

Introduzione alle Intercettazioni Telefoniche, Ambientali ed Informatiche

Autori:

L. Camporesi, Fondatore e CTO.

Abstract

Nel linguaggio comune, ma anche in quello giornalistico, vi è una diffusa mancanza di chiarezza circa il termine intercettazioni. Questo documento fornisce una definizione generale del termine ed una classificazione dei vari tipi di intercettazioni e delle tecniche d'indagine correlate.

Inoltre, illustra come e perché vengono impiegate certe tecniche, da quali enti, individui ed istituzioni, con quali costi ed i principi di base per la difesa dalle intercettazioni telefoniche, informatiche ed ambientali.

www.mobileprivacy.net

Indice

Introduzione

1 Definizioni

2 Classificazione

3 Linguaggio Comune

4 Intercettazioni Telefoniche Standard

4.1 Praticità e Costi

5 Tecniche di Intercettazione e loro Impiego

5.1 Soggetto che Esegue le Intercettazioni

5.1.1 Istituzioni Private

5.1.2 Istituzioni Estranee

5.2 Rischi per la Segretezza Delle Captazioni

5.2.1 Funzionari Coinvolti Nelle Operazioni a Titolo Professionale

5.2.2 Funzionari Infedeli

5.3 Impiego di Contromisure

5.4 Mancato Impiego di un Mezzo di Comunicazione

5.4.1 Variabili nel Mezzo di Comunicazione

5.5 Contromisure

6 Intercettazioni Ambientali

6.1 Tecniche

6.2 Contromisure

7 Intercettazioni Informatiche

7.1 Tecniche di Intercettazione e Loro Impiego

7.1.1 Cifratura

7.1.2 Modello di Attacco alle Conversazioni Skype

7.1.3 Internazionalizzazione Interconnessioni e Localizzazione Chiamate

7.2 Contromisure

Conclusioni

Introduzione

Negli anni recenti la vita sociale e politica è stata fortemente influenzata dal fenomeno delle intercettazioni telefoniche. Questo potente strumento d'indagine è sempre di più impiegato (almeno in termini numerici assoluti) in indagini penali ed è citato dai media in modo ricorrente. A fianco delle intercettazioni legali, esiste anche un mercato per le intercettazioni illegali, probabilmente molto meno sviluppato rispetto alla percezione comune.

A dispetto della presenza massiccia sui media, vi è una diffusa mancanza di chiarezza, se non addirittura confusione, sul significato di termini come intercettazione, tabulato telefonico, localizzazione. Altrettanto può dirsi per termini e tecniche relativi alle intercettazioni telefoniche, ambientali ed informatiche.

Questo documento offre una panoramica sull'argomento delle intercettazioni nel contesto specifico italiano, storicamente diverso, anche per quanto concerne le tecniche impiegate, da quello di altre nazioni. Vengono proposte alcune definizioni e delle classificazioni di termini specifici e sono presenti riferimenti ad articoli di cronaca e documenti audio-video, interviste a professionisti del settore, letteratura e documenti scientifici. Il tutto, con l'intento di approfondire e contestualizzare l'argomento nell'ambiente nazionale rimanendo lontani da speculazioni puramente teoriche.

Qualunque sia la ragione per volere approfondire il fenomeno delle intercettazioni, è bene avere riferimenti teorici, ma soprattutto informazioni dirette ed affidabili sulla pratica quotidiana, piuttosto lontana dall'immaginario collettivo.

Infine, vi sono valide e fondate ragioni per tutelare le proprie comunicazioni per quanti vivono nella legalità. Il punto di vista anglosassone, per esempio, è molto diverso da quello nazionale. Se nel nostro paese si sentono spesso affermazioni del tipo "Mi intercettino pure, tanto non ho nulla da nascondere", purtroppo anche da personaggi di rilievo, quello tipicamente anglosassone è invece "Se non ho fatto nulla di male perché mi vuoi sorvegliare?". Non dovrebbero esservi dubbi su quale sia l'approccio più civile alla questione.

Per mettere in sicurezza le proprie comunicazioni, occorre avere un'idea di chi può essere un potenziale avversario, quali tecniche di attacco possono essere impiegate e quali contromisure sono disponibili. Questo documento, anche se solo a livello introduttivo, fornisce una visione generale sull'argomento ed un numero di riferimenti utili.

1 Definizioni

Mobile Privacy adotta una definizione di [Glauco Giostra](#), ordinario di procedura penale presso l'Università La Sapienza di Roma. L'*intercettazione* è definita come “Captazione segreta, ad opera di un terzo e con strumenti tecnologici, delle comunicazioni tra due o più persone”. Questa definizione comprende tutte le forme di acquisizione delle comunicazioni, intercettazioni telefoniche, intercettazioni ambientali, intercettazioni informatiche, ecc. ed anche i diversi tipi di dati scambiati, siano essi conversazioni vocali, oppure testo (e-mail, chat) o anche file.

2 Classificazione

Negli Stati Uniti d'America i fondi stanziati per la difesa nazionale hanno fatto sì che un ammontare enorme di ricerca sia stato svolto nel settore dell'*intelligence*. Di conseguenza negli USA sono state anche sviluppate la maggior parte delle applicazioni teoriche e pratiche nel settore delle intercettazioni.

L'attività di intelligence svolta da organizzazioni, Forze di Polizia, agenzie investigative, privati, imprese, criminali, ecc., ha molti punti in comune con le forme di intelligence praticate dal governo degli Stati Uniti.

Mobile Privacy adotta quindi le [definizioni](#) [1] e le classificazioni del Dipartimento della Difesa Americano ([DoD](#)). Le tre categorie di intercettazioni - telefoniche, informatiche ed ambientali - sono considerate ciascuna come un sottoinsieme dell'insieme più ampio dell'*Intelligence delle Comunicazioni*, in lingua originale Communication Intelligence ([COMINT](#)).

3 Linguaggio Comune

Anche nel linguaggio comune, il termine intercettazioni comprende i metodi di ascolto delle conversazioni più frequentemente impiegati dalle Forze di Polizia, dalle agenzie investigative, dalle società e dai privati. Nell'ordine, le intercettazioni telefoniche, le intercettazioni ambientali e le intercettazioni informatiche.

Nel linguaggio comune tuttavia, spesso si parla di intercettazioni anche per l'analisi dei [tabulati telefonici](#) [2]. Questa in realtà può essere ricondotta nell'insieme delle tecniche dell'*Analisi del Traffico*, a sua volta un sottoinsieme dell'*Intelligence delle Comunicazioni*.

