La Apple contrasta con un brevetto i cell-site simulator stingray. Una forma di Trusted Computing?

Author : Michelangelo Di Stefano

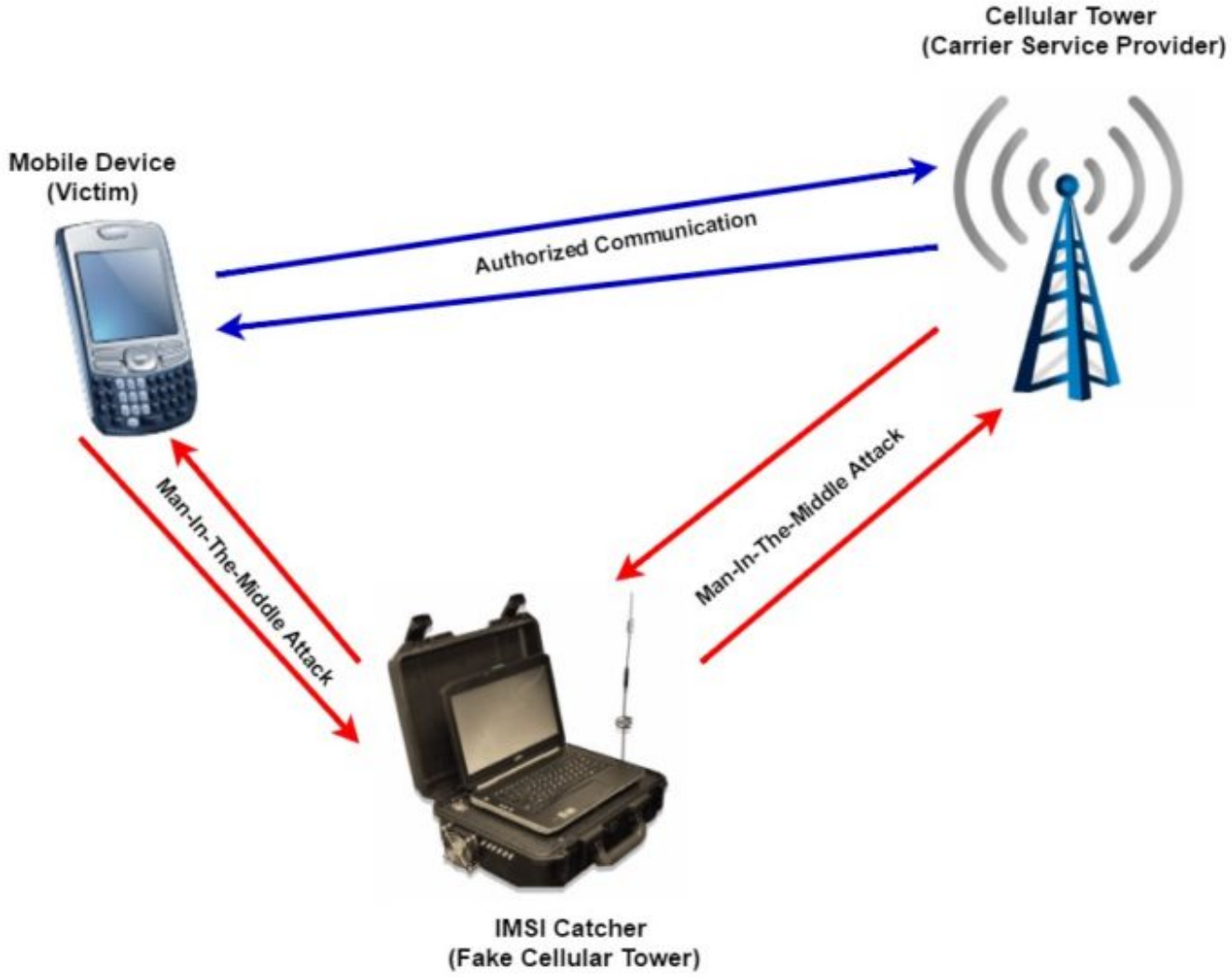
Date : 15 Marzo 2019

Si parla sempre più frequentemente di **caselle *stingray***, un prestito linguistico inglese ben diverso dall'interpretazione letterale del "pesce razza". Il termine descrive, nelle comunicazioni cellulari, uno o più **falsi ponti ripetitori** che, simulando le tradizionali antenne BTS, si insinuano tra *device* e ponte di aggancio con un **attacco *man in the middle***, acquisendo in modo silente copia del traffico prodotto in chiaro (cioè della fonia nel corso della telefonata sulla rete cellulare – e non di quella generata attraverso protocolli VoIP – nonché dei relativi metadati riconducibili all'IMSI/IMEI catturato).

