

Introduzione alla mobile forensics

di Cristina Pagetti

www.perizieinformatiche.it

Con "mobile forensics" si intende l'analisi di dispositivi mobili quali cellulari, I-Pod, sistemi di comunicazione wireless, telefoni satellitari, ecc.. Questi elementi sono potenzialmente in grado di contenere una grande quantità di informazioni: basti pensare ai dati in esso contenuti e, nel caso dei cellulari, a quelle relative alle azioni dell'utente quali, ad esempio, la sua radiolocalizzazione. Le informazioni recuperate quindi dai dispositivi mobili sono sempre più richieste come prove, in indagini della Magistratura visto che questi dispositivi sono spesso a disposizione di soggetti coinvolti in attività criminali e che l'Italia è in cima a tutte le classifiche per tasso di penetrazione e numero di cellulari posseduti da ogni utente.

La mobile phone forensics :

Il veloce sviluppo del settore della telefonia mobile fa sì che i telefoni cellulari stiano diventando strumenti sempre più potenti e con maggiori funzionalità e quindi occorre definire una metodologia di indagine rigorosa alla quale fare riferimento.

Visto che il terminale **UMTS** (Universal Mobile Telecommunications System), la tecnologia di telefonia mobile di terza generazione successore del GSM che presto soppianderà tutti gli altri protocolli, è un computer a tutti gli effetti, si vanno definendo procedure molto simili a quelle adottate con i computer con strumentazioni e problematiche però molto differenti.

Introduzione

Un telefono cellulare è un sistema dedicato composto da una CPU, una RAM, una SIM o USIM (l'equivalente di una SIM nel protocollo UMTS).

La tecnologia tipica dei cellulari sia essa GSM, GPRS o UMTS, fa in modo che non sia il radiotelefono a contenere i dati dell'abbonato ma la, **SIM-Card** (Subscriber Identity Module), una smartcard ("carta intelligente") da inserire nell'apparecchio che si desidera utilizzare. Ad essa è associato un numero seriale che sui sistemi informativi di un operatore telefonico consente di risalire a un determinato cliente dei propri servizi di telefonia mobile. La SIM-Card, estraibile dal cellulare, contiene un circuito integrato dotato di memorie volatili e non volatili.

L'abbonamento fa quindi riferimento alla carta **SIM** e non al radiotelefono. I dati permanenti che caratterizzano l'utente sono registrati dal gestore radiomobile in aree di memoria "read-only" della SIM protette in modo da non essere accessibili ai normali utenti. Tali dati riguardano l'identità "**IMSI**" (International Mobile Subscriber Identity) dell'abbonato radiomobile, la chiave di autenticazione del cliente "**KI**" (Key Identity), gli algoritmi di calcolo utilizzati per quest'ultima attività ed anche per la cifratura della conversazione. All'utente, come noto, rimangono accessibili i campi per l'inserimento dei codici **PIN** (Personal Identification Number) che deve essere digitato ogni volta che si accende l'apparecchio per abilitare l'uso della SIM. e **PUK** (PIN Unblocking Key) utilizzato per sbloccare la scheda.

Occuparsi di cellulari significa occuparsi non solo di segnali vocali ma sempre più spesso immagini, video, SMS, email, ecc.

Analisi dei cellulari: isolamento, spostamento e clonazione

Un telefono cellulare attivo presenta diversi problemi sia all'atto del ritrovamento che nella successiva analisi:

- spostare il dispositivo collegato alla rete di telecomunicazione vuole dire quasi certamente alterarne il contenuto al momento del cambio di cella

- il dispositivo attivo può continuare a ricevere chiamate e messaggi che possono determinare ulteriori alterazioni (a prescindere dal fatto che tali ricezioni possano essere utili o meno da un punto di vista investigativo).

La prima cosa da fare quando si sequestra un cellulare è l'isolamento elettromagnetico e, se questo non è possibile, lo spegnimento. Successivamente allo spegnimento è possibile effettuare copie separate della memoria del terminale e della SIM per poi passare all'analisi dei dati mediante un'opportuna workstation.

