Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Triennale in Matematica

LA CRITTOGRAFIA NEL SISTEMA SKYPE

Tesi di Laurea in Algoritmi della Teoria dei Numeri e Crittografia

Relatore:
Chiar.mo Prof.
DAVIDE ALIFFI

Presentata da:
ELENA SGUBBI

Sessione II
Anno Accademico 2011 - 2012

Indice

Introduzione

Nascita di Skype

Nell'ultimo decennio si è registrato un notevole incremento della tecnologia VoIP, Voice over Internet Protocol, ovvero di quella tecnologia che permette la comunicazione telefonica sfruttando una connessione Internet.
Skype è la tecnologia VoIP più conosciuta e utilizzata al mondo. In una riga la possiamo definire come un software VoIP proprietario e freeware basato su un network peer-to-peer. Skype è stato fondato nel 2003 dagli estoni Ahti Heinla, Priit Kasesalu, Jaan Tallin, dal danese Janus Friis e dallo svedese Niklas Zennström, i padri del software peer-to-peer di file sharing Kazaa. Precisamente nell'aprile 2003 vennero registrati i domini "skype.com" e "skype.net", mentre nell'agosto dello stesso anno venne rilasciata la prima versione del software. La sede legale di Skype si trova a Lussemburgo mentre la sede operativa è dislocata in varie città: Londra, Stoccolma, Praga, Tallin e Tartu in Estonia, e Palo Alto in California.

Già nel 2005 Skype registra un tale successo da attirare su di sé l'attenzione di giganti del settore, come e-Bay che nel Settembre dello stesso anno acquista la società Skype per 2,6 miliardi di dollari.
Tuttavia viene a crearsi una rottura tra i fondatori di Skype e i nuovi titolari, che, alla fine del 2007, porta i fondatori Niklas e Janus a lasciare la società. Questa rottura causa un forte rallentamento nell'azienda, sia nell'ambito della crescita, sia nello sviluppo produttivo. Questo periodo di transizione viene gestito da Michael van Swaaij, nominato Interim CEO [1].
Nel febbraio 2008 Skype elegge Josh Silverman come nuovo CEO, che rimarrà in carica per due anni e mezzo fino all'acquisizione da parte di Microsoft. Sotto la sua guida, Skype rilancia la sua produzione con nuovi software e aggiornamenti. In particolare la società si incentra sul miglioramento delle video-chiamate ma soprattutto punta a conquistare il mercato dei cellulari. Nel 2009 Skype lancia una nuova applicazione per iPhone che in

[1] L'acronimo CEO indica "Chief Executive Officer" ovvero l'Amministratore Delegato, mentre "Interim CEO" rappresenta una nomina di transizione.

appena due giorni supera 1 milione di download, e si prepara a lanciare un nuovo software per piattaforme Android.
Anche la campagna pubblicitaria lanciata da Skype è innovativa ed efficace. Silverman infatti ottiene l'appoggio di alcune importanti trasmissioni televisive, così, eventi come "The Oprah Winfrey Show" o quiz come "Who Wants To Be a Millionaire" utilizzano Skype per mettere in collegamento audio-video i concorrenti in studio con i telespettatori a casa. Queste nuove scelte, sia produttive che di marketing, fanno sì che per Skype cominci una nuova fase di crescita.
Il 2 settembre 2009 e-Bay vende il 65% della società ad un gruppo di imprenditori privati, tra cui la Index Ventures e la Silver Lake Partners, per 1,9 miliardi di dollari. Questa quota viene poi acquistata nel marzo 2011 dalla società FREE Inc.
Successivamente si apre una trattativa con Google e Facebook per l'acquisizione di Skype, ma il 10 maggio 2011 è il colosso Microsoft ad avere la meglio con l'offerta di 8,5 miliardi di dollari. Microsoft incorpora Skype nella propria società creando una specifica divisione chiamata Microsoft Skype Division. Dopo pochi mesi, in agosto, Skype acquisisce Group Me, un provider attivo con diverse applicazioni per i rispettivi smartphone, sottolineando ancora di più il suo nuovo interesse per i telefoni cellulari.

Il successo di Skype è confermato anche dai dati riguardanti il numero di account registrati [1].
Dopo tre anni dalla sua nascita, nel 2006, Skype conta già 100 milioni di registrazioni che crescono esponenzialmente fino ad arrivare a 474 milioni nel 2009 e, con una crescita del 28,5%, raggiungono i 663 milioni nel 2010. Sempre nel 2010, la media di utenti connessi ogni mese è stata di 145 milioni, contro i 105 dell'anno precedente, anche la media mensile dei clienti che hanno scelto servizi Skype a pagamento è aumentata, passando dai 7,3 milioni del 2009 agli 8,8 milioni nel 2010.
Anche nel 2011 Skype ha raggiunto un nuovo record, infatti a Gennaio, con la possibilità di effettuare video-chiamate Skype su iPhone, la società ha registrato 27 milioni di utenti on-line simultaneamente, che sono cresciuti fino a 30 milioni a Marzo dello stesso anno.
La figura 1 [2] mostra graficamente il successo di questo innovativo sistema VoIP, rappresentando il numero di utenti Skype on-line simultaneamente, dalla nascita nel 2003 fino a Marzo 2012. In questo modo è possibile osservare direttamente l'effettivo utilizzo di Skype e la sua continua e rapida crescita.
Quando si considera il numero di utenti registrati bisogna precisare che, in realtà, viene contato il numero di account di tipo Skype e non il numero reale di utenti, poiché questi hanno la possibilità di creare più account Skype.
Tuttavia basta considerare il fatturato di chiamate in minuti per capire che il fenomeno è ugualmente in grande espansione. Nel 2009 sono stati effettuati 113,0 miliardi di minuti di chiamate e 194,3 miliardi di minuti nel 2010, gratuitamente, cioè di tipo Skype-to-Skype. Ma anche le chiamate a pagamento sono aumentate da 10,7 miliardi di minuti nel 2009 a 12,8 miliardi di minuti nel 2010, con un costo medio mensile di 97 dollari per ogni utente.

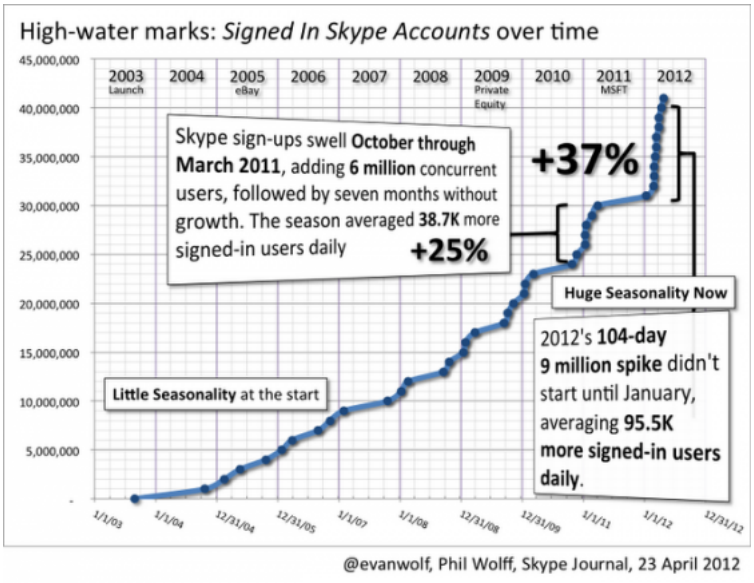

Figura 1: Utenti Skype on-line simultaneamente

I guadagni di questo colosso VoIP sono altrettanto imponenti. Nel 2009 la società ha incassato ben 718,9 milioni di dollari mentre nel 2010 Skype ha raggiunto gli 859,8 milioni di dollari.

Un numero così elevato di utenti e di accessi simultanei può creare problemi nella rete e nella sua gestione. Skype non è immune da queste problematiche.
Il primo crash della rete Skype si è verificato il 16 agosto 2007. In base alle dichiarazioni ufficiali rilasciate dalla società, il problema è stato causato da un aggiornamento dei sistemi Windows. In quel giorno, infatti, si è avuto un aggiornamento massiccio di Windows e i sistemi, dopo l'operazione, si sono automaticamente riattivati e di conseguenza hanno effettuato il login a Skype. Il numero eccessivo di login avrebbe dovuto innescare un apposito sistema di sicurezza, sviluppato per evitare sovraccarichi nei server di autenticazione, ma un errore proprio in questo sistema ha provocato un blocco della rete.
Per tale motivo questa data viene ricordata dagli utenti Skype come il "Patch Tuesday", dove il termine "patch", che letteralmente viene tradotto con "pezza", in informatica indica un file eseguibile rilasciato dai produttori del software stesso per risolvere un determinato errore di programmazione.
A questo crash ne sono seguiti altri, come quello del 22 dicembre 2010 causato da un problema nella versione 5.0.0.152 di Skype. La versione incriminata non permetteva un aggiornamento completo e automatico del software, come invece avviene normalmente nelle

altre versioni, e questo ha provocato il blocco di alcuni supernodi, elementi alla base del sistema di rete Skype. Gli addetti al lavoro hanno quindi dovuto ricostruire nuovi supernodi affinchè fosse ristabilita la situazione.
Un ultimo crash è avvenuto a maggio del 2011 dopo appena due settimane dall'acquisto di Skype da parte di Microsoft. Il blocco in questo caso è stato causato da un aggiornamento dati del sistema.

Una curiosità sul nome di questo famoso software VoIP.
In origine i fondatori avevano pensato di chiamare questo sistema "Sky peer-to-peer", poi abbreviato in "Skyper". Tuttavia alcuni domini associati al nome "Skyper" erano già occupati, quindi si pensò di sopprimere la "r" finale, ottenendo così il nome che ancora oggi lo accompagna: Skype.

Capitolo 1

I servizi di Skype

I servizi offerti agli utenti da parte di Skype sono molteplici.
Oltre all'opportunità data dal file-sharing e dalla chat, Skype deve il suo successo alle caratteristiche dei servizi telefonici offerti, che lo rendono competitivo rispetto alla telefonia tradizionale.

- Skype-to-Skype

La connessione peer-to-peer permette di comunicare via voce gratuitamente. In questo caso, sia il mittente che il destinatario devono essere collegati attraverso Internet ad un account di tipo Skype. Perciò, questa applicazione viene anche chiamata Skype-to-Skype.

- SkypeOut

SkypeOut permette invece di effettuare telefonate a pagamento verso telefoni fissi o cellulari quando il destinatario non è collegato a Skype. L'appetibilità dell'offerta è data dai costi ridotti, dovuti al fatto che la telefonata viaggia per la maggior parte attraverso Internet e solo in prossimità del destinatario i dati vengono convertiti in analogico in modo da utilizzare solo la rete telefonica locale. Quindi, per esempio, una telefonata del tipo Roma-Pechino avrà il costo di una telefonata locale e non intercontinentale.
Con questa modalità e con questo meccanismo è possibile anche inviare sms a basso costo verso tutti i cellulari.

- SkypeIn

Se SkypeOut è un servizio telefonico del tipo mittente connesso a Skype e destinatario tradizionale, SkypeIn rappresenta il servizio simmetrico, essendo orientato verso quelle telefonate con mittente "analogico" e destinatario collegato a Skype.
SkypeIn infatti permette, a basso costo, di acquistare un numero telefonico associato all'account di Skype. In questo modo il mittente può comporre tale numero tramite fisso o mobile, e la telefonata viene ricevuta sul computer che presenta l'account corrispondente, come una normale chiamata telefonica.
Con questa modalità si può anche richiedere la segreteria telefonica.
Il numero Skype si può ottenere nei seguenti Stati: Australia, Belgio, Cile, Colombia, Danimarca, Repubblica Dominicana, Estonia, Finlandia, Francia, Germania, Giappone, Hong Kong, Irlanda, Italia, Messico, Nuova Zelanda, Olanda, Polonia, Regno Unito, Romania, Stati Uniti, Sud Africa, Sud Corea, Svezia, Svizzera, Turchia e Uruguay.

