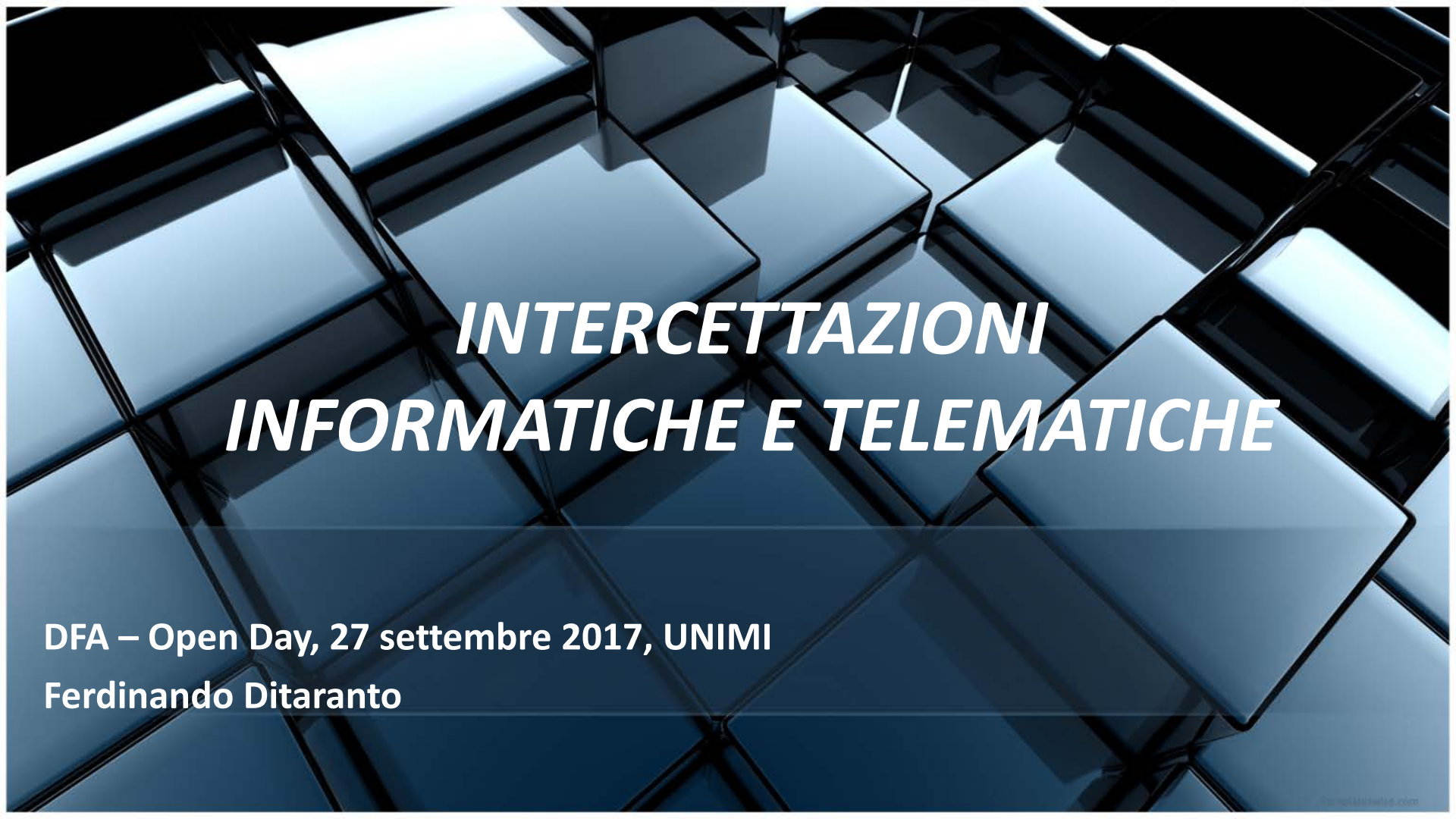


INTERCETTAZIONI INFORMATICHE E TELEMATICHE

DFA – Open Day, 27 settembre 2017, UNIMI

Ferdinando Ditaranto

WHO I AM

- ***Referente Area Reati Informatici*** *presso la Sezione di Polizia Giudiziaria della Procura della Repubblica di Monza;*
- ***Digital Forensics Specialist e Cyber Investigator****;*
- ***Perfezionato in Computer Forensics e Investigazioni Digitali*** *presso UNIMI (aa 2011/2012);*
- ***Certificazione CIFI*** *(Certified Information Forensics Investigator) e Tutor e-learning IISFA;*
- ***Certificazione ACE*** *(Accessdata Certified Examiner)*