4 Intercettazioni Telefoniche Standard

[Numericamente parlando](#) [3], in Italia le intercettazioni telefoniche sono realizzate nella quasi totalità dei casi dalle [Forze di Polizia](#) con l'assistenza tecnica degli operatori di telefonia. La struttura tecnologica privilegiata in cui viene captato il segnale vocale è rappresentata dai centri di commutazione ([Centrali Telefoniche](#) o [MSC](#)) degli [operatori di telefonia](#), strutture presso le quali le linee telefoniche obiettivo vengono fisicamente interconnesse alle linee degli altri utenti di telefonia. Le linee captate vengono deviate [quasi sempre](#) [4] con connessioni sicure, ossia [criptate](#), verso i centri di ascolto delle [Procure della Repubblica](#) che ne fanno richiesta. Mobile Privacy definisce questo tipo di intercettazione [Intercettazioni Telefoniche Standard](#).

4.1 Praticità e Costi

Le Intercettazioni Telefoniche Standard sono il metodo più efficace, economico e sicuro per effettuare captazioni delle conversazioni nel corso di indagini legali, quando applicabile. Il [costo unitario](#) per il singolo obiettivo è calato drasticamente negli anni, parallelamente all'adozione di [sistemi informatici](#) [5] sempre più performanti (nel 2003 il [costo giornaliero](#) [6] singola linea intercettata era di circa 25 euro, ridotti ulteriormente negli anni successivi). Questo grazie alla rimozione di regimi di monopolio ed alle politiche di standardizzazione dei sistemi per le intercettazioni legali ([Lawful Interception](#) [7]), introdotte dall'[ETSI](#) sulla spinta dell'industria delle telecomunicazioni.

Una richiesta di intercettazione di una numerazione segue ormai un flusso operativo standard ed il costo giornaliero è di poche decine di euro, da paragonare alle migliaia di euro necessari per un'intercettazione ambientale. Questa infatti prevede, evidentemente, l'installazione di un dispositivo di ascolto in un ambiente estraneo da parte di [agenzie specializzate](#) [8], agli ordini della [Polizia Giudiziaria](#).

5 Tecniche di Intercettazione e Loro Impiego

Tutti i tipi di intercettazione citati, telefoniche, ambientali ed informatiche, possono essere realizzati impiegando varie tecniche, con diversità di costi, accessibilità e complessità. La tecnica impiegata varia prevalentemente in funzione di quattro variabili - (1) il tipo di soggetto che esegue le intercettazioni, (2) la presenza di rischi per la segretezza delle captazioni, (3) l'adozione o meno di contromisure da parte del soggetto obiettivo e (4) l'impiego o meno di un particolare media per le comunicazioni da parte dell'obiettivo.

5.1 Soggetto che Esegue le Intercettazioni

Le Forze di Polizia hanno accesso immediato e [regolamentato giuridicamente](#) alle strutture tecniche ed organizzative predisposte [per legge](#) [9] dagli operatori di telefonia, mentre le agenzie investigative private o anche le istituzioni straniere, ad esempio le agenzie di intelligence di altri stati, [non possono averlo](#) [10].

5.1.1 Istituzioni Private

Le agenzie investigative private, per mancanza di accesso alle strutture tecnologiche degli operatori di telefonia, fanno [quasi sempre ricorso](#) [11] alle intercettazioni ambientali.

Delle eccezioni sono rappresentate dall'impiego di [IMSI Catcher](#) [12], di [dispositivi di ascolto remoto](#) [13] installati sulle linee di telefonia fissa in prossimità degli edifici, oppure negli apparecchi telefonici e di [cellulari spia](#) [14].

Un discorso a parte merita il traffico illecito di tabulati telefonici ad opera delle agenzie investigative private. Vi sono state numerose [inchieste della Magistratura](#) [15] che lo hanno portato alla luce, ed indagini giornalistiche che riportano anche i "listini" dettagliati per ciascun operatore di telefonia, con i [prezzi necessari per ottenere](#) [16] le informazioni da operatori infedeli.

5.1.2 Istituzioni Estranee

Organizzazioni dotate di competenze e di fondi adeguati, per esempio i servizi di intelligence di paesi stranieri, possono fare ricorso a tecniche più raffinate, attaccando direttamente i centri di commutazione degli operatori di rete e manomettendo i sistemi tecnologici dedicati alle intercettazioni legali, come si ipotizza sia accaduto nel famoso caso di [Vodafone Grecia](#) [17].

5.2 Rischi per la Segretezza delle Captazioni

Vi sono un numero di situazioni particolari in cui la segretezza delle indagini della Magistratura può essere compromessa, invalidandole definitivamente, situazioni già accadute in episodi passati.

In questi ed in casi analoghi, per superare gli ostacoli tecnici e per non compromettere la segretezza delle captazioni, le Forze di Polizia ricorrono a tecniche diverse, fra cui l'impiego di [IMSI Catcher](#), oppure alle intercettazioni ambientali.

5.2.1 Funzionari Coinvolti a Titolo Professionale nelle Intercettazioni Telefoniche

Può verificarsi il caso in cui il soggetto obiettivo sia impiegato presso una struttura dedicata alla gestione delle intercettazioni degli operatori di rete, o presso il [centro di ascolto](#) [18] della Procura della Repubblica che fa richiesta di intercettazione. In tal caso la segretezza delle captazioni potrebbe essere irrimediabilmente compromessa, visto che l'obiettivo gestirebbe delle pratiche che lo riguardano.

Nel [caso Telecom](#), nel cui contesto è maturata la morte per presunto suicidio di Adamo Bove, pare che questi [abbia fornito](#) [19] supporto alla Magistratura per intercettare le linee di alcuni indagati bypassando la struttura principale dedicata allo scopo ed utilizzandone una particolare accessibile esclusivamente allo stesso Bove.

5.2.2 Funzionari Infedeli

Può accadere che vi siano operatori infedeli all'interno delle strutture organizzative che operano nei processi di intercettazione.

Un caso eclatante è venuto alla luce nelle indagini sull'attività di [spionaggio Telecom](#) [20]. Pare che la Security Telecom arrivasse ad apporre un [flag](#) su numerazioni selezionate, in modo di poterne avvisare l'utilizzatore, se nella struttura tecnica preposta un operatore avesse aggiunto il numero alla lista delle utenze intercettate a seguito di una richiesta della Magistratura.