- Video-chiamate

Nel gennaio 2006 è stata introdotta la possibilità di effettuare video-chiamate attraverso una webcam, prima su piattaforme Windows e Mac, successivamente, dal 2008 è stato possibile anche per sistemi Linux.
Attualmente le chiamate audio supportano fino a 25 utenti contemporaneamente, mentre le video-chiamate fino a 5 utenti.

Al momento però, Skype non può sopperire totalmente al telefono fisso o mobile in quanto non è abilitato ad effettuare le chiamate d'emergenza.

Capitolo 2

La rete Skype

Ciò che rende innovativo il prodotto Skype è la combinazione di un sistema di tipo VoIP all'interno di una rete peer-to-peer. Questa caratteristica voleva essere evidenziata anche nel nome della società che in origine, come già accennato, doveva chiamarsi "Sky peer-to-peer" ma che per varie vicissitudini è diventata "Skype".
Una rete peer-to-peer è un network di tipo overlay, cioè "una rete sopra un'altra rete"; infatti il peer-to-peer è costituito da un insieme di nodi connessi tra loro attraverso link virtuali (e questo forma una rete) all'interno del sistema Internet (un'altra rete).

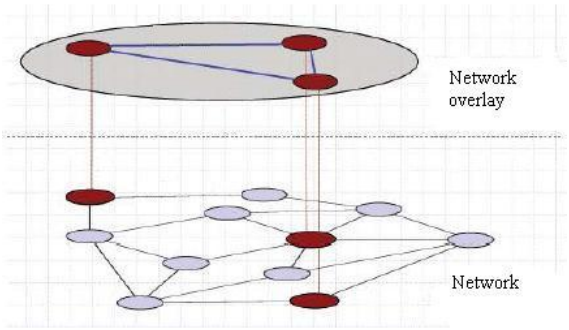

Figura 2.1: Struttura di un network overlay

Una delle operazioni più importanti in una rete peer-to-peer è il lookup delle risorse, ovvero il modo in cui vengono localizzate le risorse sulla rete. I primi sistemi peer-to-peer utilizzavano un lookup centralizzato basato su nodi fissi e il risultato era analogo ad una struttura dall'approccio di tipo client-server. Questa scelta però non era ottimale, le risorse spesso non fluivano bene andando a generare ingorghi. Inoltre un approccio centralizzato causava fragilità nell'infrastruttura. Si sviluppa così un nuovo modello decentralizzato, caratterizzato dalla mancanza di un lookup centrale, dove le informazioni vengono distribuite

sui nodi. Questo sistema permette una maggiore scalabilità ma ha come difetto l'aumento della complessità della rete. Il lookup decentralizzato può essere a sua volta di due tipi: strutturato e non strutturato. In una rete decentralizzata ma strutturata i peer si organizzano seguendo una topologia precisa con la presenza di una directory service distribuita, mentre un approccio non strutturato è caratterizzato dall'assenza di controllo sulla topologia della rete e dalla mancanza di una directory service.
Skype utilizza un network peer-to-peer decentralizzato e non strutturato.

2.1 Struttura della rete peer-to-peer

La rete si sviluppa su due livelli, questo perché sono presenti due tipi di nodi:
il nodo ordinario e il supernodo.
I *nodi ordinari*, o ordinary host, sono terminali della rete che ospitano programmi a livello applicativo, per questo in inglese vengono definiti host ovvero ospiti, e permettono di effettuare chiamate vocali e inviare messaggi istantanei.
I *supernodi* sono nodi ordinari terminali della rete Skype con caratteristiche aggiuntive.
Sono state eseguite diverse prove da parte dei ricercatori Saikat Guha della Cornell University, di Neil Daswani e Ravi Jain per Google, con lo scopo di investigare sui criteri utilizzati da Skype per promuovere un nodo a supernodo [3]. Una di queste prove consisteva nel far girare alcuni nodi Skype in diversi ambienti e aspettare fino a due settimane per osservare l'avvenuta o meno trasformazione. Si è così osservato che i nodi che presentano un collegamento di rete saturo oppure che lavorano dietro NAT non sono stati promossi a supernodi, mentre i nodi con IP pubblico e con connessione Internet a 10 Mbps sono entrati a far parte della rete di supernodi in pochi minuti.
Sembra quindi che i supernodi vengano scelti tra quei nodi che presentano abbondanza di banda di rete libera e che sono pubblicamente raggiungibili.
Ma diventare un supernodo presenta diversi svantaggi dati dal fatto che al supernodo appartengono degli oneri extra. I supernodi infatti, mettono a disposizione di Skype parte della propria banda di rete e delle proprie risorse per consentire la comunicazione, sia VoIP sia di trasferimento di file, tra tutti i client Skype. In particolare, come approfondiremo in seguito nel paragrafo 2.2 "Firewall e NAT", Skype utilizza i supernodi per veicolare completamente le chiamate di due client entrambi, o uno solo, dietro NAT che altrimenti non potrebbero comunicare tra loro proprio perché il NAT, o il firewall, impedisce la connessione.

Un altro elemento fondamentale che caratterizza la rete peer-to-peer di Skype è il *server d'accesso* o login server.
Ogni nodo deve connettersi al server d'accesso in modo da effettuare il login alla rete Skype. In questo server infatti sono registrati i nomi degli utenti e le rispettive password, permettendo l'autenticazione dell'utente. Il server d'accesso garantisce anche il rispetto

delle norme di composizione e di unicità del nome utente e della password.
Una lista cifrata di login server è codificata nel file eseguibile di Skype, il quale al momento dell'accesso si connette casualmente ad uno di questi server [4]:

- dir1.sd.skype.net:9010
- dir2.sd.skype.net:9010
- dir3.sd.skype.net:9010
- dir4.sd.skype.net:9010
- dir5.sd.skype.net:9010
- dir6.sd.skype.net:9010
- dir7.sd.skype.net:9010
- dir8.sd.skype.net:9010
- http1.sd.skype.net:80
- http2.sd.skype.net:80
- http3.sd.skype.net:80
- http4.sd.skype.net:80
- http5.sd.skype.net:80
- http6.sd.skype.net:80
- http7.sd.skype.net:80
- http8.sd.skype.net:80

La figura 2.2 [7] illustra la relazione tra nodi ordinari, supernodi e server d'accesso.
A parte il login server per l'autenticazione e l'accesso alla rete, non è presente un server centrale per le risorse di rete. Le informazioni degli utenti online e offline, infatti, sono memorizzate e propagate in un modello decentralizzato, e così anche le richieste di ricerca degli utenti.

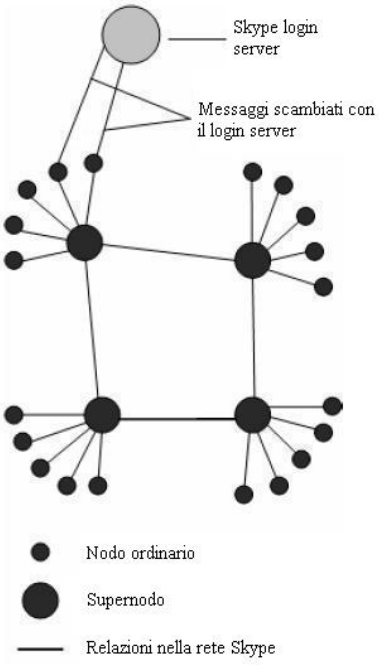

Figura 2.2: Struttura della rete Skype

È possibile elencare anche altre caratteristiche della rete Skype.
Innanzitutto le *porte* utilizzate dal sistema. Un client Skype, che non sia dietro un firewall o un NAT, apre in ascolto la porta listening corrispondente al numero 80, ossia una porta HTTP di tipo TCP, e la porta corrispondente al numero 443 di tipo HTTPS. In aggiunta il client apre una porta listening di tipo TCP e UDP al numero configurato nella finestra di connessione del computer al momento dell'installazione. A differenza di altri protocolli Internet, Skype non ha un numero di porta fisso.
Un'altra caratteristica di Skype è data dall'*host cache*, una lista di indirizzi IP e di porte dei supernodi raggiungibili, che i client costruiscono e aggiornano periodicamente. La host cache deve contenere almeno un indirizzo IP e un numero di porta di un supernodo Skype online. Se il client utilizza un sistema operativo Windows allora questa lista viene memorizzata nel registro Windows in [7] :
HKEY_CURRENT_USER/ SOFTWARE/ SKYPE/ PHONE/LIB/CONNECTION/ HOSTCACHE
Sono stati eseguiti diversi esperimenti, da parte di Salman A. Baset e Henning Schulzrinne del Dipartimento di Computer Science della Columbia University [7], e si è arrivati alla conclusione che la host cache può contenere, al massimo, informazioni per 200 supernodi.
Il *codec* è un elemento indispensabile per l'efficienza di un sistema VoIP. Il codec comprime i dati in modo da ridurre la banda richiesta per la trasmissione, per poi decomprimerli in fase

di lettura. Durante la fase di compressione, però, viene ridotta la precisione dell'immagine nei file video, e del suono nei file audio. Per questo motivo è importante utilizzare un buon codec in modo che la qualità della telefonata non venga compromessa. Skype utilizza iLBC, iSAC e un terzo codec non noto, tutti a banda larga.
Una caratteristica delle compagnie telefoniche tradizionali e dei sistemi VoIP in generale, è data dalla *soppressione del silenzio*. Con questo termine si descrive la scelta di non trasmettere pacchetti sulla rete quando uno degli interlocutori della chiamata non parla. Skype, al contrario, non utilizza la tecnica della soppressione del silenzio, generando 33 pacchetti al secondo per tutte le connessioni VoIP indipendentemente dalle caratteristiche del discorso.

2.2 Firewall e NAT

Il *firewall*, dall'inglese muro antifuoco, è un apparato di rete hardware o software la cui funzione principale è creare un filtro sui pacchetti entranti e uscenti, in modo da innalzare il livello di sicurezza della rete. Questo perché il firewall ha la possibilità di esaminare un pacchetto IP per leggere le informazioni presenti nell'header e, talvolta, per leggere anche il contenuto stesso del pacchetto (deep packet inspection). In tal modo l'apparato può eseguire operazioni di controllo, modifica e monitoraggio.
Una famiglia particolare di firewall sono i *personal firewall* ovvero software installati sui computer che filtrano solo i pacchetti entranti e uscenti da quel calcolatore, in particolare effettuano controlli su tutti i programmi presenti sul computer che tentano di accedere ad Internet.
Il funzionamento dei due firewall descritti non è lo stesso. Nel primo caso, le regole che gestiscono il flusso del traffico vengono impostate in base all'indirizzo IP sorgente, a quello di destinazione e alla porta, mentre nel personal firewall è l'utente stesso che decide a quali applicazioni è concesso l'accesso alla rete Internet e a quali è negato.
Il *NAT*, Network Address Translation ovvero traduzione degli indirizzi di rete, è una tecnica che consiste nel modificare gli indirizzi IP dei pacchetti all'interno di una comunicazione.
É possibile distinguere tra *source NAT* e *destination NAT* a seconda che venga modificato l'indirizzo sorgente o l'indirizzo di destinazione del pacchetto che inizia una nuova connessione. Una tipologia di NAT è il *NAT dinamico* che permette di modificare non solo gli indirizzi IP ma anche le porte TCP e UDP delle connessioni.
L'obiettivo dei NAT è quello di dare l'illusione di comunicare con un indirizzo IP diverso da quello effettivamente utilizzato. Questa tecnica viene usata per diverse ragioni, come ovviare alla scarsità di indirizzi IP pubblici disponibili oppure permettere una connessione tra le Intranet, ovvero reti private sviluppate sul modello di Internet ma con indirizzi IP privati, e Internet stesso, che utilizza solo indirizzi IP pubblici. I NAT vengono usati anche per ragioni di sicurezza, in quanto le tecniche utilizzate rendono i computer non direttamente raggiungibili da Internet.