Cosa si “captava” in passato

- Lettera
- Telegramma
- Telefono/Fax
- Cellulare
- SMS
- Email
- Web
- Chat

Monitoraggio dell'*intelligence* militare

- **Analisi di sessioni massive di traffico** (anche satellitare), attraverso l'uso di *filtri parametrici* (cd. *Sonde*) che scandagliano i dati in transito sui nodi di macrocomunicazione (cd. *dorsali o backbone*).
- Progetto **ECHELON** "*I cinque occhi*", elaborato dagli Stati Uniti, e supportato da UK,Nuova Zelanda, Canada e Australia, nel quale venivano impiegate tecniche sia generiche di elaborazione del parlato (cd. *Speech Processing*) o del testo (cd. *Natural Language Processing*), sia avanzate come quelle di analisi semantica (cd. *Intelligence Data Mining*) che consentono di individuare termini predeterminati. Fino a arrivare a tecniche, ancora più evolute, come la *decifratura* o l'individuazione *steganografica*.

Monitoraggio investigativo

- Si concentra tipicamente su **singole sessioni di traffico**.
- **Intercettazioni giudiziarie**(artt.266 e ss. Cpp) e **intercettazioni preventive** (artt. 226 att. Cpp e 12 L.133/2012).
- *Providers* di connettività **canalizzano il flusso di dati cifrato** (audio, video e informazioni) **verso *server* dedicati** allocati all'interno delle Procure della Repubblica (art.268 comma 3° Cpp), da cui viene **poi reindirizzato** (cd. *remotizzazione*) verso singole postazione della polizia giudiziaria (*procedura standardizzata*).
- **L'operatore di P.G. dispone di una potente interfaccia remota di controllo** con cui può, ad esempio, monitorare diverse utenze telefoniche, ascoltare un'intercettazione ambientale, regolare la sensibilità dei microfoni o applicare dei filtri ai rumori di fondo, incrociare dati, pilotare telecamere o controllare un *Trojan*.

Elemento determinante : “Fattore umano”

L’operatore di Polizia Giudiziaria *deve possedere sia* ***competenza*** *sia* ***esperienza****, caratteristiche imprescindibili che, attraverso la* ***contestualizzazione*** *e la* ***correlazione*** *del dato, consentono la* ***corretta interpretazione dell’informazione*** *carpita.*

Le intercettazioni dati nel passato “ADSL Tapping”

PASSIVE NON-INTRUSIVE ADSL TAPPING PROBE ON A ANALOG LINE

[redacted] is a system allowing the acquisition on the analog link of the data IP which pass in transit on the ADSL links.

MAIN FEATURES

- Fully passive and non-intrusive system with high impedance interface (undetectable from Customer premises equipement and Central Office).

Le intercettazioni dati nel passato “ADSL Tapping”

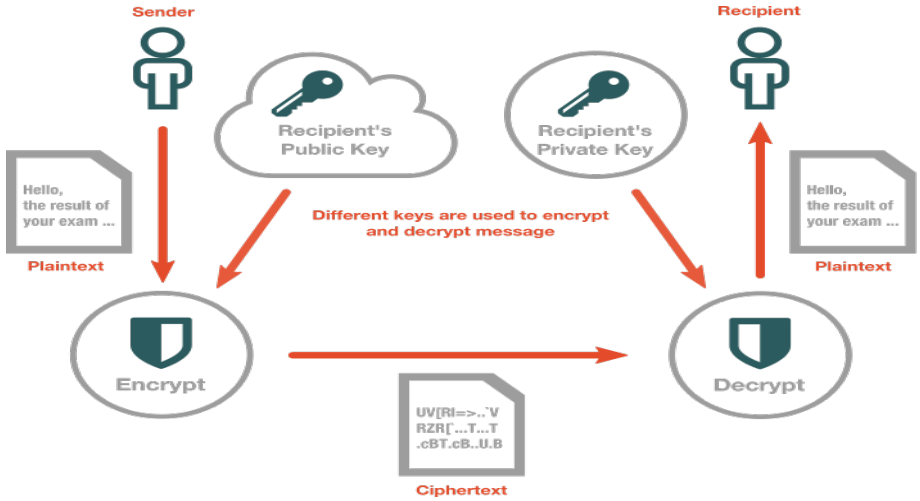
Arriva la privacy (ma per pochi)

- PGP/GPG (Zimmerman). Il fautore della crittografia asimmetrica come software libero alla portata di tutti.
- Criptofonini (2002-oggi)