Il consulente tecnico dell'Autorità Giudiziaria [Giacchino Genchi](#), parla esplicitamente di casi di fuga di notizie a favore di uomini politici che verrebbero [avvisati](#) di indagini in corso con l'uso di intercettazioni, da personale addetto alle strutture degli operatori telefonici.

[Angelo Iannone](#), ex capo della sicurezza Telecom Brasile, parla della [mancata rimozione](#) di un addetto Telecom impiegato presso la struttura dedicata alle intercettazioni. Pare che, nonostante fosse emerso in almeno un paio di inchieste che il soggetto fornisse informazioni ad esponenti della mafia sulle numerazioni poste sotto controllo, questi non sia mai stato rimosso dal suo incarico.

5.3 Impiego di Contromisure

L'utilizzo da parte del soggetto obiettivo di contromisure quali [numerazioni anonime GSM](#) [21], costringe gli investigatori all'impiego di altre tecniche, per esempio l'utilizzo, almeno in una fase iniziale, di dispositivi del tipo IMSI Catcher per identificare le numerazioni anonime, da sottoporre poi alla tecnica di Intercettazione Standard, se applicabile. Non vi sono ancora, al meglio della nostra conoscenza, casi di cronaca giudiziaria che evidenziano l'uso di [crittografia](#) su linee telefoniche PSTN o GSM per la tutela della segretezza delle conversazioni, da parte di obiettivi di indagine. Considerazioni sostanzialmente analoghe possono essere fatte per il [sistema americano](#) [22] delle intercettazioni legali, dove sono segnalati pochi sporadici casi.

5.4 Mancato Impiego di un Mezzo di Comunicazione

Alcuni soggetti evitano l'uso della telefonia fissa e mobile per non rischiare di essere ascoltati. Uno dei casi più famosi è quello del capo di Cosa Nostra Bernardo Provenzano, latitante per più di quaranta anni, che ha sempre impiegato i [pizzini](#) per comunicare con gli affiliati alla cosca. Per la sua cattura, sono stati quindi fondamentali attività di intelligence, [pedinamenti estenuanti](#) [23] e le intercettazioni ambientali, in particolare l'impiego di videocamere a distanza.

5.4.1 Variabili nel Mezzo di Comunicazione

Tutti i mezzi di comunicazione anche telefonici, che non vengono gestiti dai sistemi di [Intercettazione Standard](#) degli operatori di rete, pongono dei problemi alle Forze di Polizia. In questi casi vengono predisposti dei sistemi ad hoc, oppure si ricorre alle intercettazioni ambientali. Nel tempo poi, gli operatori telefonici aggiornano i loro sistemi di intercettazione - IMS - ([Interception Management System](#)) [24] per risolvere problemi particolari.

Un caso di cui si ha [notizia](#), è quello del sistema [Push To Talk](#) di TIM. Essendo una tecnologia relativamente nuova e di limitata diffusione, non è gestita dall'IMS di TIM, dunque non è intercettabile (o almeno non era) a livello di centrale di commutazione (MSC).

Anche le utenze in [Roaming](#), oppure in Roaming Internazionale, hanno causato (e probabilmente ancora oggi in alcuni casi causano), dei problemi per l'esecuzione delle intercettazioni, come evidenziato dal [Prefetto Alessandro Panza](#) nella sua audizione dinnanzi alla commissione del Senato "Indagine Conoscitiva sul Fenomeno delle Intercettazioni Telefoniche".

Per le modalità con cui vengono manualmente [inseriti i numeri](#) [25] di telefono nel database delle numerazioni deviate alle Procure della Repubblica e per gli aspetti tecnici del Roaming Internazionale, in passato vi sono stati sicuramente dei problemi in tal senso. Per esempio, nelle famose indagini sulle scalate alla Banca Antonveneta e al Corriere della Sera, [organi di stampa](#) riportano la non intercettabilità di numerazioni svizzere in Roaming Internazionale sulle reti italiane.

La situazione attuale per questo aspetto è in mutamento. Probabilmente alcuni, se non tutti gli operatori di telefonia mobile, hanno chiesto aggiornamenti ai loro sistemi IMS per potere intercettare anche le numerazioni in Roaming Internazionale. Vodafone Italia, attraverso il proprio Amministratore Delegato [Pietro Guindani](#), dichiara davanti alla

commissione del Senato "Indagine Conoscitiva sul Fenomeno delle Intercettazioni Telefoniche" che la propria azienda è in grado di intercettare anche questo tipo di numerazioni.

L'impiego di [GSM Box](#), combinato all'instradamento delle chiamate fisso-mobile su protocollo IP [per una parte del percorso](#), è diffuso in tutto il mondo. Questo ha causato e può causare gravi difficoltà per la localizzazione delle chiamate in partenza. In un caso di omicidio, studiato da Gioacchino Genchi, non è stato possibile risalire al mandante nonostante fosse disponibile l'elenco delle [chiamate](#) ricevute dal killer.

5.5 Contromisure

In generale le contromisure per mettere in sicurezza le proprie telecomunicazioni sono due, la *Cifratura* e l'*Anonimato*. Quando possibile, meglio ancora, una combinazione delle due.

Per effettuare chiamate fortemente sicure si può ricorrere, per esempio, a dei cellulari GSM con software di cifratura di un produttore affidabile, impiegando contestualmente delle numerazioni anonime. Questa soluzione comporta l'utilizzo di terminali dotati dello stesso software da parte dei due o più interlocutori.

Nel caso in cui si vogliono mettere in sicurezza le chiamate effettuate verso utenti dotati di normali telefoni fissi o mobili, si può far leva esclusivamente sull'anonimato del chiamante, dando per scontato che il destinatario della chiamata può essere obiettivo di intercettazioni. Un'ulteriore contromisura per rafforzare l'anonimato è rappresentata dalla modifica della voce del chiamante, realizzabile con appositi dispositivi elettronici.

Vi sono poi altri importanti aspetti relativi alla sicurezza per entrambi i casi considerati. Questi si possono riassumere nelle definizioni di *Contatti* (chi chiama chi, quando, con che frequenza, con che durata, ecc.) e *Localizzazione* (i luoghi da cui sono originate e verso cui sono dirette le chiamate).