Proprio le caratteristiche dei firewall e dei NAT creano notevoli problemi nella comunicazione VoIP tra nodi che utilizzano queste tecniche. Alcune problematiche sono date dal fatto che [4] :

- gli indirizzi IP e i numeri di porte interni non sono ricavabili perché i NAT li riscrivono;
- l'uso di firewall e NAT blocca la sessione in fase di ricezione;
- il protocollo UDP non è utilizzabile per via delle caratteristiche dei NAT;
- il firewall blocca molte porte;
- la sessione da TCP a NAT è, di default, di sola andata.

Skype, tuttavia, riesce a districarsi tra le varie problematiche consentendo la comunicazione anche tra client che usano firewall e NAT.
Sono stati condotti diversi esperimenti, da parte dei ricercatori Saikat Guha della Cornell University, di Neil Daswani e Ravi Jain per Google [3], con lo scopo di esaminare in dettaglio i meccanismi di comunicazione utilizzati da Skype. L'esperimento consisteva nell'avviare due client con versione Skype 1.1.0.13 per Linux su computer separati, e osservare gli indirizzi IP sorgenti e di destinazione dei pacchetti inviati e ricevuti, in risposta a varie richieste poste a livello applicativo.
Si è quindi osservato che in Skype i nodi inviano traffico di controllo (control traffic) oltre a informazioni, messaggi istantanei e richieste per sessioni di tipo VoIP e di tipo trasferimento di file, attraverso i supernodi della rete peer-to-peer.
Se le richieste inviate da un peer vengono accettate dalla controparte, allora viene stabilita una connessione diretta tra i due client.
Come già accennato, i problemi si creano quando entrano in gioco firewall e NAT.
Per studiare questo importante aspetto, i ricercatori hanno ripetuto l'esperimento prima per un client dietro NAT/firewall e successivamente per entrambi i client dietro differenti NAT/firewall.
Si è quindi osservato che, se un solo client è dietro NAT/firewall, Skype usa una connessione inversa (connection reversal) in cui è il nodo che utilizza NAT/firewall ad avviare una sessione TCP/UDP come mezzo per iniziare una sessione VoIP o di trasferimento file.
Invece, se entrambi i client sono dietro NAT/firewall, Skype usa un attraversamento NAT di tipo STUN per stabilire una connessione diretta tra i client. Nel caso in cui l'attraversamento NAT fallisca o il firewall blocchi alcuni pacchetti Skype, allora si ricorre ad un approccio di tipo TURN, in cui la sessione è trasmessa da un supernodo raggiungibile pubblicamente.
Approfondiamo questi nuovi dettegli.
Per "attraversamento di NAT" si intende un insieme di tecniche che stabiliscono e mantengono una connessione Internet con un utente dietro NAT. Queste vengono utilizzate soprattutto per applicazioni di rete client-to-client, in particolar modo per rete peer-to-peer. Esistono molte tecniche di attraversamento ma non esiste un unico metodo che

permette di attraversare tutti i tipi di NAT, poiché il loro comportamento non è standard. Per esempio, molti metodi richiedono l'assistenza di un server che generi indirizzi IP pubblici, alcuni utilizzano questo server solo per stabilire la connessione, mentre altri trasmettono tutti i dati attraverso il server stesso.
Il primo attraversamento NAT usato da Skype è, come appena visto, il Session Traversal Utilities for NAT, STUN. Questo permette al client di ottenere un indirizzo di trasporto, consistente in indirizzo IP e porta, adatto nel ricevere pacchetti provenienti da altri peer. Tuttavia gli indirizzi generati da protocolli STUN non sono utilizzabili da tutti gli utenti. Per questo motivo Skype utilizza, in secondo luogo, un attraversamento di tipo TURN, cioè Traversal Using Relays around NAT. Il TURN è un protocollo che fornisce le stesse funzioni di sicurezza garantite da un NAT/firewall ma allo stesso tempo permettere una connessione verso un altro singolo peer. I dati vengono trasmessi attraverso un server che gira, appunto turn, le tabelle contenenti indirizzi IP e porte, in modo tale da generare indirizzi di trasporto che permettano di ricevere pacchetti da quasi ogni peer. Quindi TURN fornisce al client quasi sempre la connettività, ma ciò richiede dei costi molto alti in termini di efficienza, come l'aumento della latenza (ovvero del tempo di risposta di un sistema) causando dei ritardi nella comunicazione voce-video in tempo reale. Per questo motivo Skype utilizza il protocollo TURN solo come ultimo approccio nel caso in cui il protocollo STUN non ottiene esiti positivi.

Complessivamente il meccanismo impiegato da Skype per adempiere alle richieste VoIP e di trasferimento file risultano robuste anche per NAT e firewall, ottenendo inoltre un'ottima corrispondenza voce-video in tempo reale.

2.3 Caratteristiche della rete Skype

Come accennato nel primo capitolo, Skype è un sistema VoIP proprietario, quindi i protocolli e le caratteristiche del sistema e della rete non sono resi noti. Tuttavia, equipe di studiosi hanno condotto diversi esperimenti con l'intento di studiare e analizzare le peculiarità di questo sistema.
In questo capitolo, attraverso gli studi condotti da diversi esperti, si cercano di esaminare alcune caratteristiche della rete peer-to-peer di Skype.

2.3.1 Churn

Con il termine *churn* si intende l'"agitazione" della rete peer-to-peer, ovvero il continuo processo di ingresso e di uscita di nodi dalla rete. Il churn è una caratteristica molto importante e da monitorare continuamente per far si che il traffico venga gestito in maniera ottimale. Senza un controllo dei nodi presenti nella rete, è possibile che alcuni pacchetti vengano instradati verso nodi mancanti mentre invece alcuni nuovi nodi non vengono

considerati, riducendo così l'efficienza della rete. Per questo il churn è stato ampiamente studiato soprattutto in reti di file-sharing peer-to-peer nelle quali questo parametro raggiunge livelli molto alti. In queste reti infatti, il tempo di sessione di un nodo, ovvero l'intervallo di tempo che intercorre tra l'ingresso di un nodo nella rete e la sua uscita, può essere breve, anche di soli pochi minuti. In questi casi il churn è gestito attraverso frequenti aggiornamenti con ristrutturazioni dinamiche della rete e periodiche manutenzioni del traffico, in modo da mantenere la compattezza della rete stessa.
L'obiettivo di questo paragrafo è quello di studiare il churn nella rete dei supernodi di Skype. Per far ciò è necessario introdurre tre esperimenti eseguiti in parallelo da parte dei ricercatori Saikat Guha della Cornell University, di Neil Daswani e Ravi Jain per Google [3].

1. Attività nella rete dei supernodi:
   in questa prova si è osservata l'attività di un supernodo Skype nella rete per 135 giorni, precisamente dal 1 Settembre 2005 al 14 Gennaio 2006, con versione 1.2.0.11 per Linux. In totale sono stati raccolti 13 GB di dati inviati e ricevuti dal supernodo relativi a trasmissioni di tipo VoIP e di trasferimento file.

2. Popolazione dei supernodi:
   sono stati individuati gli indirizzi IP e i numeri di porte di nodi e supernodi nel periodo compreso tra il 25 Luglio 2005 e il 12 Ottobre dello stesso anno. Skype prevede che ogni client abbia una propria host cache, cioè una lista di indirizzi IP di supernodi e di porte alle quali accedere, che viene regolarmente aggiornata. È stato allora elaborato uno script che esegue diverse operazioni sulla host cache dell'utente. Innanzitutto lo script analizza la lista degli indirizzi IP dei supernodi per poi sostituire interamente tale lista con un singolo indirizzo IP di un supernodo scelto dalla lista stessa. Con questa operazione il client è costretto, al successivo accesso, ad utilizzare esclusivamente quel supernodo. Si attende poi l'aggiornamento della host cache con i nuovi indirizzi IP dei supernodi ai quali il nodo è connesso. Lo script, a questo punto, svuota nuovamente la lista e l'intero procedimento si ripete.
   Attraverso questo meccanismo è stato possibile effettuare una scansione della rete dei supernodi. Inoltre, come effetto secondario, lo script ha memorizzato anche il numero degli utenti Skype online quando il client era connesso alla rete.

3. Istantanee di supernodi online:
   per ottenere le istantanee dei supernodi online, è stato creato uno script che invia dei ping a livello applicativo verso i supernodi.
   Un *ping* è un programma che misura il tempo impiegato dai pacchetti per raggiungere un altro dispositivo di rete e poi tornare indietro. Tecnicamente un ping invia un pacchetto di tipo ICMP *echo request* verso un supernodo e rimane in attesa della corrispondente risposta che avviene con l'invio di un pacchetto di tipo *echo reply*. Il programma calcola poi il numero di pacchetti inviati e ricevuti, la loro dimensione,

il tempo totale trascorso tra l'invio di ogni pacchetto e la ricezione della risposta corrispondente, la media dei tempi e la percentuale di risposte ottenute. Per questo, il ping viene spesso utilizzato per attestare la raggiungibilità di un altro computer connesso alla rete.
Ogni istantanea è il risultato dell'invio di ping paralleli verso un set di 6000 supernodi scelti casualmente dalla host cache. Ogni istantanea è stata eseguita in 4 minuti e ripetuta dopo un intervallo di 30 minuti. L'esperimento, di durata un mese, ha avuto inizio il 12 Settembre 2005.

I dati ottenuti da queste prove permettono di studiare il churn nella rete peer-to-peer dei supernodi di Skype.
Vediamo in dettaglio.

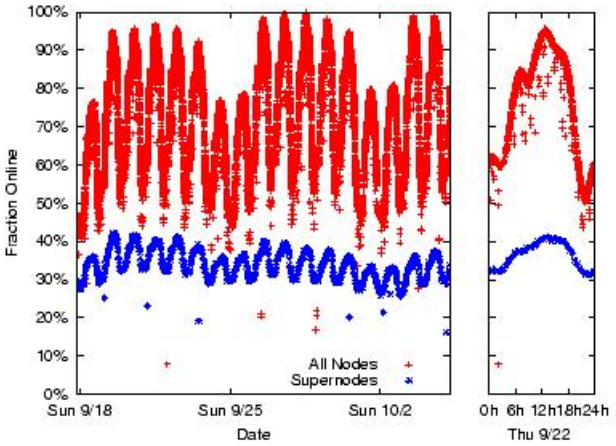

Figura 2.3: Percentuale di nodi e supernodi attivi

La figura 2.3 [3] confronta il numero di supernodi con il numero di utenti online. Il grafico è diviso in due parti: la parte a sinistra mostra la variazione giornaliera della popolazione dei client e dei supernodi dal 18 Settembre al 4 Ottobre 2005, mentre a destra viene mostrato un particolare che evidenzia la variazione oraria relativa a mercoledì 22 Settembre.
Dall'analisi del grafico è possibile effettuare diverse osservazioni. Innanzitutto si evince che il numero di supernodi è più stabile rispetto a quello degli utenti online, in quanto la popolazione dei client varia più del 40% ogni giorno mentre la popolazione dei supernodi è più stabile con una variazione inferiore al 25%. Tuttavia è necessario precisare che su 6000 supernodi verso i quali sono stati inviati dei ping, come descritto nel terzo esperimento, solo 2078 supernodi hanno risposto almeno una volta e di questi solo il 30-40% erano online in qualsiasi momento.
Dal grafico si rileva il massiccio utilizzo di Skype anche, e soprattutto, in ambito lavorativo.