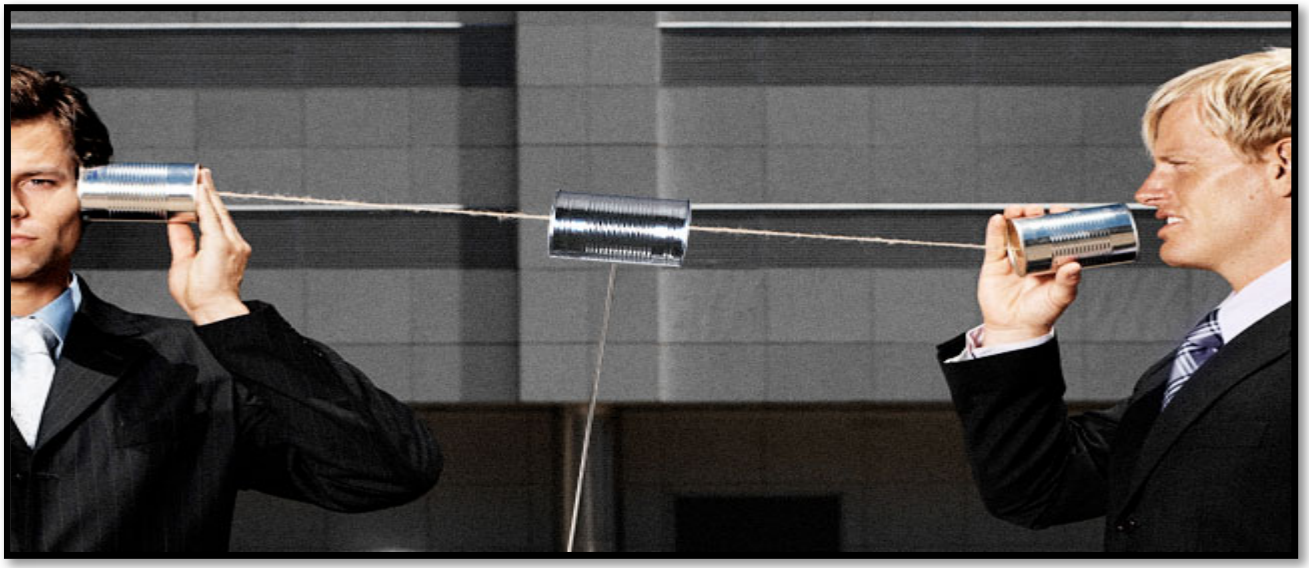

CRONACA

Messina Denaro e il telefono imprendibile da 4.000 euro

Un pentito: "La primula rossa di Cosa Nostra usa un cellulare di lusso e non intercettabile"



Il declino del MAN IN THE MIDDLE



LA CRYPTO-MOBILE

Crypto Voice IP
Email, Messenger, Files

Il sistema di sicurezza dell'informazione [redacted] garantisce la protezione crittografica dei dati su computer e tablet durante la connessione internet:
-messaggi di testo;
- E-mail;
- file (foto, audio, video, documenti);
- chiamate VoIP
Il sistema [redacted] garantisce la comunicazione sicura sui social network: Skype, Viber, Facebook, Twitter e LinkedIn.