Anche per mettere in sicurezza questi due importanti aspetti vi sono delle contromisure, come l'impiego di particolari reti progettate per la gestione della sicurezza e l'utilizzo di telefoni satellitari specifici.

Per mettere in sicurezza le telecomunicazioni non sono raccomandabili metodi che fanno affidamento sull'impossibilità di intercettazione per l'arretratezza temporanea dei sistemi disponibili. L'esperienza insegna che il panorama tecnologico cambia con rapidità e la disponibilità di informazioni aggiornate non è mai quella necessaria.

E' invece possibile ricorrere a dei [Sistemi di Sicurezza Anti Intercettazioni](#) che coprono tutti gli aspetti sopra discussi ed altri ancora. Nella sicurezza in generale, ed allo stesso modo in quella delle telecomunicazioni, sono i dettagli che fanno la differenza. La sicurezza ha più a che fare con ciò che non bisogna fare piuttosto con quello che si può fare.

6 Intercettazioni Ambientali

In tutti i casi sopracitati può rendersi necessario il ricorso a metodi di intercettazione diversi dall'Intercettazione Telefonica Standard. Il metodo privilegiato da Forze di Polizia, agenzie investigative private, organizzazioni, privati e criminali è senza dubbio quello delle intercettazioni ambientali.

6.1 Tecniche

Nella quasi totalità dei casi è prevista l'intrusione in un ambiente frequentato (o un ambiente in prossimità) dall'obiettivo. A volte può essere estremamente difficile realizzare le captazioni, specie quando gli obiettivi sono appartenenti alla criminalità organizzata.

Fra i casi aneddotici, quello narrato da Pietro Grasso, procuratore nazionale antimafia. Nella sua [audizione](#) dinnanzi alla commissione del Senato "Indagine Conoscitiva sul Fenomeno delle Intercettazioni Telefoniche" riporta di un caso in cui gli investigatori hanno applicato delle microspie ad un albero nel bel mezzo di un campo. L'operazione si era resa necessaria perché gli indagati, per evitare le microspie che sospettavano piazzate nei loro ambienti, si recavano all'aperto in un campo per potere conversare al sicuro.

Le intercettazioni ambientali sono realizzate in una moltitudine di modi, impiegando le più svariate tecnologie. Prevalentemente vengono utilizzati [microspie](#), microregistratori, microfoni direzionali, videocamere, microcamere, tracciamento GPS, ecc.

6.2 Contromisure

La sorveglianza elettronica può essere contrastata con un numero di contromisure, che sono all'origine all'industria della controspionaggio elettronica, o TSCM ([Technical Surveillance Counter-Measures](#) [26]).

Fondamentalmente per ciascun metodo o tecnologia di Sorveglianza, esiste ed è applicabile il relativo metodo di Controspionaggio. La difficoltà risiede nell'applicare tutte le innumerevoli contromisure disponibili per gli altrettanti modi di attacco.

Il Dipartimento della Difesa degli Stati Uniti definisce un'analisi TSCM (una bonifica ambientale) come: "Un servizio fornito da personale qualificato, per rilevare la presenza di dispositivi tecnologici di sorveglianza e pericoli, e per identificare punti deboli che potrebbero facilitare la penetrazione tecnologica degli ambienti esaminati. Una bonifica ambientale consiste in una valutazione professionale della sicurezza tecnica degli ambienti esaminati e normalmente avviene con ispezione visiva, elettronica e fisica all'interno ed in prossimità dell'ambiente in esame".

Per una prima rapida e semplice auto analisi nel caso di sospetti di intercettazioni ambientali, è disponibile una [Check List](#) di controllo.

Sul mercato esistono diverse società che forniscono [prodotti](#) e [servizi](#) per la sorveglianza e la controspionaggio.

7 Intercettazioni Informatiche

Le telecomunicazioni, a causa dell'evoluzione tecnologica e della riduzione dei costi correlata, stanno progressivamente migrando verso la tecnologia [VoIP](#) - Voice Over Internet Protocol, letteralmente voce su protocollo Internet. Le telecomunicazioni voce sempre di più transitano sulla rete Internet anziché sulle reti telefoniche.

Dal punto di vista concettuale, non vi sono grandi differenze fra le intercettazioni di conversazioni telefoniche tradizionali e conversazioni VoIP. In Entrambi i casi, la captazione può avvenire sia in prossimità dell'obiettivo, sia presso i centri di commutazione degli operatori telefonici (che forniscono anche accesso alla rete Internet) e presso le strutture tecnologiche di semplici fornitori di accesso Internet ([Service Provider](#)).

Nella pratica, al momento le Forze di Polizia realizzano le intercettazioni con una combinazione di accessi presso i vari punti della rete Internet.

7.1 Tecniche di Intercettazione e Loro Impiego

Gli operatori di rete mobile e di rete fissa offrono la deviazione dei flussi di dati (contrapposti alla deviazione delle linee voce) ai server delle Procure della Repubblica, come per esempio dichiarato dall'Amministratore Delegato di Vodafone Italia [Pietro Guindani](#).

A livello internazionale vi è la tendenza ad andare nella direzione di applicare anche alle comunicazioni VoIP la captazione presso i centri di commutazione dei vari operatori. L'[ETSI](#), organizzazione che gestisce lo standard GSM, raccomanda agli operatori uno [standard](#) in proposito.

Le tecnologie VoIP hanno però introdotto ulteriori variabili che complicano le operazioni di intercettazione e di Analisi del Traffico, se raffrontate alle tecnologie telefoniche tradizionali.

7.1.1 Cifratura

Il programma software per chiamate VoIP più diffuso al mondo è [Skype](#). Da un PC, ma anche da un telefono cellulare, consente di fare chiamate verso altri PC e cellulari dotati di Skype. Inoltre consente di fare chiamate anche verso numerazioni di rete fissa (PSTN) e mobile (GSM, UMTS). In questo caso si parla di chiamate [SkypeOut](#).

Il programma è stato sviluppato da [informatici estoni](#) cresciuti sotto il governo sovietico, che davano per scontato che qualcuno ascoltasse le conversazioni telefoniche. Per questo, come parte del pacchetto software, hanno inserito l'algoritmo [AES](#), quanto di più avanzato e sicuro disponibile pubblicamente in fatto di cifratura.