Infatti sono evidenti importanti variazioni diurne con un picco di utilizzo durante le normali ore lavorative e con una riduzione anche del 40-50% durante la notte, come evidenziato nello zoom a destra del grafico 2.3. Anche le variazioni settimanali sono significative in quanto si ha un calo del 20% di utenti online nel fine settimana rispetto alla media dei giorni lavorativi.
Anche il grafico 2.4 [3] conferma il massiccio uso di Skype durante le ore lavorative, ma in particolare evidenzia la distribuzione geografica dei supernodi attivi.

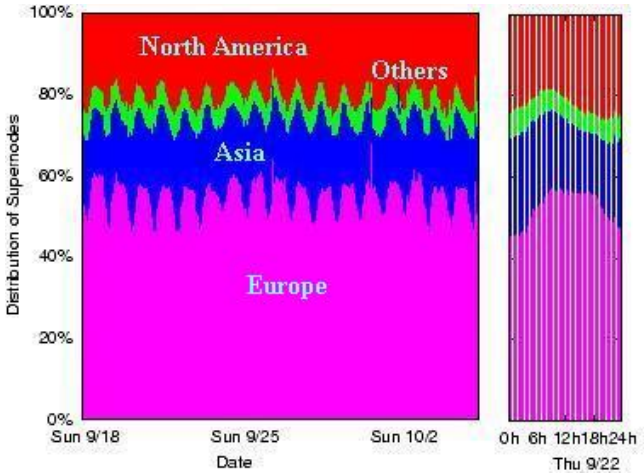

Figura 2.4: Distribuzione geografica dei supernodi attivi

L'Europa contiene il 45-60% dei supernodi della rete Skype, il Nord America contribuisce con il 15-25% mentre l'Asia rappresenta il 20-25% dei supernodi.
Per le aree geografiche considerate, il picco di accessi a Skype si verifica intorno a mezzogiorno, ora locale. Questa caratteristica differenzia Skype rispetto ad una classica rete di file-sharing peer-to-peer, infatti in quest'ultima gli utenti scaricano file avviando processi che hanno la durata di giorni, se non settimane.
Le caratteristiche, quindi, in termini di tempo di sessione e di picchi di utilizzo sono diverse rispetto a quelle registrate in Skype.

Grazie alle istantanee ottenute con il terzo esperimento, è possibile confermare che l'ingresso di nodi nella rete Skype è concentrato soprattutto alla mattina, mentre le uscite dalla rete si verificano verso sera, come mostrato dall'ingrandimento della figura 2.5 [3] .
La mediana del tempo di sessione di un supernodo è di 5.5 ore, valore più alto rispetto alla corrispondente media calcolata su reti di file-sharing peer-to-peer. Bisogna però precisare che in questo calcolo si è tenuto conto sia dei supernodi che dei nodi.

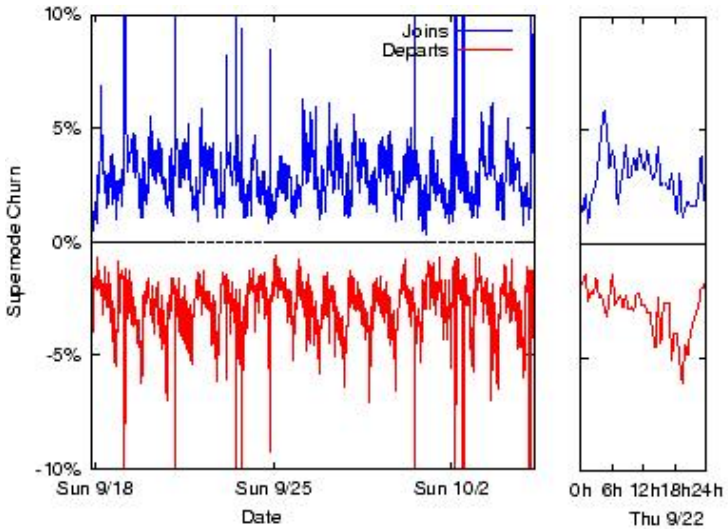

Figura 2.5: Percentuale di supernodi entranti e uscenti dalla rete

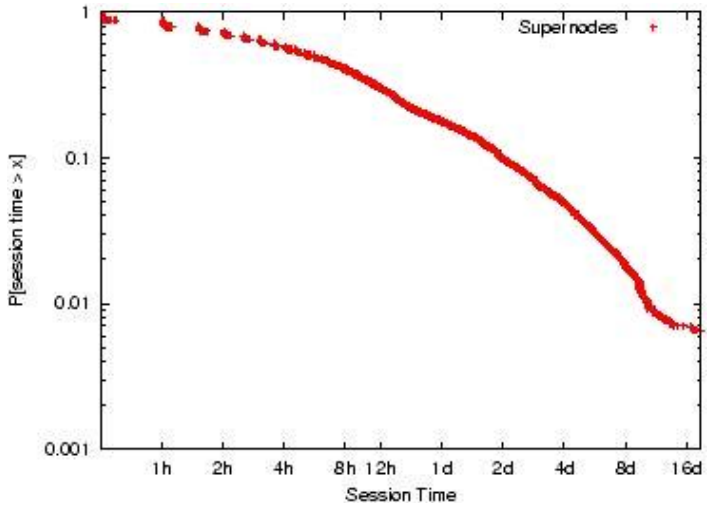

Figura 2.6: Grafico del complementare della CDF del tempo di sessione

La figura 2.6 [3] mostra il complementare della CDF del tempo di sessione dei supernodi Skype. Per CDF, Cumulativa Distribution Function, si intende la funzione di ripartizione che associa ad ogni tempo di sessione la probabilità dell'evento "tempo di sessione $\leq$ x". Questo tipo di distribuzione risulta utile soprattutto per identificare leggi di potenza, ovvero leggi della forma: $f(x) = ax^k + o(x^k)$
Tenendo conto delle problematiche incontrate durante gli esperimenti e delle perdite dei dati dovute all'elevato livello di sicurezza di Skype, è possibile approssimare il grafico ottenuto con un segmento. Dal grafico si ricava quindi una legge di potenza. La natura di questa distribuzione suggerisce che le entrate e le uscite di supernodi nella rete Skype non possano essere modellate attraverso processi uniformi o di Poisson con parametro di proporzionalità costante. Conseguentemente, i risultati di esperimenti passati che modellano il churn con questi processi, se applicati a Skype potrebbero risultare fuorvianti.
Per modellare l'ingresso dei supernodi nella rete è necessario considerare un processo di Poisson con tassi orari variabili, più alti alla mattina rispetto che alla sera per via dell'andamento orario dell'ingresso dei supernodi nella rete, come già analizzato.
Considerando la definizione di distribuzione di Poisson con tasso variabile, è possibile calcolare la probabilità che nell'intervallo di tempo $(a, b]$ si verifichino k ingressi nella rete:

$$P[(N(b) - N(a)) = k] = \frac{e^{-\lambda_{a,b}(\lambda_{a,b})^k}}{k!}$$

dove:
$k = 0, 1, \ldots$
$N(b) - N(a)$ rappresenta il numero di eventi nell'intervallo di tempo $(a, b]$;
$\lambda_{a,b} = \int_a^b \lambda(t)\ dt$ rappresenta il tasso variabile.

Concludendo, è risultato un churn molto piccolo nella rete dei supernodi, con un comportamento diurno e un tempo di sessione medio di diverse ore. Inoltre la modellazione del churn di Skype si ottiene con una distribuzione di Poisson con tassi variabili orari. Questa appartiene alla famiglia di distribuzioni heavy-tailed, nella quale le code sono più pesanti rispetto ad una distribuzione esponenziale e quindi tendono a zero più lentamente (per maggiori chiarimenti e approfondimenti sulla distribuzione heavy-tailed e di Poisson si rimanda all'Appendice A).
Come accennato precedentemente, non solo la modellazione ma anche il monitoraggio del churn è un aspetto importante nella gestione di una rete. Considerando il fatto che più del 95% dei supernodi presente in un'istantanea è presente anche in quella successiva, eseguita dopo un intervallo di 30 minuti, è d'obbligo concludere che Skype effettua periodici controlli e aggiornamenti della rete, in modo da mantenere costante la disponibilità dei supernodi.

2.4 La rete peer-to-peer in VoIP

Skype, utilizzando una rete peer-to-peer per le trasmissioni di tipo VoIP, ha introdotto un nuovo modo di comunicare: sfruttare la rete disponibile e le risorse dei supernodi per coordinare le chiamate, utilizzando solo in alcuni casi, e comunque in minima parte, la rete telefonica tradizionale.
In questo paragrafo, quindi, si vuole analizzare il ruolo che la rete peer-to-peer gioca nel contesto VoIP di Skype, senza trascurare però l'aspetto del trasferimento di file. Studiamo perciò l'apporto che i supernodi danno alla rete peer-to-peer di Skype.

A questo scopo, è necessario analizzare il grafico 2.7 [3], il quale mostra la banda di rete utilizzata dai supernodi ad intervalli di tempo di 30 secondi.
Risulta che per il 50% del tempo i supernodi consumano meno di 205 bps. Quindi sembra che i supernodi sostengano un costo di banda piccolo per la maggior parte del tempo.
Ora, identifichiamo le varie tipologie di traffico e le separiamo tra loro. Otteniamo, così, il traffico di controllo, il traffico dati di trasmissioni VoIP, il traffico del trasferimento di file e il traffico generato dalla messaggistica istantanea. Questa operazione di separazione è resa difficoltosa dall'utilizzo, da parte di Skype, di operazioni di cifratura sul proprio traffico di controllo e di dati. Si deve così ricorrere ad approcci statistici. Tuttavia questo metodo non è ottimale, infatti può classificare erroneamente piccoli trasferimenti di file come traffico di controllo, ma in generale fornisce una buona stima sul traffico di Skype.