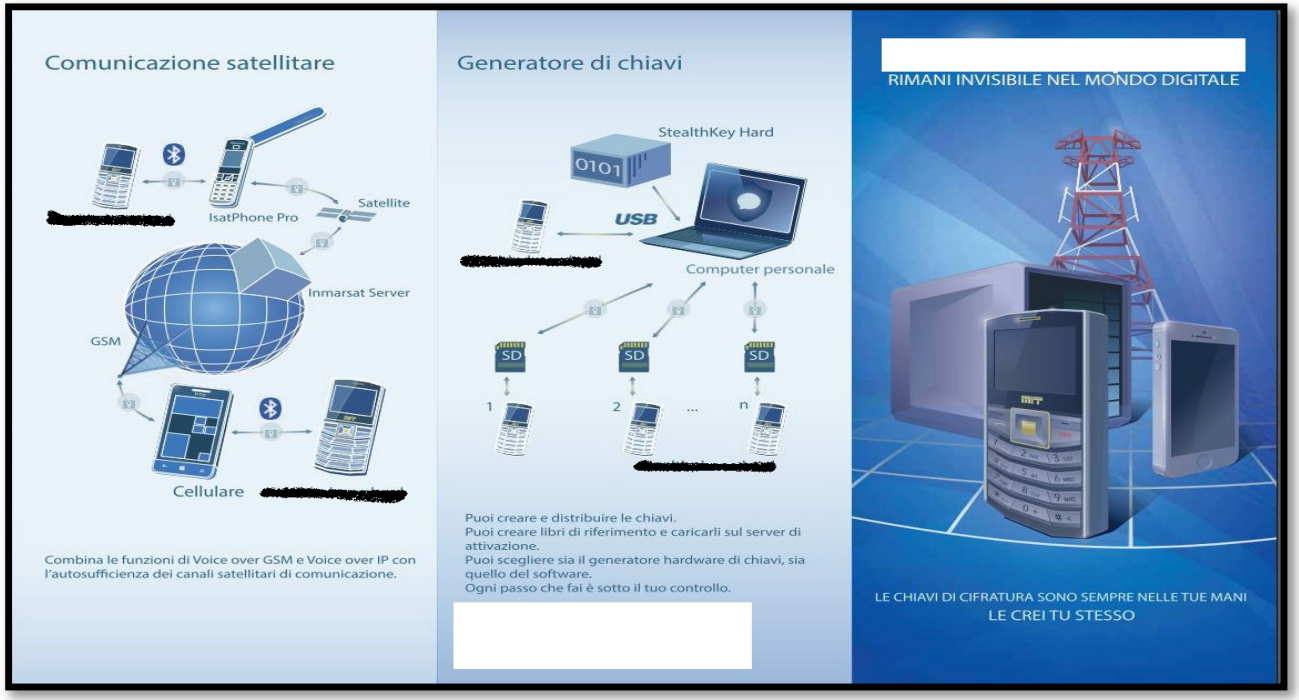
Crypto Voice over GSM

La cifratura nei canali di comunicazione esistenti: Skype, Viber, reti satellitari e telefoniche o stazioni radio

Crypto OfficeGate

Garantisce la protezione crittografica per la tua rete corporativa. La soluzione hardware e software per lo scambio sicuro di informazioni tra una rete corporativa locale (telefono o IP) e utenti remoti per mezzo delle soluzioni [redacted] installate.

LA CRYPTO-MOBILE

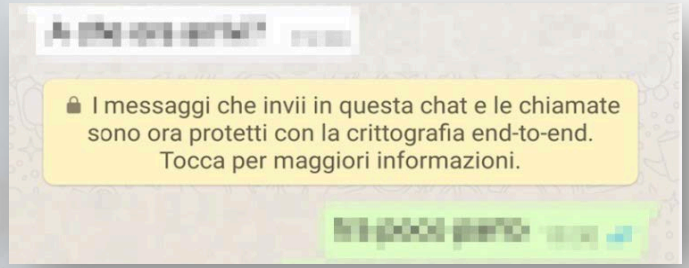


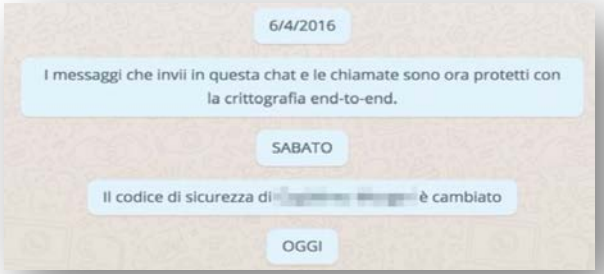
Le nuove tecnologie sono per (quasi) tutti

- Sistemi di messaggistica (chat/audio/video) su PC
  - Skype, Jabber, Facebook Messenger
- Sistemi di messaggistica (chat/audio/video) su cellulare
  - Whatsapp, Telegram, Signal, Viber, Snapchat, Twitter, Google
- Chiamate VoIP
  - Facebook Messenger, Whatsapp, Signal
- La rete Tor
  - Chat sul Dark Web
- Protocolli alternativi
  - BitMessage

La cifratura “end-to-end”

- Whatsapp, Telegram, Signal, Viber
- Chat, audio, video ma anche file e desktop sharing
- Cifrate fin dall’inizio, vanno ora verso cifratura **end-to-end**
- Inutili gli attacchi **verso il server del *provider***





La *cifratura “end-to-end”*

- La sicurezza si sposta sul dispositivo, non più sul server che diventa un mero “tramite” spesso senza archiviazione log
- Differenza tra cifratura semplice ed end-to-end:
  - La cifratura “**semplice**” prevede che la chiave sia condivisa con il server e quindi i messaggi siano visibili ad esso (può archiviarli)
  - La cifratura “**end-to-end**” fa sì che la chiave sia nota soltanto agli interlocutori (il server non legge né archivia i messaggi)

Il “Tallone di Achille” della *cifratura end-to-end*

- Risulta vulnerabile alla tecniche di **Spoofing** (cd. falsificazione dell’identità digitale)**.** L’attaccante potrebbe avviare uno scambio di pacchetti simulando di essere uno dei nodi legittimati allo scambio e, pertanto, otterrebbe le chiavi di cifratura e, dunque, riuscirebbe a decifrare i messaggi.
- Il ***device*** che contiene le chiavi di cifratura **potrebbe essere violato** attraverso una vulnerabiltà non nota (Zero Day) del sistema “bersaglio”.

IL MALWARE
(maliciuos software)

- Il malware è un **programma** (sequenza di istruzioni) che ***subdolamente*** si installa su un computer, smartphone, tablet, etc. sfruttando una **vulnerabilità nella sicurezza** del dispositivo (cfr. *exploit*) e consentendo ad un attaccante di assumere il **completo controllo da remoto**.