Ad oggi, l'algoritmo AES, standard adottato dal Governo degli Stati Uniti, non è violabile. Probabilmente non lo sarà per un ventennio. Quando le Forze di Polizia si imbattono in indagati che conversano con due PC utilizzando Skype, non riescono ad ascoltare le conversazioni pur intercettando (ricevendo in copia dall'operatore telefonico o fornitore di accesso) il flusso di dati, che [risulta incomprensibile](#) [27].

Per ovviare a questo ostacolo, si è ricorsi ad un altro modello di attacco, che non prevede più l'assistenza tecnologica degli operatori che forniscono accesso alla rete. Il modello è applicabile non solo a Skype, ma a tutti i software VoIP che fanno uso di algoritmi di cifratura, come per esempio un client VoIP con [protocollo SIP](#) che utilizzi [Zfone di Philip Zimmermann](#).

7.1.2 Modello di Attacco alle Conversazioni Skype

Il punto debole dei software VoIP cifrati è il sistema operativo del computer o telefono cellulare su cui sono installati. Questo è un problema che non solo non troverà soluzione, ma è [destinato a peggiorare](#) [28] con l'aumento della complessità dei sistemi operativi.

Per esempio è possibile introdurre un software di tipo Trojan in un PC con sistema operativo Windows non rilevabile dai programmi antivirus commerciali.

Il modello di attacco messo a punto dalle [forze di polizia europee](#) [29] è progettato proprio in questo modo. [Progettisti software](#) [30] scrivono dei codici di tipo Trojan che possono essere installati sia con accesso fisico al computer obiettivo (intrusione nei locali come per il piazzamento di microspie ambientali) oppure in modalità remota, per esempio con l'invio in allegato ad una e-mail (per un caso di furto di dati è stata attaccata in questo modo la rete del [Corriere della Sera](#), dal [Tiger Team Telecom](#)).

Una volta installato, il software spia si occupa di captare la voce dell'utilizzatore del computer su cui è installato prima che venga cifrata dall' algoritmo AES e quella dell'interlocutore dopo che è stata decifrata. Il software verosimilmente agisce fra la scheda audio del computer ed il software VoIP, captando le conversazioni digitalizzate ma in chiaro. Una copia della conversazione può così essere inviata presso la destinazione desiderata.

7.1.3 Internazionalizzazione Interconnessioni e Localizzazione Chiamate

Skype, ma anche altri tipi di servizi VoIP, offrono la possibilità di fare chiamate verso le normali reti fisse e mobili. Questo significa che una chiamata partita da un PC ed instradata sulla rete Internet, in un certo punto deve essere deviata sulla rete fissa o mobile. Questo punto, nella maggior parte dei casi, fisicamente [si trova nel territorio](#) in cui risiede la numerazione cui è destinata la chiamata.

Per esempio, se un PC italiano effettua una chiamata SkypeOut su una numerazione americana di rete fissa, il dispositivo di instradamento della chiamata dalla rete Internet alla rete fissa si troverà quasi certamente sul territorio americano. Questo perchè il fornitore di accesso alla rete fissa che si trova negli USA può acquistare una chiamata di tipo urbano, al più basso costo possibile. Vengono così evitati i costi delle chiamate internazionali, ragione per cui il VoIP è tanto conveniente per questo tipo di telecomunicazioni.

A volte però le cose possono complicarsi ulteriormente. Skype può decidere di acquistare il traffico da un rivenditore qualunque, con una struttura tecnologica residente in un paese qualsiasi. La stessa chiamata SkypeOut diretta verso gli USA può per esempio essere acquistata da un rivenditore in Inghilterra, il quale la ridirezionerà sempre attraverso la rete Internet, verso gli USA. Negli USA la chiamata verrà instradata dalla rete Internet alla rete fissa, come nel caso precedente.

Se non vengono messe in atto strategie particolari dal fornitore di servizi VoIP, in questo caso Skype, l'elemento che determina l'identità della chiamata in partenza è [l'indirizzo IP](#). Il rivenditore inglese però, per ragioni tecniche e commerciali, può cambiare l'indirizzo IP del chiamante, assegnandone uno nuovo. Il fornitore di accesso americano vedrà un indirizzo IP diverso da quello del PC da cui è partita la chiamata in origine, e la correlazione fra i due indirizzi IP sarà conosciuta solo al rivenditore inglese.

Nel caso [Roveraro](#), verosimilmente è accaduta una cosa simile. I rapitori del finanziere utilizzavano Skype per effettuare chiamate SkypeOut, le quali per loro natura non portano l'identificativo del chiamante. Non solo, ma le chiamate SkypeOut, pur partendo dall'Italia dirette verso un numero di rete fissa o mobile italiana, transitavano per una struttura tecnologica di [interconnessione australiana](#).

Gli investigatori hanno rilevato chiamate anonime per la richiesta del riscatto ed anche il fornitore di accesso alla rete fissa o mobile di casa Roveraro, non è stato in grado di indicare l'indirizzo IP del PC da cui sono state effettuate le chiamate. Secondo le notizie di stampa, gli investigatori hanno dovuto rivolgersi direttamente ad E-Bay, proprietaria di Skype, per chiedere collaborazione.

L'esplosione nel numero di fornitori di servizi VoIP non farà che peggiorare questo tipo di problema. Nel caso in cui il fornitore di servizi sia una piccola o media società residente in uno stato con cui l'Italia non ha un accordo bilaterale in materia di assistenza giudiziaria, potrebbe essere impossibile per le Forze di Polizia localizzare il luogo di partenza delle chiamate, oppure semplicemente, farlo con ritardo rispetto alle esigenze delle indagini.

7.2 Contromisure

Per mettere in sicurezza le comunicazioni VoIP valgono gli stessi principi fondamentali considerati per le comunicazioni telefoniche. La cifratura delle conversazioni va sempre utilizzata e non è difficile farlo. E' sufficiente utilizzare Skype, oppure, per coloro che giustamente diffidano della sua sicurezza, per esempio utilizzare un [qualsiasi client VoIP](#) che faccia uso del protocollo SIP ed integrarlo con [Zfone](#) di Philip Zimmermann.

L'anonimato assume un ruolo ben più importante nelle comunicazioni informatiche rispetto a quelle telefoniche. E' l'unica contromisura efficace rispetto al modello di attacco che prevede l'installazione di software di tipo Trojan capaci di aggirare la cifratura delle comunicazioni, modello non applicabile alle normali comunicazioni telefoniche. Fino a che l'indirizzo IP dell'obiettivo è sconosciuto, non è evidentemente possibile installare in modalità remota un software spia.