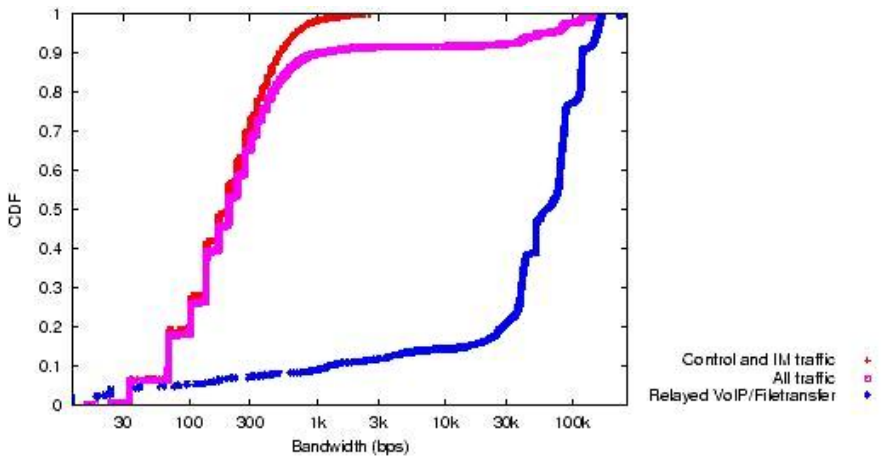

Figura 2.7: CDF della banda utilizzata dai supernodi ad intervalli di 30 sec

Risulta che un supernodo è impegnato nella trasmissione dati per il 9.6% del tempo. Questo valore è più piccolo di quanto ci si aspetta, ma ciò è spiegabile dall'uso di validi sistemi di attraversamento NAT, che stabiliscono sessioni dirette di tipo VoIP o di trasfe-

rimento file tra utenti dietro NAT o firewall.
Durante questo tempo, per trasmettere i dati il supernodo usa mediamente 60 kbps oltre ad un piccolo consumo di potenza e memoria rispetto ad un nodo ordinario.

2.5 Comportamento degli utenti di Skype

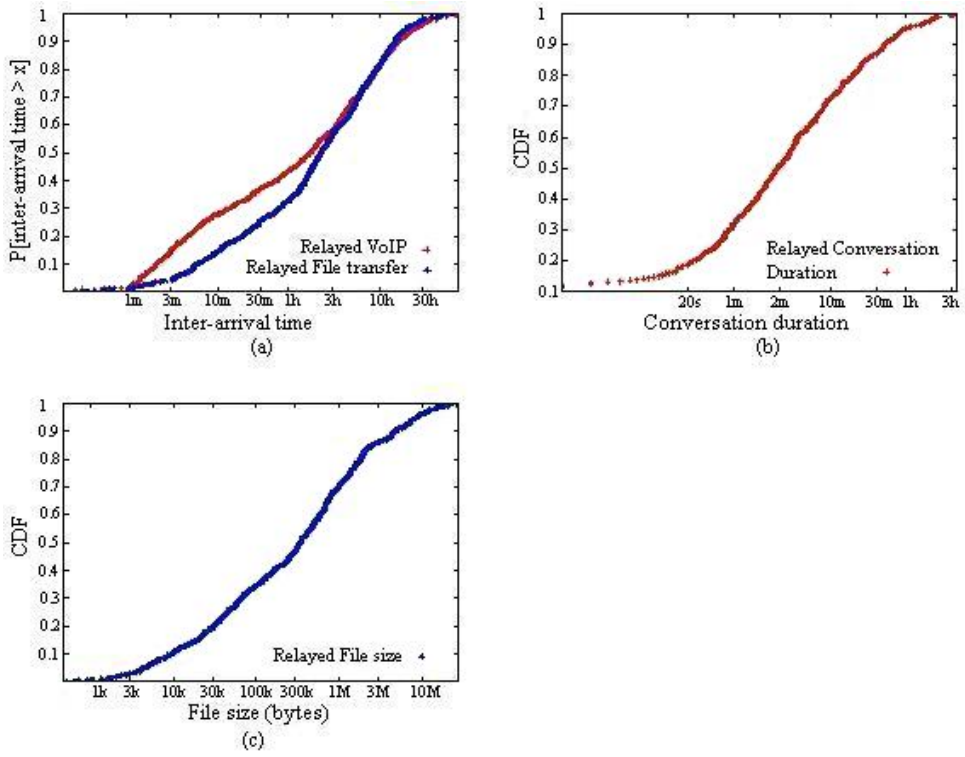

Figura 2.8:
(a) CDF del tempo che intercorre tra l'arrivo di due pacchetti successivi
(b) CDF della durata delle conversazioni
(c) CDF della dimensione dei file trasferiti

I grafici riportati nella figura 2.8 [3] mostrano alcune tendenze degli utenti Skype.
I dati, utilizzati per costruire tali grafici, sono ottenuti dall'esperimento 1 descritto precedentemente. La cifratura del traffico Skype ha creato notevoli problematiche, limitando l'osservazione solo a sessioni di tipo VoIP e di trasferimento file trasmesse attraverso supernodi e non per sessioni dirette o di messaggistica istantanea. Questo ha impedito lo studio di gran parte del traffico, portando ad una perdita di dati stimata attorno al 85%,

tanto che sono stati raccolti solo 1121 dati in 135 giorni di test.
Per questi motivi non è possibile parlare di uno studio del comportamento degli utenti Skype, bensì solo di tendenze.
Se la scarsità di dati raccolti è un fattore negativo per questo tipo di ricerche, dal punto di vista della sicurezza della rete, invece, i risultati sono incoraggianti. Come approfondiremo nel capitolo 4, la cifratura dei messaggi e del traffico, rende Skype impenetrabile ad attacchi esterni.
Ritornando al comportamento degli utenti, il grafico 2.8(a) confronta il tempo che intercorre tra l'arrivo di due pacchetti successivi trasmessi attraverso supernodi, in sessioni di tipo VoIP e di trasferimento file. In entrambi i casi i tempi seguono una distribuzione di Poisson. In questo grafico è possibile anche fare un confronto tra le chiamate VoIP e i trasferimenti di file; si osserva così che gli utenti prediligono utilizzare Skype per effettuare chiamate rispetto a trasferimenti di file.
Il grafico 2.8(b) mostra la durata delle chiamate effettuate con Skype. La durata media delle telefonate è di 12min 53sec, un valore più alto rispetto alla media dei 3 min di chiamate telefoniche tradizionali. La ragione di questa differenza è data dal fatto che le chiamate VoIP di tipo Skype-to-Skype sono gratuite, o comunque a basso costo, mentre le chiamate telefoniche tradizionali hanno tariffe più alte.
Il grafico 2.8(c) mostra invece le dimensioni dei file trasferiti utilizzando Skype. La dimensione media è di 346 kB. Questa dimensione è più piccola di quelle associate a file di tipo audio o video, mentre è simile alle dimensioni di file di documenti, presentazioni e foto. In questo modo è possibile ottenere la tipologia dei file maggiormente scambiati tra utenti Skype.

Concludendo, gli utenti Skype hanno dei comportamenti diversi sia rispetto agli utenti di telefonia tradizionale, per quanto riguarda la durata delle chiamate, sia rispetto agli utenti di reti di file-sharing, per quanto riguarda la tipologia di file condivisi.

2.6 Rete Skype vs rete peer-to-peer

Come più volte affermato, Skype si basa su una rete peer-to-peer per localizzare altri utenti, per trasmettere comunicazioni vocali, trasferimenti di file e per soddisfare le richieste degli utenti.
Una rete peer-to-peer è una rete informatica che connette tra loro diversi calcolatori, permettendo condivisioni e scambi di dati. La particolarità di una rete peer-to-peer è data dall'assenza di una gerarchia tra i nodi, in inglese peer cioè pari. Essi infatti sono tra loro tutti equivalenti in quanto possono fungere sia da client che da server verso gli altri nodi della rete, così qualsiasi nodo è in grado di avviare un trasferimento di dati.
Un esempio di rete peer-to-peer pura è la rete di file-sharing per la condivisione di file, e

rappresenta l'antitesi di un sistema di tipo client-server nei quali sono solo ed esclusivamente i server a gestire le risorse. Alcune reti usano invece un sistema peer-to-peer ibrido, riproducendo il modello client-server per alcuni compiti, come la ricerca di altri peer, mentre usano il modello peer-to-peer per tutte le altre richieste.

La rete Skype, è una rete peer-to-peer ibrida, in quanto molti aspetti la differenziano da una rete peer-to-peer pura.
Innanzitutto Skype si affida ad un server centrale di autenticazione per identificare gli utenti e per distribuire gli aggiornamenti del software, al contrario di una rete pura peer-to-peer che non ammette server. La rete Skype comprende anche altri server di tipo secondario localizzati in vari Paesi per le funzioni di SkypeIn e SkypeOut, già descritte precedentemente, che raccordano la rete Skype con la rete telefonica tradizionale.
Inoltre alcuni peer Skype vengono promossi a *supernodi*, secondo alcuni parametri dati dalla disponibilità di banda, dall'assenza di NAT/firewall e dalla presenza di un indirizzo IP pubblico. I supernodi hanno diversi compiti, tra cui consentire la connessione tra utenti dietro NAT/firewall; quest'ultimi utenti infatti scansionano la rete Skype cercando dei supernodi e con essi formano e mantengono una connessione, in modo tale da permettere una comunicazione anche tra peer dietro NAT/firewall. La presenza dei supernodi crea una gerarchia tra i nodi della rete, minando l'uguaglianza tra i peer.
Anche alcuni comportamenti degli utenti Skype differiscono dai comportamenti degli utenti delle classiche reti peer-to-peer di file sharing. Come già visto, gli utenti Skype prediligono utilizzare le funzioni di chiamate VoIP, e quando ricorrono ai servizi di trasferimento file condividono documenti, presentazioni o foto. Comportamento diverso per gli utenti di file-sharing che trasferiscono principalmente file di tipo audio-video.

Capitolo 3

La crittografia in Skype

Skype utilizza la crittografia per diversi scopi. Nei capitoli precedenti è stato accennato l'uso della crittografia in Skype per cifrare il traffico in modo da non consentirne lo studio e la classificazione. Questo obiettivo è stato pienamente raggiunto. Come visto nei paragrafi 2.5 e 2.6 del capitolo precedente, equipe di studiosi hanno provato a studiarne il traffico, ma la cifratura ha portato ad una perdita dei dati stimata attorno all'85% consentendo lo studio solo su un numero ristretto di dati. In particolare l'osservazione del traffico è limitata solo a sessioni di tipo VoIP e di trasferimento di file trasmesse esclusivamente attraverso supernodi, mentre viene negata la valutazione di sessioni di chat e qualsiasi sessione trasmessa in maniera diretta tra i nodi. Anche la classificazione dei pochi dati ottenuti non è ottimale, è infatti necessario utilizzare un approccio statistico che prevede la possibilità di errori.
Ma l'uso della crittografia da parte di Skype non si limita alla sola cifratura del traffico. La crittografia viene usata per risolvere uno dei problemi più delicati per un sistema VoIP: l'autenticazione degli utenti. In Skype questo obiettivo viene raggiunto creando, per ogni utente, un Certificato di Identificazione firmato digitalmente dal Server Centrale. Così, quando si avvia una sessione, ogni peer verifica l'identità degli utenti attraverso tale certificato.
Un'altra innovazione introdotta da Skype riguarda la cifratura del contenuto dei messaggi trasmessi nella rete peer-to-peer, per consentire una comunicazione privata e una maggiore sicurezza contro attacchi di tipo hacker.

Ed è proprio in questo capitolo che verrà analizzato l'aspetto crittografico di Skype, sia per l'autenticazione che per la segretezza della comunicazione.

3.1 Il protocollo

Il protocollo utilizzato da Skype, sia per l'autenticazione degli utenti sia per criptare i messaggi trasmessi, è di tipo proprietario. Di conseguenza non è osservabile e studiabile se non dagli addetti ai lavori. Tuttavia diverse equipe di crittografi sono riuscite a dedurre alcune caratteristiche del sistema. In particolare il crittografo Tom Berson con il suo Anagram Laboratories ha condotto diversi studi, finché nell'aprile 2005 è stato contattato direttamente da Skype per analizzare, valutare e migliorare proprio il protocollo proprietario di sicurezza [8]. Questa equipe ha analizzato il codice base della versione 1.3 di Skype.