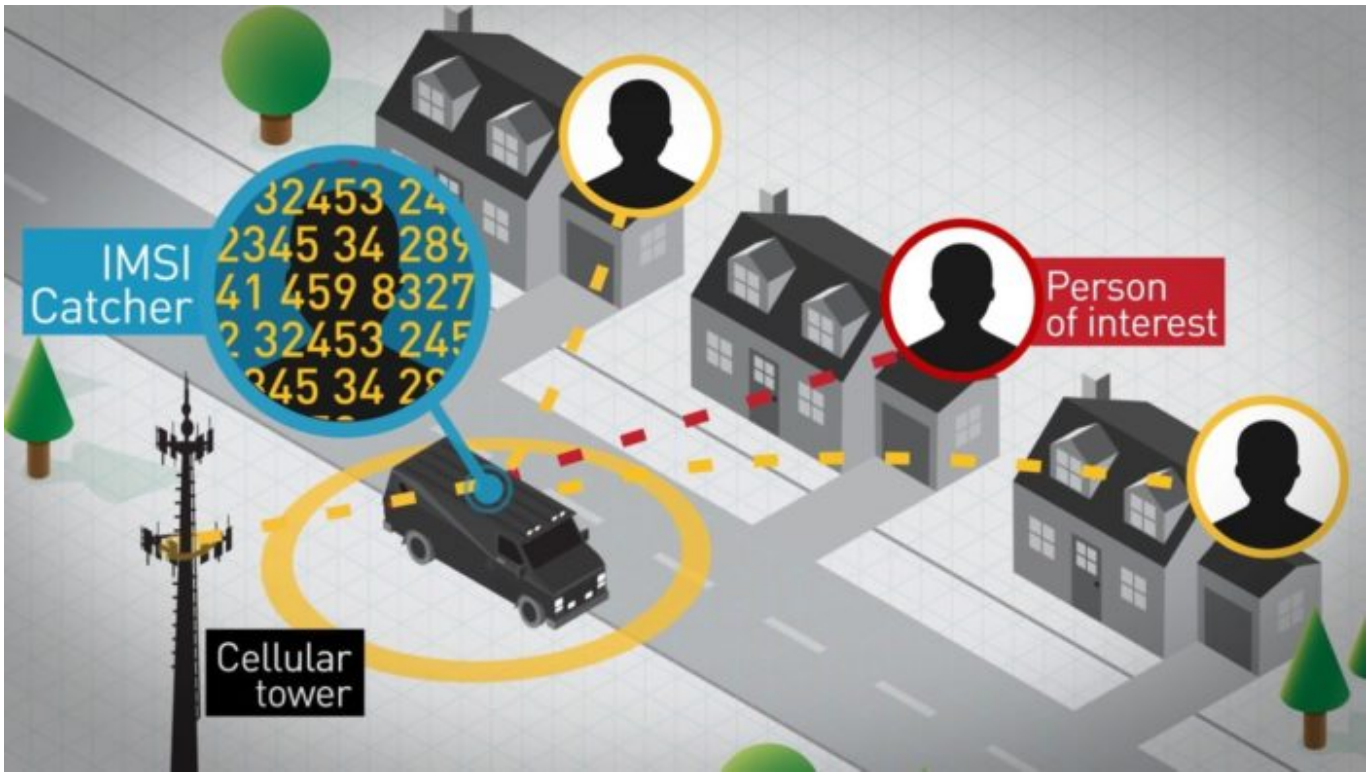
Un attacco che, letto nel contesto dell'architettura delle reti di comunicazione GSM, avviene al livello più elementare di interconnessione, cioè **tra la Stazione Mobile** (o *Mobile Station – MS*, che corrisponde all'apparato telefonico cellulare dell'utente) **e la Stazione Radio Base** (*o Base Transceiver Station – BTS*, che identifica l'apparato radio ricetrasmittente presente in ogni cella).

Si tratta di una **tecnica di *snitch* dinamica**, che “insegue” il *target* frapponendosi tra questo e la BTS, una struttura, quest’ultima, che nella consuetudine delle telecomunicazioni viene rilevata dall’utente automaticamente secondo una prassi “fiduciaria” consolidata, una sorta di **rapporto privilegiato, detto di *trust***, in analogia al termine usato nell’ambito giuridico per inquadrare un “*affido*”.