Come è strutturato:

- Diversi livelli:
  - **Dropper**: componente (facoltativa) che provvede a **scaricare** sul target il vero e proprio “captatore”
    - Email con Allegato, SMS, Link su Whatsapp, rete WiFi, attacco su rete, etc…
  - **Payload**: il “captatore”, un programma che acquisisce le informazioni richieste e le invia a un centro di raccolta (o le archvia per futura acquisizione)

Requisiti (tecnici) dei captatori

- Invisibilità agli Antivirus/Antispyware (almeno del dropper, il payload si può isolare in modo diverso)
- Invisibilità al sistema (nessun rallentamento o processo evidente)
- Possibilità di comunicare con l'esterno senza farsi rilevare (supporto cambio banda, trasmissione differita, etc…)
- Persistenza (a riavvio, aggiornamenti sistema, librerie, etc…)

Potenzialità dei nuovi captatori

- Acquisizione audio/video ambientale (con attivazione silente webcam/microfono)
- Acquisizione dei sistemi di messaggistica/web criptati
- Keylogger
- Acquisizione posta elettronica, documenti, filmati, registrazioni, web history, password, SMS, etc…
- Geofencing (Smartphone)
- Attivazione selettiva su utente (PC)

Perché servono i captatori

- Utenza non necessariamente legata a numeri di cellulare ma solo più al dispositivo (non si sa neanche chi intercettare per via telematica/telefonica…)
- L'utenza si sposta in modo imprevedibile (da ADSL di casa, ufficio, SIM, locali pubblici, hotel, etc...)
- Utilizzo cifratura end-to-end (es. chat)
- Utilizzo cifratura verso i servizi (es. siti web, email, etc…) che
- Utilizzo servizi esteri che tengono dati criptati (lasciando password all'utente) o in luoghi poco collaborativi
- Intercettazione telematica/telefonica inutile

Problematiche tecnico-giuridiche dei “captatori”

- Identificare autore delle fonti di prova
- Stabilire limiti su ciò che si è autorizzati a captare:
  - Quanto (quantità e livello di dettaglio)
  - Quando (orario, giorni, etc…)
  - Cosa (chat, ambientale, video, email, etc…)
  - In che luogo (casa, ufficio, auto, esterno, etc…)
- Non alterare elementi presenti sul sistema
- Non inserire elementi sul sistema

Problematiche tecniche dei “captatori”

- Eccessivo consumo della batteria dei cellulari
- Sopravvivere agli aggiornamenti di sistema
- Evadere antivirus e firewall
- Eccessivo traffico (voce/video in particolare, anche su PC)
- Non diventare porta d’accesso per criminali
- Non poter essere “riciclati” da chi li trova
- Evitare di utilizzare canale voce/dati perché compare nel tabulato di fatturazione dell’utente

Limiti nel funzionamento

- Senza rooting/jailbreak si è limitati nel tipo di dati acquisiti
  - WhatsApp, Facebook, Viber, Skype, Gmail non accessibili altrimenti
  - Audio e video ambientale non accessibili altrimenti
- Anche con rooting/jailbreak, l'aggiornamento del sistema (in particolare su iOS) ripristina lo stato iniziale ed elimina il jailbreak
- Il jailbreak è rilevabile, si può "nascondere" ma con delle App facili da installare è identificabile
- Il jailbreak rende vulnerabile il sistema

Problematiche d'installazione

- Richiede sempre più spesso intervento utente
- Bisogna sapere che telefono usa (se si ha numero si risolve con l'IMEI)
- Molto difficile/impossibile fare rooting/jailbreak da remoto
- I dispositivi sono configurati di fabbrica per non permettere esecuzione di app non autorizzate (verifica applicazioni, debug mode, etc…)
- Anche avendo accesso fisico al dispositivo, può essere presente PIN o cifratura:
  - su iOS si può rimuovere ma richiede tempo e intervento di terzi
  - su Android si può in genere rimuovere
  - su Windows Phone (es. Nokia Lumia) non si può rimuovere…

Rooting (android)

- Su Android è lo “sblocco” dei privilegi di amministratore che permette di accedere a tutti i dati e intercettarne il traffico
- Non è complesso da eseguire, richiede accesso al dispositivo
- Non è realizzabile su tutti i dispositivi

Jailbreak (iOS)

- Su iOS (sistemi Apple) è lo “sblocco” dei privilegi di amministratore che permette di accedere a tutti i dati e intercettarne il traffico
- Piuttosto complesso da eseguire, richiede accesso al dispositivo
- Non è realizzabile sull’ultima versione di iOS e sulla precedente a 32bit
- Gli aggiornamenti di sistema lo “annullano” (è necessario quindi impedire che agli utenti vengano segnalati)