Dallo studio sul protocollo è risultato che, nonostante il sistema crittografico sia proprietario, Skype non utilizza un nuovo e proprio algoritmo di cifratura bensì assembla e unisce primitive crittografiche standard, tra le quali:

- il cifrario a blocchi AES;
- il crittosistema a chiave pubblica RSA;
- lo standard per la firma digitale ISO 9796-2;
- la funzione hash SHA-1;
- la cifratura a flusso RC4.

Anche in sezioni non prettamente crittografiche vengono utilizzati criteri già testati e affermati. Per esempio nella generazione di numeri primi viene impiegato il Test di Miller-Rabin mentre nella creazione di alcune chiavi private viene adottato il Metodo Montgomery.
L'uso di standard crittografici e metodi numerici già affermati rappresenta una scelta vantaggiosa sotto vari punti di vista. Innanzitutto è complesso e costoso realizzare un sistema crittografico nuovo ed efficiente, inoltre sono necessarie molte prove, verifiche e test per controllare la sua efficacia, la sua sicurezza, e per scovare i punti deboli che lo rendono vulnerabile. Per un prodotto come Skype, invece, il tempo è essenziale. In tali settori è necessaria la tempestività, e quindi sfruttare algoritmi già affermati e validi risulta vantaggioso.

3.2 Implementazione di RSA

L'RSA è un cifrario a chiave pubblica ideato, nel 1977, dai ricercatori Rivest, Shamir e Adleman, da qui la sigla RSA.
Il vantaggio offerto da un sistema a chiave pubblica sta nel non richiedere la condivisione di una chiave segreta. Questa tipologia di cifrari è basata sull'idea seguente. Un utente A ha due chiavi, una privata e una pubblica. Un utente B invia ad A messaggi cifrati attraverso la chiave pubblica di A, ed essendo pubblica qualsiasi utente può farlo, ma la

decifrazione può essere eseguita solo con la chiave privata di A, quindi solo A stesso può decifrare il messaggio che ha ricevuto.

Vediamo in dettaglio la generazione di un paio di chiavi RSA.
Innanzitutto è necessario generare due numeri primi grandi, chiamati p e q.
Skype genera dapprima due numeri casuali grandi con l'algoritmo RC4, che analizzeremo nel paragrafo 3.5, successivamente utilizza il test di primalità di Miller-Rabin per determinare se i numeri considerati sono primi.
Il numero di iterazioni di default del test di Miller-Rabin implementato da Skype è 25. In questo modo la probabilità che il test identifichi un numero composto come primo è estremamente bassa, precisamente la probabilità è inferiore a 10^{-16}. Per calcolatori che hanno una limitata velocità di elaborazione, 25 iterazioni sono troppo dispendiose in termini di tempo quindi Skype le riduce a sole 5. Ancora in questo caso il test garantisce una probabilità di errore bassa, pari a 0.00063, rendendo l'algoritmo efficiente anche per questi calcolatori.
Una volta che i due numeri primi grandi, p e q, sono stati determinati, si calcola il loro prodotto andando a definire quello che viene chiamato il *modulo* di RSA: $n = pq$
Si calcola la funzione di Eulero ϕ di n, cioè si calcola il numero dei valori interi positivi minori e primi con n stesso. Essendo n un numero di cui si conosce la scomposizione in fattori primi allora il calcolo si limita ad una semplice operazione: $\phi(n) = (p-1)(q-1)$.
L'*esponente di cifratura*, che chiamo e, è un valore primo con $\phi(n)$.
Si costruisce così la chiave pubblica RSA, costituita dalla coppia *(e,n)*.
La chiave privata, o *esponente di decifrazione* d, è calcolata in modo tale che valga la seguente relazione:

$$de \equiv 1 \mod \phi(n)$$

Per migliorare l'algoritmo di calcolo dell'esponente di decifrazione, Skype utilizza la riduzione di Montgomery anziché la riduzione di Euclide. Montgomery, sebbene usi calcoli aggiuntivi, sostituisce le divisioni richieste dal metodo Euclideo, che risultano computazionalmente onerose, con semplici e rapide divisioni per 2.

Nel cifrario RSA le funzioni di cifratura e decifrazione sono immediate.
Sia *(e,n)* la chiave pubblica e $m \in \{0, 1, ..., n-1\}$ il messaggio da cifrare.
La funzione di cifratura RSA che permette di trovare il messaggio cifrato c è:

$$c \equiv m^e \mod n$$

mentre, data la chiave privata d, la funzione di decifrazione per ritrovare il messaggio originale è:

$$m \equiv c^d \mod n$$

Skype rende più efficiente l'implementazione di RSA usando nei passaggi critici il linguaggio assembly, ovvero il linguaggio di programmazione più vicino al linguaggio macchina.

La sicurezza effettiva del sistema RSA non è conosciuta.
Tuttavia è ritenuto un cifrario sicuro, perché l'unico modo finora noto per forzare RSA è conoscere l'esponente di decifrazione d e ciò equivale a conoscere il valore della funzione di Eulero $\phi(n)$, ma non è possibile conoscere $\phi(n)$ senza conoscere p e q. Cioè, la sicurezza di RSA è collegata alla capacità di fattorizzare il numero n, ma, ad oggi, non esistono algoritmi di fattorizzazione efficienti.

3.3 La firma digitale

La firma digitale è un meccanismo di sicurezza che presenta diversi scopi. Essa, infatti, autentica il mittente del messaggio per tutti gli utenti della rete, in quanto solo il soggetto autentico può apporre la firma. Inoltre, la sua presenza attesta l'integrità del documento in questione e la non ripudiabilità.

Skype utilizza la firma digitale principalmente per l'autenticazione degli utenti.
Il sistema di firma impiegato da Skype agisce in ambito RSA.
Tecnicamente, se m è il messaggio da firmare, *(e,n)* la chiave pubblica e d la chiave privata del firmatario, la firma s corrispondente viene calcolata come segue:

$$s \equiv m^d \mod n$$

Il destinatario riceve il messaggio firmato composto dalla coppia *(m,s)*, e verifica la validità della firma attraverso un'altra elevazione a potenza:

$$m \equiv s^e \mod n$$

Quindi la firma dipende da tre elementi: la chiave privata, la chiave pubblica e il messaggio. La dipendenza dalla chiave privata permette solamente al mittente di apporre la propria firma, mentre la chiave pubblica consente ad ogni utente di effettuare l'autenticazione. La relazione tra il messaggio e la firma garantisce, invece, l'integrità del messaggio stesso.

Skype utilizza la chiave RSA in modo conforme allo standard ISO 9796-2.
Questo standard, emanato nel 2002 dall'International Organization for Standardization, si occupa, fra gli altri argomenti, dello schema di firma digitale basato sul meccanismo di fattorizzazione di interi.
Seguendo questo standard non viene firmato il messaggio in sé, ma una combinazione di dati che comprende anche il messaggio. Precisamente, per un piccolo flusso di dati da firmare, la sequenza di bit che viene firmata può assumere una della due forme seguenti, espresse in base esadecimale [8]:

$$4A < messaggio >< sha1(messaggio) > BC$$

$$4BBB...BA < messaggio >< sha1(messaggio) > BC$$

Per un grande flusso di dati, il messaggio viene scomposto in più parti. Ognuna di queste parti viene firmata concatenata con altri dati seguendo lo standard:

$$6A < messaggio\_parziale >< sha1(messaggio\_completo) > BC$$

Lo standard ISO 9796-2 prevede la firma di tale combinazione solo per il primo blocco del messaggio, mentre nei successivi blocchi viene firmato direttamente il testo del messaggio . Per il controllo della firma, Skype decifra prima l'RSA con la chiave pubblica poi controlla la combinazione di bit ottenuta, che viene chiamata anche padding.

3.4 La funzione hash: SHA-1

Una funzione hash è un'applicazione $h : \{0,1\}^* \to \{0,1\}^n$ unidirezionale, dove il dominio $\{0,1\}^*$ rappresenta l'insieme delle stringhe di lunghezza arbitraria, mentre il codominio è costituito da stringhe con lunghezza fissata da n. Il valore di n cambia in base al tipo di funzione hash che si utilizza. Nelle funzioni SHA si parte da 160 bit, fino ad arrivare a 512 bit.
Il risultato finale di una funzione hash viene chiamato *message digest*, ovvero impronta del messaggio.
Per definizione di unidirezionalità, se $y \in \{0,1\}^n$ allora è computazionalmente impossibile ricavare un x appartenente a $\{0,1\}^*$ tale che $h(x) = y$.
Un'altra caratteristica molto importante per una funzione hash è data dalla resistenza alle collisioni. Ovvero, data una funzione hash h, è computazionalmente impossibile trovare due valori m_1 e m_2 diversi ma tali che abbiano la stessa immagine, $h(m_1) = h(m_2)$.
Un esempio, molto usato in crittografia, è dato dalle funzioni SHA, Secure Hash Algorithm, sviluppate a partire dal 1993 dalla National Security Agency, NSA.
Della famiglia SHA fanno parte 5 funzioni: SHA-1, SHA-224, SHA-256, SHA-384 e SHA-512.
L'applicazione più utilizzata è la SHA-1 che produce un digest di 160 bit.

Anche Skype, per proteggere i propri dati sia nell'autenticazione degli utenti, sia nella cifratura dei messaggi che in altri ambiti, utilizza la funzione hash SHA-1.
Tuttavia l'algoritmo SHA-1 implementato da Skype non è completamente uguale a quello originale rilasciato dall'NSA. Secondo l'analisi effettuata da Tom Berson e l'Anagram Laboratories [8], il codice usato da Skype risulta più semplice, pulito ed essenziale rispetto all'originale.
La sua validità è comunque garantita, grazie alle verifiche eseguite dall'equipe con l'ausilio

di vettori test. Questi sono vettori noti e dei quali si conosce il risultato nel codice originale. La prova consiste nell'inserire i vettori test come input nell'algoritmo da testare e poi confrontare i risultati ottenuti con quelli noti. Se il risultato prodotto corrisponde a quello conosciuto allora si può affermare che i due algoritmi si equivalgono.
Un esempio di verifica per la funzione SHA-1 è dato dai vettori test di Jim Gillogly e Francois Grieu [9].
Per vedere più in dettaglio questi vettori conviene indicare con *bitstring*#n la stringa costituita dalla ripetizione dei bit in *bitstring* per n volte e con il simbolo | l'operazione di concatenazione. Quindi, per esempio, vale l'uguaglianza: $110\#3|1 = 1101101101$
I vettori test di Gillogly e Grieu con i corrispettivi risultati sono i seguenti:

$$110\#148|11 : CE7387AE577337BE54EA94F82C842E8BE76BC3E1$$

$$110\#149 : DE244F063142CB2F4C903B7F7660577F9E0D8791$$

$$110\#149|1 : A3D2982427AE39C8920CA5F499D6C2BD71EBF03C$$

$$110\#149|11 : 351AAB58FF93CF12AF7D5A584CFC8F7D81023D10$$

$$110\#170 : 996386921E480D4E2955E7275DF3522CE8F5AB6E$$

$$110\#170|1 : BB5F4AD48913F51B157EB985A5C2034B8243B01B$$

$$110\#170|11 : 9E92C5542237B957BA2244E8141FDB66DEC730A5$$

$$110\#171 : 2103E454DA4491F4E32DD425A3341DC9C2A90848$$

$$011\#490 : B4B18049DE405027528CD9E74B2EC540D4E6F06B$$

$$011\#490|0 : 34C63356B308742720AB966914EB0FC926E4294B$$

$$011\#490|01 : 75FACE1802B9F84F326368AB06E73E0502E9EA34$$

$$011\#491 : 7C2C3D62F6AEC28D94CDF93F02E739E7490698A1$$

Il test viene eseguito come descritto prima, verificando le corrispondenze tra i risultati. Ma per un controllo più approfondito e sicuro, è possibile usare vettori ancora più lunghi:

$$110\#1431655764|11 : 1EEF5A18969255A3B1793A2A955C7EC28CD221A5$$

$$110\#1431655765 : 7A1045B914672AFACE8D90E6D19B3A6ADA3CB879$$

$$110\#1431655765|1 : D5E09777A94F1EA9240874C48D9FECB6B634256B$$

$$110\#1431655765|11 : EB2569043C3014E51B2862AE6EB5FB4E0B851D99$$

$$011\#1431655764|01 : 4CB0C4EF69143D5BF34FC35F1D4B19F6ECCAE0F2$$

$$011\#1431655765 : 47D92F911FC7BB74DE00ADFC4E981A8105556D52$$

$$011\#1431655765|0 : A3D7438C589B0B932AA91CC2446F06DF9ABC73F0$$

$$011\#1431655765|01 : 3EEE3E1E28DEDE2CA444D68DA5675B2FAAAB3203$$

Per quanto riguarda l'implementazione di SHA-1 in Skype non sono state identificate anomalie, perciò l'algoritmo SHA-1 originale e quello modificato da Skype si equivalgono, anche e soprattutto dal punto di vista della sicurezza.