I vincoli investigativi

Il repertamento sulla scena del crimine dei telefoni cellulari, e la loro successiva analisi forense in laboratorio, costituiscono un settore di studi emerso recentemente come appendice del forensic computing ed ora prepotentemente in auge come area a se stante date le discrepanze che si sono presentate dovute ai seguenti fattori:

- la portatilità dei dispositivi oggetto di analisi
- l'impiego di particolari interfacce, di batterie e di hardware estraneo a computer e server
- l'impiego massiccio di memorie volatili in perenne alimentazione che sostituisce la memoria di massa utilizzata come magazzino semipermanente di dati
- la presenza di stati di "idle" o ibernazione automatici, per contrastare lo spreco della limitata energia contenuta nelle batterie, che determinano cambiamenti anche indesiderati dei dati delle memorie e talvolta simulano situazioni di spegnimento dei dispositivi (es. monitor nero, insensibilità ai tasti, ecc.);
- l'assenza di uno standard costruttivo universale, che determina l'esistenza di famiglie di dispositivi in grado di fornire gli stessi servizi digitali basandosi su hardware sostanzialmente diversi ed il cui approccio durante l'analisi forense deve quindi essere differente
- la continua produzione di nuovi cellulari e smart phone
- la presenza di sistemi operativi ad hoc di carattere proprietario e quindi non aperti

I principi del forensic computing, quali l'immodificabilità dei dati del reperto, il logging delle attività di indagine, devono comunque essere seguiti anche nel repertamento ed analisi dei cellulari.




Il cellulare sulla scena del crimine

Lo spegnimento del dispositivo, seppur impiegato per impedire che chiunque vi acceda fisicamente compiendo eventualmente danni, non è l'approccio migliore in assoluto e sicuramente non è quello che fornisce i risultati delle analisi nel più breve tempo possibile. Questo perché:

- il sistema spento potrebbe chiedere, in fase di riattivazione, un PIN sconosciuto
- la batteria tenderà a scaricarsi lentamente fino ad esaurirsi da cui la necessità di procedere all'acquisizione del relativo alimentatore;
- le batterie possono essere più di una ed alcune di esse, se rimosse o esaurite possono determinare perdite definitive di dati.

Trovare un tecnico specializzato in grado di procedere con l'esame del dispositivo (non disattivato!) in prossimità della scena del crimine sarebbe ottimale, a patto che il tutto avvenga in una camera schermata.

A questo proposito sono stati realizzati diversi dispositivi di grande utilità per l'analisi in tempo reale ed il trasporto. Ad esempio le Jamming device, le tende di Faraday e i contenitori schermati.

| | |
|--|---|
|  | <p>Esempio di Jamming device in vendita su ebay . Consente di impedire l'utilizzo dei telefoni cellulari e quindi di inibire il funzionamento dello stesso senza doverlo spegnere Costo: 149 Euro</p> |
|  | <p>La Wireless StrongHold Tent (brevetto richiesto) della Paraben è progettato per permettere l'acquisizione sicura di dati da dispositivi wireless impedendo la fuoriuscita del segnale stesso dall'area di acquisizione. La struttura protettiva è trasportabile e può ospitare una persona ed un pc portatile per eseguire l'acquisizione. Costo: 1400 euro circa</p> |
|  | <p>La Wireless StrongHold Bag della Paraben è il contenitore perfetto per ogni tipo di dispositivo wireless. L'incident response team può usare tale contenitore per schermare il dispositivo da segnali wireless che potrebbero inquinare la fonte di prova. Lo speciale materiale a triplo strato con cui la borsa è realizzata (Nickel, Rame, Silver Plate Nylon) è la chiave per proteggere il device in esso contenuto dai segnali indesiderati. Costo: 34 Euro</p> |

L'Analisi del contenuto dei cellulari

I metodi per l'analisi delle SIM e degli smart phone sono in continuo aggiornamento e sono implementati mediante sia strumenti sia hardware che software. Diviene importante ai fini dell'analisi capire di che tipologia di telefono mobile si tratta ed impiegare metodi e strumenti adeguati al fine di rilevare velocemente le informazioni più opportune. **A questo proposito si dividono i dispositivi mobili fondamentalmente in 3 categorie:**

Basic phone: implementa i servizi di SMS e chiamata vocale;

Advanced phone: implementa i servizi del basic più gli EMS , una forma di chat basata su SMS, un collegamento ad un email server per la gestione di una particolare casella e la navigazione su WAP;

High End phone: allarga i servizi degli advanced phone al più ampio spettro del full instant messaging (IM) supportando uno specifico applicativo come client software, del multimedia messaging con gli MMS, della posta elettronica supportando i protocolli POP /IMAP ed SMTP nonché la possibilità di navigazione reale su Internet mediante HTTP.