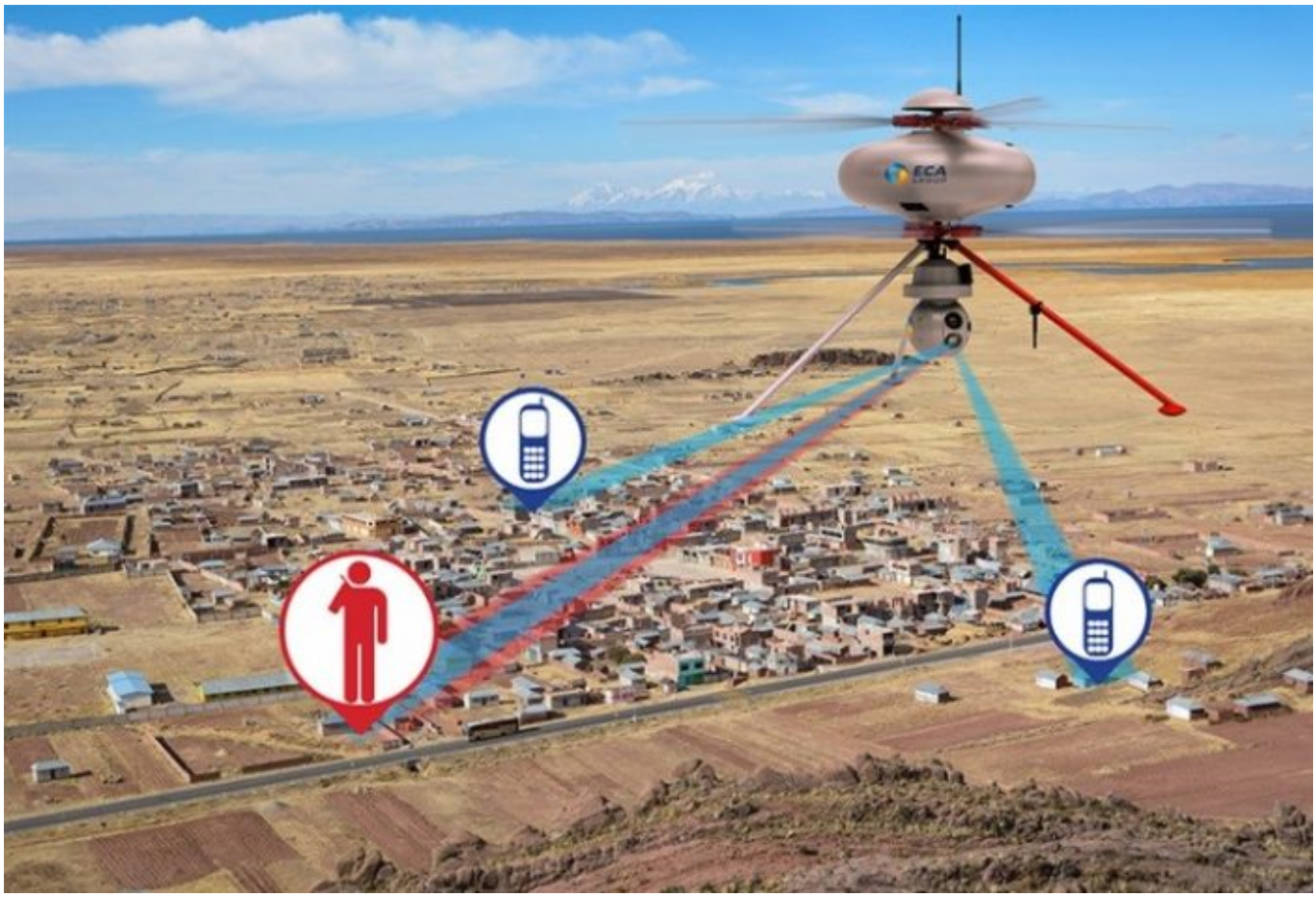
Il presupposto di “*trust*” viene, allora, **ingannato** attraverso pratiche infide di *Treacherous Computing* generate **dai *cell-site simulator* o *C.S.S.,*** simulatori di ripetitori meglio noti con il **termine tecnico *IMSI Catcher.***



Tecnologie *dual use* di intercettazione tattica, in passato in grado di procedere alla scansione della microzona d’interesse rilevando tutti segnali GSM presenti e, da qui, accoppiando IMSI ed IMEI di ogni utente presente sulla rete, riuscendo ad acquisirne i metadati di base.