3.5 La generazione di numeri casuali

La qualità del metodo di generazione di numeri casuali è un fattore rilevante per quanto riguarda la sicurezza delle sessioni peer-to-peer.
La generazione di numeri casuali è piuttosto complessa, perché attraverso un algoritmo (quindi attraverso una serie di istruzioni deterministiche) si devono creare numeri che non seguano criteri e logiche di sequenze.
Skype utilizza i numeri casuali per diversi scopi crittografici, per esempio nella generazione di coppie di chiavi RSA e di chiavi AES, o nella verifica dell'autenticazione dell'identità.
A seconda dell'utilizzo futuro dei numeri casuali, Skype genera questi numeri con metodi diversi.

Per la creazione di chiavi AES, viene utilizzato il programma di generazione di numeri casuali della piattaforma del client, che quindi varia in base al sistema operativo.
I sistemi operativi con potenza di elaborazione limitata costituiscono un ambiente difficoltoso per generare tali numeri e, di conseguenza, la qualità della casualità dei numeri non è efficiente. Nelle piattaforme Windows invece, la generazione di numeri casuali è efficiente ed il meccanismo è di più facile studio.
In tal caso, Skype effettua chiamate di sistema Win32 ad una funzione del sistema operativo. Queste chiamate restituiscono dei bit, ai quali sono aggiunti alcuni salt, ovvero sequenze di bit. Il risultato viene ulteriormente modificato attraverso una funzione hash, in particolare attraverso la funzione SHA-1, ottenendo una sequenza da 64 bit. Viene calcolata poi l'entropia delle chiamate di sistema che sono state effettuate.
L'entropia, nella teoria dell'informazione, misura in bit la quantità di informazione presente in un segnale aleatorio. Matematicamente, l'entropia H di una variabile aleatoria X è la media dell'autoinformazione $I(x_i)$ dei possibili valori della variabile $X = (x_1, \dots x_n)$. Precisamente:

$$H(X) = E[I(x_i)] = \sum_{i=1}^{n} I(x_i)\ P(x_i) = \sum_{i=1}^{n} P(x_i)\ log_2\ \frac{1}{P(x_i)}$$

Il protocollo, a questo punto, segue le indicazioni descritte in un documento RFC.
In generale il Request For Comments, è un documento che riporta informazioni e specifiche riguardanti innovazioni e metodologie da utilizzare su Internet. Le RFC sono prodotte dall'Internet Engineering Task Force, un'organizzazione internazionale fondata nel 1986 il cui obiettivo è sviluppare e promuovere documenti tecnici per migliorare la gestione e lo sviluppo dei protocolli Internet. La caratteristica principale dell'IETF è data dal libero accesso ai gruppi di ricerca, così ogni persona può partecipare e fornire suggerimenti.
Skype utilizza l'RFC 1750 che tratta della generazione di numeri casuali. Seguendo la procedura standard descritta, vengono mescolati i bit in base all'entropia calcolata.
Il risultato ottenuto è la generazione di un numero che è possibile considerare casuale.

Per la creazione di chiavi RSA serve un generatore di numeri casuali grandi e Skype utilizza l'algoritmo RC4.
L'implementazione di RC4 è standard e la chiave di input fornita da Skype all'algoritmo è costituita da una serie di bit casuali (per approfondire il funzionamento dell'algoritmo si rimanda all'Appendice B).
I numeri così generati vengono considerati come presunti numeri primi e la loro primalità è verificata con il test di Miller-Rabin. Se risultano primi, allora, andranno a creare una coppia di chiavi RSA.

3.6 Registrazione di un utente Skype

La registrazione è uno dei passi più importanti e delicati in un sistema di tipo VoIP per quanto riguarda la sicurezza. Qui si pongono le basi per un efficiente meccanismo di autenticazione degli utenti.

Per la registrazione, Skype utilizza il protocollo RSA a chiave pubblica.
Al momento dell'installazione del software Skype, in ogni client vengono memorizzate diverse informazioni tra le quali anche la chiave pubblica V_S del Server Centrale e un identificatore per la verifica della firma digitale.
La chiave privata del Server, invece, la indico con S_S.
Il Server possiede due coppie di chiavi di diversa lunghezza, una da 1536 bit e l'altra da 2048 bit. La scelta sulla lunghezza della chiave viene fatta dal Server in base alla richiesta da parte dell'utente di poter accedere ad alcuni servizi chiamati premium, come SkypeIn o SkypeOut. Se l'utente effettua una registrazione standard, senza acquistare servizi, allora il Server utilizza la coppia di chiavi di modulo più basso, da 1536 bit. Se l'utente effettua la registrazione Skype attraverso il diretto acquisto di un servizio premium allora il Server Centrale utilizza la coppia di chiavi con modulo più lungo, da 2048 bit. Se l'acquisto di un servizio premium avviene successivamente alla registrazione, il server aggiorna la chiave utilizzando il modulo più lungo.

Avvenuta l'installazione, può incominciare il procedimento di registrazione dell'utente.
L'utente sceglie lo username, che chiamo A, e la password corrispondente, che chiamo P_A.
Il client genera quindi una coppia di chiavi RSA per l'utente, (S_A, V_A). Analogamente alla coppia di chiavi del Server, indico con S_A la chiave privata e con V_A la chiave pubblica dell'utente con username A.
Ora, la chiave privata S_A, e la password protetta dall'azione di una funzione hash $H(P_A)$, vengono memorizzate in modo sicuro nella piattaforma dell'utente.
Nel caso specifico di un client con piattaforma Windows, queste informazioni vengono me-

morizzate attraverso Windows CryptProtectData API[1].
Il client stabilisce, poi, una sessione con il Server Centrale. La sessione stabilita è protetta da un sistema AES con chiave di lunghezza 256 bit, generata dal client attraverso il generatore di numeri casuali della piattaforma su cui lavora l'utente.
Stabilita la sessione, il client verifica l'autenticità del Server con cui è connesso. Anche in questo caso l'autenticazione avviene attraverso la verifica con la chiave pubblica che era stata memorizzata nel client al momento dell'installazione.
Una volta appurata l'attendibilità, il client invia al Server Centrale diverse informazioni tra cui lo username A scelto dall'utente, la password protetta da una funzione unidirezionale hash $H(P_A)$ e la chiave pubblica V_A.
Al Server Centrale spetta il compito di stabilire la regolarità dei dati ricevuti. In primo luogo verifica che l'utente abbia rispettato le regole imposte per la scelta dello username, per esempio non devono esserci spazi e non devono comparire caratteri speciali. Anche nella scelta della password ci sono delle regole, per esempio la lunghezza da 6 a 20 caratteri. Il server verifica poi l'unicità dello username A scelto.
Accertate queste regolarità il Server Centrale memorizza in un database la coppia di dati $(A, H(H(P_A)))$.

Il Server Centrale crea e firma digitalmente il Certificato d'Identità per l'utente A, IC_A. Il Server memorizza all'interno del Certificato IC_A lo username e la chiave pubblica legandoli tra loro attraverso la firma privata del Server: $(A, V_A)^{S_S}$. Come ultimo passo il Server invia il Certificato d'Identità IC_A al client corrispondente.

3.7 La comunicazione tra utenti

Anche nell'ambito della comunicazione tra utenti, la verifica dell'identità dei peer e la riservatezza sul contenuto della conversazione sono elementi fondamentali per un buon sistema VoIP. Per tale motivo Skype affida questi compiti alla crittografia.
Verrà ora analizzato il protocollo per la comunicazione Skype tra due utenti.

Si considerino due utenti Skype: A e B. Precisamente, sia A il chiamante e sia B il chiamato e tra essi non sussista alcuna sessione di comunicazione Skype preesistente.
Viene creata una nuova chiave condivisa di sessione da 256 bit, SK_{AB}, che permette di stabilire una nuova sessione di comunicazione tra i due utenti. Questa nuova sessione avrà luogo per tutta la durata della conversazione, o meglio, finché sarà presente del traffico in ambo le direzioni e successivamente per un intervallo di tempo prefissato.
Una volta che la sessione termina, la chiave condivisa viene memorizzata finché uno dei

[1] API indica Application Programming Interface, è un'interfaccia di programmazione che rappresenta un insieme di funzioni scritte in linguaggio C e assembly per cifrare dati in particolari strutture chiamate *dataBlob* contenenti un numero arbitrario di array di bytes.

due client esce dalla rete Skype. Quando questo si verifica, la chiave SK_{AB} viene azzerata. Supponiamo invece, che gli utenti A e B abbiano già stabilito precedenti sessioni di comunicazione Skype. In tal caso, quando il chiamante A contatta il chiamato B, viene ristabilita la sessione ripristinando la precedente chiave condivisa SK_{AB} che era stata memorizzata.

Essendo Skype un sistema su rete peer-to-peer dove tutti gli utenti sono equivalenti tra loro, dove nessun peer ha vantaggi rispetto agli altri, si ha che il protocollo per la generazione della chiave condivisa è simmetrico.
I due utenti A e B contribuiscono entrambi e in ugual misura alla creazione di SK_{AB} generando ciascuno 128 dei 256 bit della chiave. La creazione di questi bit avviene attraverso un meccanismo che si basa sulla generazione di numeri casuali, i quali vengono poi elaborati per mezzo di vari processi. I particolari di questa elaborazione variano in base alla piattaforma del client dell'utente. Nel paragrafo 3.5 è stato descritto più in dettaglio tale procedimento per un sistema operativo Windows.
I due contributi vengono poi scambiati tra gli utenti sotto forma di crittogrammi RSA in modo che la chiave finale sia condivisa da entrambi. A questo punto le due parti vengono assemblate con un sistema di tipo cryptographically sound[2] per formare la chiave finale di sessione condivisa.