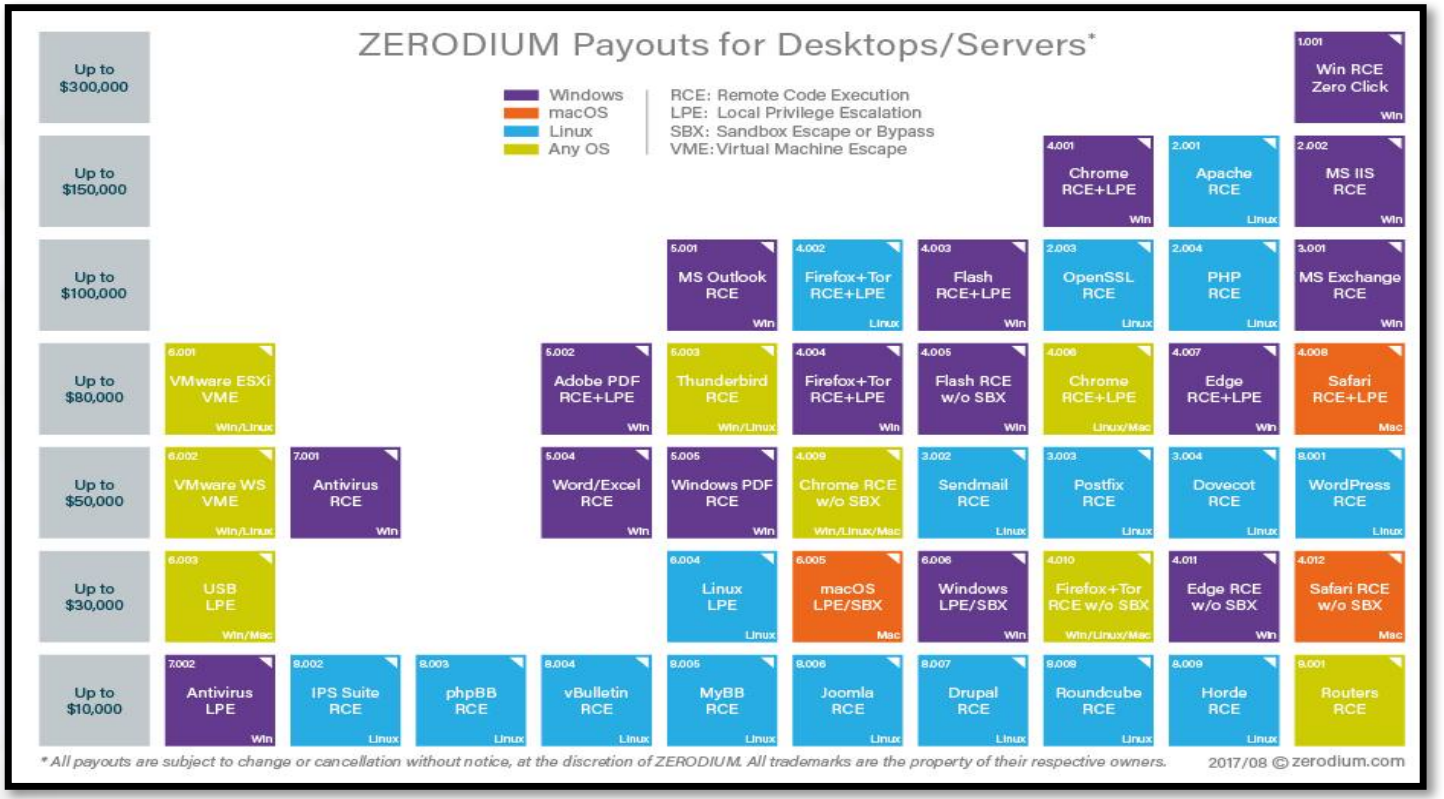
SECURITY

Update all iOS devices to 9.3.5 immediately, or risk a remote jailbreak

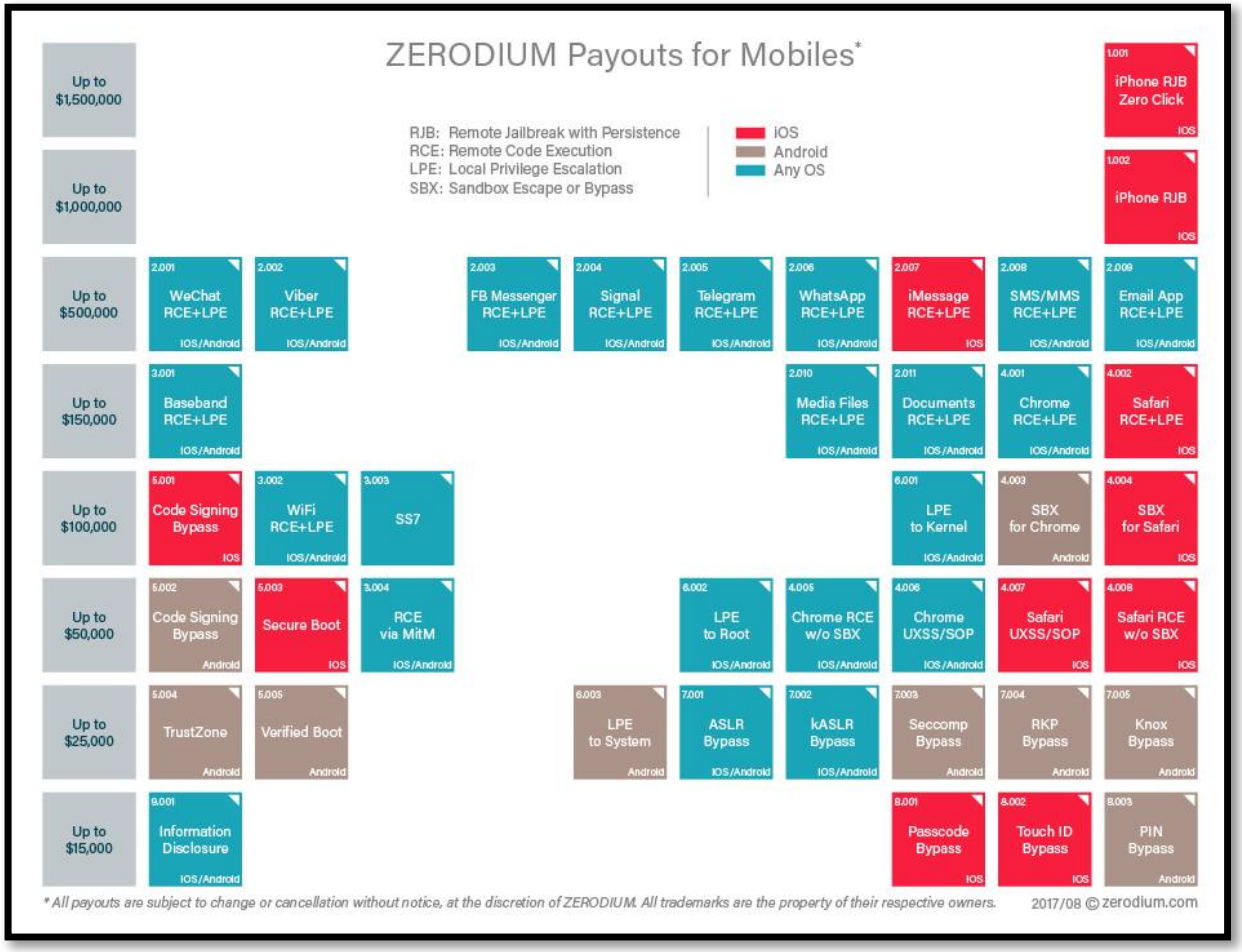
A critical new Apple iOS update patches three iOS flaws that cybercriminals used to steal confidential messages and eavesdrop using device cameras and microphones.

By Alison DeNisco | August 30, 2016, 8:12 AM PST

http://www.techrepublic.com/article/update-all-ios-devices-to-9-3-5-immediately-or-risk-a-remote-jailbreak/



https://www.zerodium.com/program.html



https://www.zerodium.com/program.html

citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Possibili alternative

- Intercettazione tradizionale sulla linea
- Intercettazione avanzata sulla linea (spoofing, rogue cell, SS7)
- Acquisizione locale “fisica” del dispositivo (PIN/Encryption?)
- Acquisizione di dati sincronizzati remoti o backup (Cloud o PC)

Intercettazione tradizionale sulla linea

- Ancora valida per telefonate ed SMS (telefonica)
- Sempre meno efficace per i dati (telematica)
