei dati a cui accede un utente Apple Watch passa semplicemente attraverso il dispositivo e in realtà proviene dall’iPhone stesso, dette attività possono lasciare tracce sullo smartwatch, che una mirata analisi forense può rivelare.

Attualmente ci sono quindi molte domande che attendono risposte.

Una cosa è certa: i messaggi e le mail che transitano dai dispositivi mobili sono ormai milioni; la quantità dei dati sarà uno dei più grandi problemi per le investigazioni e ciò dovrà comportare un approccio sensibilmente diverso al trattamento degli stessi.

I servizi cloud rappresentano la vera sfida del futuro e forse l’unica alternativa in caso di dispositivi bloccati o cifrati; questi ambienti, fortemente virtualizzati e distribuiti, non consentono per ovvie ragioni fisiche e giuridiche, un’acquisizione fisica del dispositivo, ma permettono la lettura dei dati, mediata dall’infrastruttura cloud, con le stesse criticità già citate.

Per il futuro, gli operatori del settore dovranno individuare nuove metodologie forensi atte a rendere valide ed ammissibili le prove acquisite in giudizio per il tramite della tecnologia cloud.

Ad oggi, sulle tematiche della Mobile Forensics e della Mobile Cloud Forensics, rimangono aperte diverse questioni tecniche e giuridiche; primeggia comunque il dibattito tra la privacy degli utenti e le esigenze di Giustizia, che a parere del sottoscritto, dovrebbero essere mediate per l’ottenimento di un buon compromesso.

NOTE

- [1] Alla data di stesura dell’articolo, le factory image stabili ed i file OTA della versione 8 (**Oreo)** non sono ancora disponibili al download, tra l’altro solo per alcuni dispositivi.
- [2] In informatica l'espressione **comunicazione tra processi** (in inglese **Inter-Process Communication** o **IPC**) si riferisce a tutte quelle tecnologie software il cui scopo è consentire a diversi processi di comunicare tra loro scambiandosi dati e informazioni. https://it.wikipedia.org/wiki/Comunicazione_tra_processi
- [3] La tecnologia ASLR (Address Space Layout Randomization) viene implementata come sistema di protezione minimo per contrastare i tentativi di attacco di tipo buffer overflow.
- [4] NX technology, developed by NoMachine, and commonly known as 'NX' is a proprietary computer program that provides hosted desktop and remote access. It consists of a suite of NoMachine software products related to desktop virtualization and application delivery for server-based computing and cloud-based environments. https://en.wikipedia.org/wiki/NX_technology
- [5] *"GCC extension for protecting applications from stack-smashing attacks"*. Research.ibm.com*. Retrieved 2014-04-27*.

A cura di: **Cosimo de Pinto**