La messa in sicurezza dei Contatti (chi chiama chi, quando, con che frequenza, con che durata) è fortemente dipendente dall'anonimato, visto che per una qualsiasi conversazione VoIP, vi sono comunque una moltitudine di dispositivi intermedi lungo la rete Internet che registrano in file di log un numero di dati.

Per la Localizzazione (i luoghi da cui sono originate e verso cui sono dirette le chiamate) è possibile ricorrere alle stesse contromisure descritte per le intercettazioni telefoniche, prevalentemente a connessioni di tipo satellitare che, per loro natura, sono difficili da localizzare con precisione utile.

Conclusioni

La letteratura e la conoscenza sviluppate negli USA, prevalentemente in ambito militare, consentono di definire e classificare secondo schemi esistenti le intercettazioni telefoniche, ambientali ed informatiche.

La tecnica di intercettazione privilegiata dalle Forze di Polizia è quella telefonica, che prevede l'assistenza diretta degli operatori di telefonia. Nel mondo delle intercettazioni legali, esistono però un numero impensato di casi di fuga di notizie, generalmente a vantaggio di politici, funzionari e criminali. Questa ed altre ragioni, spingono spesso gli investigatori ad utilizzare altre tecniche, fra cui le intercettazioni ambientali.

Le intercettazioni ambientali sono anche il mezzo preferito dalle agenzie investigative private per raccogliere informazioni sulle conversazioni dei loro obiettivi. Solo in alcuni specifici casi, è possibile per le agenzie realizzare delle intercettazioni telefoniche.

Le intercettazioni informatiche, rese difficili dalla diffusione di Skype, il client VoIP più popolare al mondo, sono ora alla portata delle Forze di Polizia e, in tempi brevi, lo saranno anche per gli hacker.

Per individui ed enti che operano nella legalità, vi sono una serie di valide ragioni per difendere le proprie comunicazioni da attacchi esterni. Fra queste, il traffico illecito di tabulati telefonici e le intercettazioni illegali. Allo scopo, sono disponibili una serie di contromisure da integrare in Sistemi di Sicurezza. Una sola contromisura generalmente mal si adatta a situazioni di rischio, ed è quindi necessario disporre il giusto mix di contromisure.

Note

[1] DoD - Dizionario dei Termini Militari e Similari.

Vedere il dizionario del Dipartimento della Difesa degli Stati Uniti d'America per i termini militari ed i termini associati.

http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

[2] Analisi dei Tabulati Telefonici.

L'analisi dei dati accessori delle telecomunicazioni, in particolare quelle GSM, è una fonte di informazioni preziosa, per esempio per l'analisi forense, ma anche per indagini illegali. Nel documento (in lingua inglese), una presentazione per un corso di Analisi Forense delle telecomunicazioni GSM del professor K. C. Hilton dell'Università dello Staffordshire, nel Regno Unito.

http://www.mobileprivacy.net/PDF/GSM_Forensics.pdf

[3] Dati Ministero Giustizia Numero Intercettazioni e Costi.

In questo documento, i dati ufficiali del Ministero della Giustizia per gli anni 2003 - 2006 relativamente ai bersagli di intercettazioni. Sono dettagliati i numeri di ciascuna Procura della Repubblica, per tipo di intercettazione - se ambientale, telefonica o di altro tipo (presumibilmente informatica) ed i costi relativi.

http://www.mobileprivacy.net/PDF/Intercettazioni_Dati_Aggregati_Ministero_Giustizia.pdf

[4] Sicurezza del Sistema delle Intercettazioni Legali.

Al meglio della nostra conoscenza, non sono disponibili documenti pubblici di analisi o illustrazione dei sistemi di sicurezza impiegati in questo delicato settore. Vi sono però alcuni episodi noti tutt'altro che rassicuranti, uno dei quali è descritto dal Garante per la Privacy. Questi ha imposto lo stop ad un operatore telefonico per quanto riguarda le comunicazioni dei dati accessori di chiamate intercettate, perché forniti in chiaro per via telematica, senza che fossero cifrati (criptati).

<http://www.garanteprivacy.it/garante/doc.jsp?ID=1408286>

[5] Interception Management System.

Le modalità tecniche con cui vengono effettuate le Intercettazioni Standard GSM sono fondamentalmente le stesse per i quattro operatori. Questo perché è lo standard GSM che detta le linee guida dell'architettura del sistema di intercettazione e soprattutto perché le reti GSM sono state storicamente costruite da poche grandi aziende fra cui Nokia, Siemens, Ericsson, ecc.

Il sistema di gestione delle intercettazioni che utilizzano gli Operatori di Rete tipicamente è una parte accessoria acquistata separatamente rispetto alle altre infrastrutture.

Nel tempo sono filtrati documenti riservati che descrivono l'architettura del Sistema di Intercettazione Standard Ericsson e dei corsi di formazione per gli operatori che lo utilizzano in modalità remota, da una sede centralizzata dell'operatore telefonico.

http://www.mobileprivacy.net/PDF/Interception_Management_System.pdf

[6] Costo delle Intercettazioni Legali

Il costo giornaliero per ogni singola linea telefonica deviata ad una Procura della Repubblica è riportato nel documento conclusivo del Senato "Indagine Conoscitiva sul Fenomeno delle Intercettazioni Telefoniche".

<http://www.senato.it/documenti/repository/commissioni/stenografici/15/comm02/02a-20061129p-IC-0194.pdf>

[7] Sistemi di Intercettazione Legale

Nel documento (in lingua inglese) è rappresentato lo schema generale dell'ETSI per i sistemi di intercettazione legali che fanno affidamento sui dispositivi di commutazione degli operatori di rete. Lo schema è applicabile anche alle comunicazioni VoIP.

http://en.wikipedia.org/wiki/Lawful_interception

[8] Installazione Microspie

L'installazione di una microspia per intercettazioni ambientali, legali o meno, deve essere fatta senza lasciare tracce di intrusioni. In genere, le agenzie specializzate che lavorano per conto della Polizia Giudiziaria impiegano ex ladri

professionisti, gli unici dotati delle competenze necessarie per introdursi in ambienti estranei protetti quali abitazioni, automobili, ecc.