- Utile per localizzazione (telematica in particolare)
- Sul GSM, tenere presente il cambio SIM (IMSI Vs. IMEI)

Intercettazione avanzata sulla linea

- Come per la tradizionale, ma ci si frappone digitalmente nella comunicazione (Man in the Middle/Spoofing)
- Sul GSM, si può fingere di essere la cella BTS e agganciare il telefonino

Intercettazione avanzata sulla linea

- Il protocollo SS7 permette di utilizzare funzioni degli operatori ed eseguire localizzazione, deviazione chiamate, ricevere ed inviare SMS a nome di utenze terze, etc…
- Il problema è che non lo sa fare soltanto l'A.G.

By Exploiting a flaw in the SS7 protocol hackers can access every conversation and text message mobile users send from everywhere in the world.

Hackers can spy on every mobile phone user wherever it is.

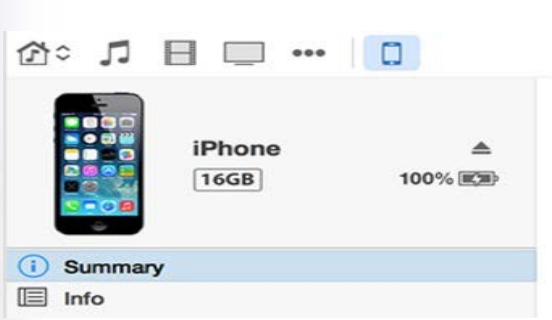
Channel Nine's 60 Minutes has revealed the existence of a security hole in modern telecommunication systems that could be exploited by cyber criminals to listen in on phone conversations and read text messages.