Per ognuna di queste categorie di telefono si deve procedere ad una tipologia di analisi differente perché molto diverse sono le informazioni rilevabili evidenti e nascoste. Gli smart phone sono ovviamente high end phone per cui richiedono l'analisi più avanzata.

Le SIM/USIM

Al contrario delle media card le SIM sono unità altamente standardizzate, con un contenuto uniforme e protocolli di interfaccia ben noti. Per questo motivo sono nati dei tool software che operano attraverso lettori di smart card i quali sono in grado di copiare i dati di basso livello della SIM per poi interpretarli fornendo informazioni utili all'investigatore tecnico.

L'hardware del telefono

L'analisi dell'hardware del cellulare o smart phone, escludendo SIM e media card, rimane l'attività più complessa ma anche quella che produce mediamente una notevole mole di risultati investigativi.

L'analisi può essere condotta su tre livelli possibili e precisamente:

1. **non invasiva**: copia dei dati e ricostruzione mediante interfaccia specializzata che collega il terminale radiomobile ad un PC il quale, con un software speciale prende il comando del sistema embedded - è un'ottima modalità per rilevare dati cancellati (es. SMS, MMS, ecc.);
2. **semi-invasiva**: in camera schermata impiegando l'interfaccia del sistema mobile che opera sulla SIM/USIM inserita ed operativa - metodo sicuro e veloce ma limitato riguardo la varietà dei dati estraibili;
3. **invasiva**: copia dei dati mediante estrazione fisica dei chip di memoria - ottima e completa, soprattutto in presenza di sistemi danneggiati, ma difficilmente di natura ripetibile.

Un nuovo strumento ma ... occhio alla privacy!

Un nuovo strumento, chiamato **Cell Phone SIM Card Spy** permette di recuperare i dati che avete cancellato. Per usarlo (è una chiave usb) basta inserire la scheda sim nel dispositivo e collegarlo al pc: sul vostro computer potrete così leggere e modificare tutte le informazioni salvate sulla scheda, inclusi i messaggi cancellati



Due le funzioni principali: quella spia e quella di recupero dei dati. Quest'ultima è possibile mediante il software **Recovery PRO**. La prima si può realizzare mediante il software **SIM Card spy**.

In definitiva è possibile cancellare, editare, salvare le informazioni presenti nella propria SIM, nel caso in cui si debba cambiare SIM o telefono ma anche recuperare informazioni che si credevano perdute per sempre.

Todd Morris, presidente della BrickHouse azienda produttrice ha detto al New York Post che con questo strumento "*Circa la metà delle persone sposate trova qualcosa di negativo sul cellulare del partner. Pensano di avere cancellato i loro messaggi, ma si sbagliano*". Per giustificare l'utilizzo l'azienda afferma che questo dispositivo è utile (anche) ai genitori per controllare i propri figli e ai manager di un'azienda per controllare l'uso che i propri dipendenti fanno dei telefonini aziendali.

Occorre ricordare che **Cell Phone Sim Card Spy** è un dispositivo che viola la privacy, anche nel caso in cui lo si utilizzi per controllare i propri figli, ma Morris ha comunque un suggerimento per chi è preoccupato della propria privacy: "*Prendete la SIM card e distruggetela, o tagliatela. Questo è l'unico modo per avere una garanzia che i dati vadano persi*".

Se utilizzato per l'analisi forense va ovviamente collegato ad un write blocker che va interposto tra di esso e il computer che esegue l'analisi, per garantire l'accesso alla Sim card in sola lettura.

Bibliografia:

www.wikipedia.it per il significato dei termini tecnici

Articolo di Marco Mattiucci, "Mobile forensic", da www.marcomattiucci.it

Articolo di Massimo Adduci, "Mobile forensic", da www.cybercrimes.it