<http://ricerca.repubblica.it/repubblica/archivio/repubblica/2004/11/17/in-auto-al-bar-al-computer-cosi.html>

[9] Intercettazioni Legali

In Italia gli operatori telefonici sono obbligati per legge a fornire i servizi necessari per eseguire le intercettazioni. Non è sempre stato così in passato e la cosa è tutt'altro che scontata. Negli Stati Uniti per esempio, solo di recente la legislazione (CALEA, Patriot Act) è stata modificata in questo senso. Prima gli investigatori dovevano dotarsi di mezzi propri.

http://www.agcom.it/L_naz/cod_comunicaz_dl259_03.htm

[10] Intercettare le Telecomunicazioni di Paesi Stranieri

Intercettare le telefonate sulle linee fisse e mobili di un paese straniero non è questione semplice, a dispetto delle suggestioni cinematografiche. In una intervista di Report (RAI Tre) ad un ex dirigente Telecom, si comprende come in definitiva, per avere facile accesso a tutte le conversazioni sulle linee fisse partenti dall'Italia verso il Medio Oriente (ed in arrivo da), i servizi segreti americani abbiano chiesto l'accesso fisico ad un centro di commutazione situato a Palermo.

http://www.mobileprivacy.net/Video_Intercettare_Le_Telecomunicazioni_Di_Un_Paese_Straniero.html

[11] Intercettazioni Ambientali Agenzie Investigative Private

Si tratta di un tema delicato, per il quale le associazioni di categoria stanno esercitando attività di *lobbying* tese ad ottenere una legislazione chiara e che consenta loro di esercitare l'attività professionale nel rispetto della legge. A volte purtroppo, la cronaca giudiziaria riporta casi di violazioni come quello descritto nell'articolo.

[12] IMSI Catcher

E' un dispositivo elettronico utilizzato dalle Forze di Polizia e probabilmente anche da agenzie investigative private dotate dei fondi necessari per l'acquisto e la gestione.

L'IMSI Catcher è in grado di ricavare l'IMSI (International Mobile Subscriber Identity Module), un numero che identifica in modo univoco un utente GSM, risiedente nella carta SIM e di intercettare le chiamate GSM.

Le specifiche GSM richiedono che il cellulare si autentichi alla rete, ma non richiedono che la rete si autentichi al cellulare. Questa falla nella sicurezza ben conosciuta è sfruttata dagli IMSI Catcher.

L'IMSI Catcher assume le sembianze di una antenna (BTS) della rete GSM, aggancia tutti i cellulari nel suo campo d'azione e ne estrae gli IMSI. E' poi in grado di forzare il cellulare obiettivo a comunicare con l'antenna in chiaro, disattivando l'uso dell'algoritmo di cifratura a standard GSM A5, normalmente impiegato in Europa.

Quindi è in grado di registrare le conversazioni. Un'applicazione molto utile è l'identificazione di numerazioni anonime eventualmente utilizzate da l'obiettivo di un'indagine, come accaduto a Giampiero Fiorani e Stefano Ricucci nelle indagini sulle scalate al Corriere della Sera ed Antonveneta.

Una volta identificate, le numerazioni anonime possono essere comodamente intercettate con il metodo standard da una sala d'ascolto di una Procura della Repubblica.

http://en.wikipedia.org/wiki/IMSI_catcher

[13] Intercettazione Linee Telefonia Fissa

Le linee di telefonia fissa possono essere intercettate installando un numero di dispositivi con differenti tecnologie. Alcune prevedono l'accesso diretto all'apparecchio telefonico, altre solo ai cavi in prossimità dell'edificio in cui si trova il telefono obiettivo. Quanto possa essere semplice installare dei dispositivi per intercettare le chiamate su una linea fissa, è stato evidenziato da diverse inchieste giornalistiche, fra cui Le Iene (Mediaset) e Report (RAI), cui si riferisce il filmato del collegamento.

http://www.mobileprivacy.net/Video_Intercettare_Telefoni_Fissi_Internet_ADSL.html

[14] Spy Phone

E' possibile trasformare qualunque telefono GSM in un dispositivo spia, con un intervento hardware oppure software. Fra le funzioni implementabili vi sono: Ascolto Ambientale; Inoltro SMS Inviati/Ricevuti; Inoltro Lista Chiamate; Intercettazione Chiamate; Localizzazione del Cellulare.

http://www.spiare.com/software_spyphone.html

[15] Traffico Tabulati Telefonici

Alcune importanti e delicate inchieste della Magistratura (Laziogate, RADAR Telecom, ecc.), hanno evidenziato il fenomeno della vendita di tabulati telefonici, da parte di operatori infedeli dipendenti di Operatori di Rete, o loro società fornitrici di servizi in *Outsourcing*. Nell'articolo de L'Espresso è riportato anche il tariffario in uso in quel periodo.

<http://espresso.repubblica.it/dettaglio/Self-service-Telecom/1303687>

[16] Traffico Tabulati Telefonici

Un'inchiesta del Sole24Ore evidenzia come dopo un periodo di "calma" relativa seguito alle indagini degli anni 2005-2007, il traffico di informazioni dagli Operatori di Rete sia ripreso a pieno ritmo.

<http://www.ilsole24ore.com/art/SoleOnLine4/Economia%20e%20Lavoro/2008/03/call-center-ladri-tariffario.shtml?uuid=d4566fc0-f40e-11dc-8cf7-00000e25108c&DocRulesView=Libero>

[17] Caso Vodafone Grecia

Nell'illustrazione riportata dal collegamento, lo schema di attacco impiegato da un ente non identificato, verosimilmente la CIA, oppure un'agenzia equivalente, per intercettare illegalmente il Primo Ministro greco e circa cento personalità politiche ed economiche di primissimo piano. L'attacco è stato portato penetrando fisicamente quattro MSC (Centri di Commutazione) di Vodafone Grecia, nei dintorni di Atene. E' stato installato un software spia che ha fatto uso del modulo IMS - Interception Management System, un componente Ericsson destinato alle intercettazioni legali, al momento non utilizzato dall'operatore di rete. Visto l'alto contenuto tecnologico dell'attacco, è ovvio pensare ad una organizzazione adeguatamente finanziata per poterlo realizzare.

http://www.mobileprivacy.net/Immagini/Intercettazioni_Linea_RES.jpg

[18] Intercettazione Funzionari Addetti alle Intercettazioni

Può capitare, ed è quanto accaduto al responsabile della centrale di ascolto della Procura della Repubblica di Roma, Nicola Frugis Caggianelli. Una stima fatta da Mobile Privacy conta almeno 5.000 persone che ogni giorno, in Italia, maneggiano delle registrazioni di intercettazioni acquisite legalmente.