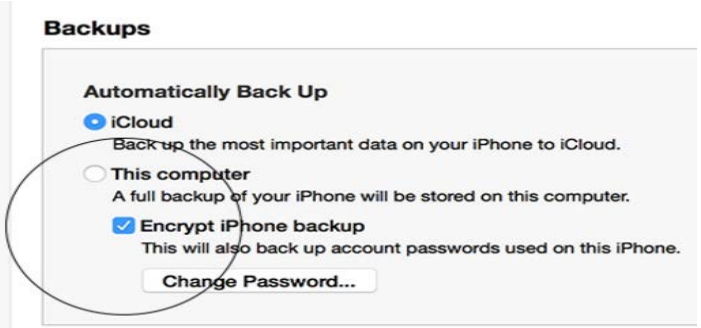
Acquisizione locale “fisica” del dispositivo

- Necessario avere fisicamente il dispositivo, da cui estrarre i dati
- Molto praticata post-sequestro o durante le perquisizioni
- Possibili diversi tipi di acquisizione:
  - Logica: quello che il cellulare è disposto a fornire
  - Filesystem: i file presenti sul dispositivo
  - Fisica: intera “memoria” da cui si può recuperare il cancellato (via software oppure Chip-Off, Flasher box o JTAG)
- Questioni giuridiche legate a **ripetibilità e irripetibilità** dell’accertamento/copia (Art. 359/Art. 360 c.p.p.)

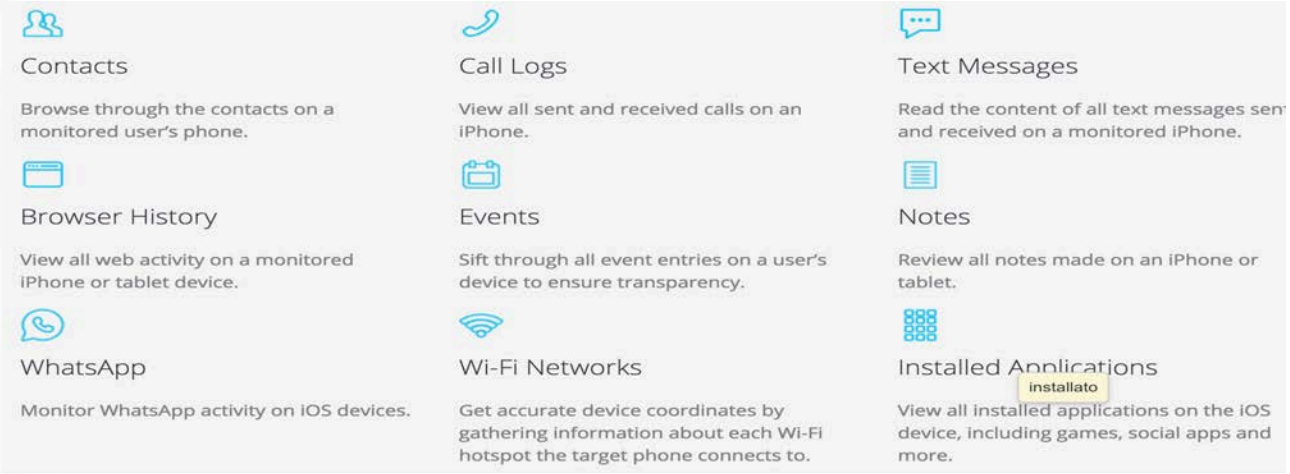
Acquisizione di dati sincronizzati remoti o backup

- Spesso gli utenti eseguono backup su PC o su iCloud
- Anche se l'utente esegue backup criptati, su iCloud sono in chiaro, basta avere le credenziali o chiedere ad Apple





Acquisizione di dati sincronizzati remoti o backup



Acquisizione di dati sincronizzati remoti o backup

- Se si conoscono le credenziali iCloud/Goole, si può acquisire il backup (incuse chat, documenti, etc…) dal Cloud
  - L'utente può aver impostato autenticazione a due fattori
  - L'utente potrebbe non aver abilitato il backup sul Cloud
  - L'utente potrebbe aver cambiato credenziali dopo il sequestro
- Se non si conoscono le credenziali, si possono cercare sul PC sincronizzato (salvate su Keychain o acquisirle direttamente dal token di sincronizzazione) oppure richiedere i dati via MLAT

GRAZIE PER L'ATTENZIONE ☺

http://terenzio.net/parlare-che-stress/

ferdinando.ditaranto@giustizia.it

@enigmadt

it.linkedin.com/in/ferdinandoditaranto