Strumenti sempre più evoluti ed insidiosi, ormai da diversi anni in grado di "*presentarsi sulla rete*" come una *fake* BTS – in taluni casi robotizzate su sofisticati droni intelligenti – da qui duplicando, in modalità anonima, il flusso di informazioni trasmesse dal *device* ed effettuando la **captazione dinamica dell'apparato in movimento**, se del caso disturbando i protocolli di comunicazione più avanzati che viaggiano attraverso la c.d. *voice over long term evolution (VoLTE)*, degradandone il segnale verso uno *standard* GSM.



Ecco, allora, la nuova trovata di Cupertino: si tratterebbe di un brevetto in grado realizzare una crittografia *end to end* tra la rete (quindi con il "*trust*" rappresentato dalla BTS) e l'ID univoco di un *iPhone*, quindi, si suppone, una forma di privilegiato *trusted computing*.

Attesa la scarna consistenza delle indiscrezioni trapelate è difficile, allo stato dell'arte, comprendere quale sia la portata dello strumento anti intercettazione che - è bene evidenziarlo - riguarderà comunque le intrusioni M.I.T.M. e non le intercettazioni giudiziarie tradizionali che, nella maggior parte dei casi, avvengono attraverso la predisposizione di un sistema di *gateways* (L.I.G.) sulle dorsali parametriche di comunicazione (L.I.N.), a cura dei gestori telefonici.

La *Apple*, nelle sue evoluzioni del *software iOS*, si è sempre distinta, rispetto alle tecnologie concorrenti, in relazione alla sicurezza informatica ed alla tutela della *privacy* verso i suoi consumatori, in primo luogo attraverso una propria piattaforma di acquisti delle applicazioni, con uno *store* sempre monitorato e catalogato, per evitare spiacevoli intrusioni spia.

Una accortezza filtrata "blindando" gli apparati nei vari aggiornamenti, così da aggirare, nel caso di operazioni brutali di *jailbreak,* tentativi di amministrazione del sistema operativo e, conseguentemente, della possibilità di inoculazione di *spyware* o, come indicato dal legislatore nel codice di procedura penale, di "*captatori informatici*".

Un'attenzione, ormai da anni, sempre più raffinata, considerato che il sistema *iOS* da molto

tempo ha introdotto la tecnologia di messaggistica proprietaria *end to end* c.d. *iMessage* (per un certo tempo contrastata soltanto da un analogo sistema, detto *pin to pin*, presente sulle piattaforme *BlackBerry*) e quella di *video call* nota con il termine *FaceTime.*

Un'accuratezza che, considerata l'eventualità di acquisizione di un *iPhone* da parte di soggetti terzi che non hanno il privilegio di amministratore, prevede da tempo opzioni di autodistruzione del contenuto dell'apparato dopo un certo numero di accessi andati a vuoto, adottando perdipiù, già dal modello 5S, l'identificazione biometrica attraverso l'impronta digitale, ormai divenuta obsoleta con le nuove procedure di autenticazione con tecnologie di *imagery intelligence*, attraverso l'identificazione facciale.

Si tratta di applicativi di nicchia che anche i moderni strumenti di analisi forense e di autopsia digitale fanno spesso fatica a contrastare.

Rimane però il quesito di base che, già in passato, ha investito il colosso della mela e quello delle comunicazioni VoIP o della cripto-messaggistica multimediale veicolate dai vari applicativi *social media*: l'esigenza, nel rispetto della *privacy,* di mettere a disposizione delle autorità governative, per esigenze di giustizia e di sicurezza interna, delle tecnologie di comunicazione utilizzate dai gestori.

Espressione, quella attinente i "*gestori telefonici*", che non può più essere intesa, *strictu sensu*, quale onere delle compagnie che gestiscono il traffico ed amministrano le reti, oggi impossibilitate a qualsivoglia forma di controllo sulle comunicazioni digitali protette da autenticazioni *HyperText Transfer Protocol over Secure Socket Layer* (HTTPS), o crittografate da procolli *end to end* e, in alcuni casi, *peer to peer*, sulle innumerevoli piattaforme *social*.

Si tratta di un'esigenza, quantomeno in ambito comunitario, a cautela di quella ossidata, quanto indispensabile, Risoluzione adottata il 17 gennaio 1995 dal Consiglio Europeo in materia di intercettazioni legali delle comunicazioni, recepita in Italia soltanto nel 2003 con il Decreto Legislativo 1 agosto 2003, n. 259 che ha disciplinato, per la prima volta, il ***Codice delle comunicazioni elettroniche*** nell'ordinamento interno.

Articolo a cura di **Michelangelo Di Stefano**