<http://www.ilgiornale.it/a.pic1?ID=269780&START=0&2col=>

[19] Intercettazione Funzionari Addetti alle Intercettazioni

E' capitato anche nelle indagini sulla sequestro Abu Omar. Nell'articolo, una descrizione di come Adamo Bove, funzionario Telecom ed ex poliziotto morto in circostanze misteriose, abbia aiutato i magistrati per superare questo ostacolo. E' interessante notare che sia le linee guida ETSI che le legislazioni di alcuni paesi, prevedono che il processo di intercettazione sia completamente trasparente per l'operatore telefonico. Questo non accade in Italia, aumentando così il numero di persone coinvolte nei processi ed il rischio di eventuali fughe di notizie.

http://www.corriere.it/Primo_Piano/Cronache/2006/07_Luglio/23/biondani.html

[20] Intercettazione Funzionari Addetti alle Intercettazioni

In questo video Milena Gabanelli di Report (RAI 3) spiega, con il supporto di trascrizioni di intercettazioni disposte dalla Magistratura, come è emerso che la Sicurezza Telecom avesse organizzato un sistema anti intercettazione per alcune particolari utenze.

http://www.mobileprivacy.net/Video_Intercettazioni_Segretezza_Delle_Operazioni_01.html

[21] Identificare una Numerazione Anonima GSM

Le Forze di Polizia ricorrono anche a tecniche di attacco tecnologico per identificare le eventuali numerazioni anonime in uso all'obiettivo, quando l'economia dell'indagine lo giustifica.

Nell'articolo viene descritto (anche se probabilmente sono presenti diversi errori in merito alle caratteristiche dei dispositivi tecnologici) l'impiego di un dispositivo del tipo IMSI Catcher per identificare prima le numerazioni in uso al banchiere Giampiero Fiorani e poi quelle dell'immobiliarista Stefano Ricucci.

http://www.mobileprivacy.net/PDF/Articolo_Ricucci.pdf

[22] Intercettazioni e Crittografia

Whitfield Diffie e Susan Landau nel loro libro "Privacy on the Line" citando i dati ufficiali del governo degli Stati Uniti, riportano di pochi isolati casi in cui gli investigatori hanno incontrato un ostacolo alle intercettazioni in telecomunicazioni criptate.

<http://books.google.it/books?id=nMY8yHaTQI4C&printsec=frontcover&dq=privacy+on+the+line&sig=ACfU3U0Yfa18ylb2oJHyQqOvpQ1F7dZNnQ#PPA215,M1>

[23] Intercettazioni Ambientali in Pratica

Nel documentario-fiction della RAI "Scacco al Re" è raccontato, anche dagli stessi protagonisti, il lavoro estenuante necessario per la cattura del capo di Cosa Nostra Bernardo Provenzano. Nell'immaginario collettivo gli investigatori raggiungono i loro obiettivi impiegando tecnologie sofisticate, ma non è esattamente così. Le tecnologie vengono effettivamente utilizzate - intercettazioni ambientali, telefoniche, riprese visive. Nella realtà però sono le competenze e la capacità di abnegazione degli uomini sul campo, che fanno la differenza, come sempre.

<http://www.rai.tv/mpprogramma/0,,RaiTre-Cronistidistrada%5E23%5E26005%5Et-1,00.html>

[24] Interception Management System

Nel documento del collegamento è illustrato il sistema di intercettazione Ericsson, impiegato da diversi operatori telefonici. Classificato dalla Ericsson come "Strettamente Confidenziale", in qualche modo è filtrato all'esterno.

http://www.mobileprivacy.net/PDF/Interception_Management_System.pdf

[25] Interception Management System

Nel collegamento il Manuale d'Uso impiegato dagli addetti alle intercettazioni presso gli operatori telefonici, per apprendere l'uso delle varie funzioni.

http://www.mobileprivacy.net/PDF/Interception_Management_System_01.pdf

[26] TSCM - Technical Surveillance Counter Measures.

Abbreviazione utilizzata in ambito militare USA per indicare i processi di Bonifica Ambientale e le tecniche di Controsorveglianza attraverso l'uso di dispositivi elettronici.

<http://en.wikipedia.org/wiki/TSCM>

[27] Intercettazioni Skype

Come testimoniato dal Prefetto Alessandro Panza dinnanzi alla commissione del Senato "Indagine Conoscitiva sul Fenomeno delle Intercettazioni Telefoniche", intercettare il flusso dati di una comunicazione Skype è inutile, perché i dati digitali sono cifrati con l'algoritmo AES. Vi sono però altri metodi per ottenere l'audio in chiaro.

<http://www.senato.it/documenti/repository/commissioni/stenografici/15/comm02/02a-20060720a-IC-0053.pdf>

[28] Sicurezza Sistemi Operativi

I sistemi operativi moderni Windows, Linux, ma anche Symbian e Windows Mobile sono e saranno affetti da falle nella sicurezza. L'argomento è trattato, fra gli altri, da Bruce Schneier nel libro "Secret and Lies" e da Ross Anderson in "Security Engineering".

<http://books.google.it/books?id=eNhQAAAAMAAJ&q=secret+and+lies+schneier&dq=secret+and+lies+schneier&pgis=1>

[29] Intercettazioni Skype

Come evidenziato da un famoso documento della polizia tedesca filtrato su Wikileaks.

http://wikileaks.org/wiki/Skype_and_the_Bavarian_trojan_in_the_middle

[30] Intercettazioni Skype

In questa intervista, David Vincenzetti parla di un software messo a punto dalla società Milanese Hacking Team e destinato alle Forze di Polizia per intercettare conversazioni Skype.

http://www.mobileprivacy.net/PDF/Intercettare_Skype.pdf

Mobile Privacy LTD

Unit 150, Imperial Court,
Exchange Street East, Liverpool,
L2 3AB, UK
Tel: +44 161 4084963
e-mail: info@mobileprivacy.net
Web: www.mobileprivacy.net

Copyright © 2008 Mobile Privacy. Tutti i diritti riservati. Mobile Privacy è un marchio registrato di Mobile Privacy LTD. Altri prodotti o marchi qui menzionati possono essere marchi registrati dei rispettivi proprietari.