Un nodo cruciale nella sicurezza della comunicazione è, come più volte accennato, l'autenticazione degli utenti. Per raggiungere questo scopo Skype esegue un doppio controllo sull'identità.
Innanzitutto i peer si scambiano i propri Certificati d'Identità, in questo caso IC_A e IC_B, e ne accertano la validità. Poiché ogni Certificato è firmato dal Server Centrale con la chiave privata S_S, è possibile controllare l'autenticità utilizzando la chiave pubblica del Server V_S memorizzata nel client di ogni utente al momento dell'installazione.
Un'ulteriore verifica avviene al momento dell'avvio della sessione di comunicazione.
Il client A genera in modo casuale una sequenza di 64 bit, chiamata *challenge*, e la invia all'altro peer B. Il client di B modifica il challenge ricevuto con operazioni standard, il risultato, chiamato *response*, viene poi firmato con la chiave privata di B e rinviato all'utente di partenza A. L'utente A verifica la correttezza del response grazie alla chiave pubblica di B estrapolata dal Certificato d'Identità IC_B. Lo stesso iter è svolto da B nei confronti di A.
Questo viene eseguito più volte. Se si verificano errori la sessione viene bloccata, altrimenti si ha la conferma dell'identità dell'altro utente.
Tale meccanismo risulta analogo al protocollo SSH. In questo modo si ha l'autenticazione tra due utenti, senza che avvenga uno scambio di informazioni private attraverso un canale non ancora sicuro.

[2]Per sistema cryptographically sound si intende un sistema con una forza crittografica sufficiente da rendere un attacco crittoanalitico computazionalmente impraticabile.

3.8 La cifratura dei messaggi Skype

Per rendere segrete e private le comunicazioni tra utenti, Skype utilizza un sistema di cifratura avanzato. Come per la registrazione di un utente, anche in questo caso sono adoperati standard crittografici, combinati in modo tale da ottenere un risultato ottimale. Skype impiega il sistema crittografico Advanced Encryption Standard, AES.

Analizziamo in dettaglio la procedura per criptare i messaggi Skype.
Poiché AES è un cifrario a blocchi, il testo viene suddiviso in blocchi di 128 bit.
Ogni blocco viene cifrato con il sistema CRT.
La struttura classica del cifrario CRT è caratterizzata da un contatore (counter), della stessa lunghezza dei blocchi. Il contatore varia da blocco a blocco e solitamente la variazione è data dall'incremento di un'unità durante il passaggio ad un blocco successivo.
A questo punto avviene la cifratura: il contatore viene cifrato con un sistema crittografico, poi si applica la funzione XOR tra il contatore cifrato e il blocco del testo in chiaro.
L'operatore XOR somma due valori espressi in bit secondo le regole mostrate in tabella 3.1. Si osserva che questo operatore è equivalente alla somma mod 2.
Il risultato di tale meccanismo è un blocco cifrato.
Il processo di decifrazione è analogo alla cifratura. Innanzitutto è necessario considerare lo stesso contatore e lo stesso sistema crittografico utilizzati per la cifratura del messaggio considerato. Adoperando la funzione XOR tra il blocco del testo cifrato e il contatore cifrato, si ottiene il messaggio originale in chiaro.

Il CRT utilizzato da Skype ha un meccanismo del tutto analogo.
Il counter di Skype è una sequenza di 128 bit data dalla seguente concatenazione [8]:

$$salt : salt : packet\_index : block\#$$

dove

- ogni *salt* rappresenta un valore del tutto casuale di 32 bit ed entrambi i client coinvolti nella conversazione contribuiscono alla loro generazione;
- il *packet_index* è un valore di 48 bit che varia da buffer a buffer;
- il *block#* è un valore di 16 bit che varia da blocco a blocco.

Il contatore viene criptato, come da procedura standard CRT, e il sistema di cifratura utilizzato da Skype è proprio AES.
La chiave per avviare AES ha lunghezza 256 bit e corrisponde alla chiave condivisa di sessione SK_{AB}.
L'AES implementato da Skype è standard. Il crittografo Tom Berson e l'Anagram Laboratories [8] hanno confrontato l'AES di Skype con l'AES standard per mezzo di chiavi e

vettori test. I risultati ottenuti confermano la corrispondenza tra i due sistemi.
A questo punto del processo di cifratura, si applica la funzione XOR tra il blocco del testo in chiaro e il contatore cifrato con AES.
Si è ottenuto un blocco cifrato.
Passando a cifrare il blocco successivo, il contatore viene incrementato e solo i bit di ordine più basso subiscono un cambiamento. In questo modo l'unica parte del contatore che prevede una modifica è la variabile *block#*.
Si itera questo procedimento per tutti i blocchi del testo in chiaro del buffer.

Riassumendo, il procedimento di cifratura segue lo schema seguente:
$P_1 \otimes AES_{SK}(X_1) = C_1$;
$P_2 \otimes AES_{SK}(X_2) = C_2$;
...
$P_i \otimes AES_{SK}(X_i) = C_i$;
...
dove P_i rappresenta l'i-esimo blocco del testo in chiaro, X_i il contatore al passo i-esimo e C_i l'i-esimo blocco cifrato.

Al termine di tale operazione, vengono aggiunti due byte che sono direttamente legati alla cifratura dei blocchi precedenti.
Per determinare questi byte, infatti, viene calcolato il CRC sul messaggio cifrato precedentemente (in Appendice B verrà discusso il funzionamento del Controllo a Ridondanza Ciclica, CRC).
Poi, viene applicato l'operatore XOR tra il CRC appena calcolato e gli ultimi due byte della variabile chiamata *packet_index* che fa parte del contatore. Tale somma viene memorizzata negli ultimi due byte del buffer.
A questo punto si passa alla cifratura del buffer successivo e anche la variabile *packet_index* cambia, in quanto dipende dal buffer stesso.

Iterando il procedimento si ottiene la cifratura del messaggio originale scambiato tra due utenti Skype.

Tabella 3.1: Regole dell'operatore XOR

A	B	A xor B
0	0	0
0	1	1
1	0	1
1	1	0

Capitolo 4

Analisi sulla sicurezza di Skype

L'analisi sulla sicurezza del sistema Skype è resa complessa da molteplici fattori.
In primo luogo è necessario conoscere la sicurezza e la potenza dei computer utilizzati da entrambi gli utenti della conversazione, in quanto, come già visto, la chiave di sessione condivisa è creata equamente da entrambi i computer coinvolti. Bisogna poi tener conto che il sistema è di tipo peer-to-peer, quindi può verificarsi un attacco da parte di qualsiasi utente della rete. Inoltre, ad ogni accesso il software Skype controlla se ci sono aggiornamenti disponibili e, in caso affermativo, si aggiorna automaticamente. Ma il problema principale è dato dal protocollo proprietario e segreto. Le sole informazioni che si hanno provengono dalla società Skype, mentre le equipe di ricerca non autorizzate dalla compagnia non sono riuscite a estrapolare niente di nuovo e rilevante.

Comunque affinché un sistema VoIP sia considerato sicuro ed efficiente, devono essere soddisfatte alcune proprietà [10].

- Privacy

Il sistema deve impedire a terzi di ascoltare, disturbare, modificare la conversazione tra utenti.
Per questo motivo Skype cifra tutte le conversazioni attraverso protocolli e algoritmi, come analizzato nel capitolo precedente. Per rendere più robusto il sistema, viene cifrato anche il traffico in modo che sia difficoltoso individuarlo.
Tuttavia il sistema potrebbe presentare dei punti deboli. Per esempio, sebbene Skype non consenta la registrazione delle conversazioni vocali, tuttavia memorizza la messaggistica istantanea in un "history" file. Attraverso l'uso di spyware, o altre applicazioni, questo file potrebbe essere recuperato e letto da terzi. Un altro punto critico per la privacy si ha nei servizi di SkypeOut e SkypeIn. Quando la comunicazione viaggia attraverso la rete Internet, le informazioni e il traffico sono cifrati secondo gli standard Skype, ma, durante il passaggio alla rete telefonica tradizionale, la comunicazione viene decifrata ed è soggetta alle intercettazioni come una qualunque comunicazione telefonica.

- Autenticità

Il sistema deve garantire l'autenticazione degli username, ovvero, quando un utente comunica con un altro utente, deve avere la certezza di dialogare proprio con la persona indicata dallo username.
Il procedimento di verifica e di autenticazione di un utente avviene grazie al rilascio di un Certificato d'Identità da parte del Server di Autenticazione Skype secondo le modalità già descritte precedentemente. Ma anche in questo caso possono crearsi dei punti deboli nel sistema. Infatti esistono diversi metodi per attaccare le password, come analizzeremo in seguito.
Tuttavia, Skype è, prevalentemente, un sistema di comunicazione vocale e questo consente agli utenti un metodo di autenticazione aggiuntivo. In Skype la voce è biometrica, quindi una persona è identificabile anche dalla caratteristica vocale. Se poi si pensa alla videocomunicazione allora l'autenticazione è scontata, sempre che si conosca la voce e l'aspetto dell'utente con cui si comunica.

- Disponibilità

In generale il servizio Internet offre una minore disponibilità rispetto alla rete telefonica tradizionale PSTN. Sebbene Internet sia stato progettato in modo da risultare più efficiente rispetto alla linea tradizionale di comunicazione, la rete PSTN offre una disponibilità che raggiunge il 99,99905%.
Conseguentemente, anche Skype non può raggiungere risultati ottimali in questo ambito. Inoltre ci sono diversi aspetti che compromettono la sua disponibilità potenziale. Per esempio, se si verificassero problemi al Server Centrale di autenticazione, le comunicazioni verrebbero interrotte.

- Sopravvivenza

Se la rete Skype risulta danneggiata, la comunicazione deve essere comunque garantita e il sistema deve fare in modo che questa non venga interrotta.
Skype cerca sempre di connettere direttamente gli utenti tra loro. Ma, quando questo non risulta possibile, esso sfrutta la sua caratteristica rete peer-to-peer. Con l'ausilio dei supernodi, viene cercato il percorso alternativo più veloce ed efficiente possibile, così che la comunicazione possa avere successo.

- Elasticità

L'elasticità di una rete rispecchia la velocità con la quale la comunicazione viene ristabilita in caso di danneggiamento della rete stessa.
Skype, come già accennato, ha subito diversi crash dovuti a varie cause: da un numero eccessivo di login simultanei a un problema nell'aggiornamento di sistema. In questi casi i tecnici hanno presto ristabilito la rete grazie anche alla creazione di nuovi supernodi che hanno permesso nuovi collegamenti tra gli utenti e ripristinato, così, le comunicazioni.

- Integrità della conversazione

Un sistema VoIP deve fare in modo che i file trasmessi arrivino intatti ai destinatari e che non vengano persi pacchetti e informazioni durate la loro trasmissione.
Come per gli altri protocolli, anche in questo caso non si conoscono esattamente i mezzi adottati da Skype per controllare il proprio traffico. Tuttavia le misure analizzate nel capitolo precedente forniscono un quadro generale di come anche questo aspetto non venga trascurato. Un esempio è dato dall'uso del CRT per la cifratura dei messaggi. Il CRT adopera un contatore che permette al client di controllare l'esatta sequenza dei pacchetti cifrati, garantendo una verifica della corretta trasmissione e ricezione del messaggio.

- Integrità del sistema

Per studiare l'integrità del sistema si considera se e come Skype disturbi altre applicazioni presenti nel computer dell'utente.
In particolare il sistema può essere sfruttato da terzi come mezzo per infettare il client attraverso spyware. Tuttavia questo è un rischio che presentano anche altri software di tipo VoIP.
Per quanto riguarda invece l'integrità del sistema quando si utilizzano servizi di condivisione di file, è necessario comparare Skype con altri programmi di file-sharing, come KaZaA. Questi ultimi sono dotati di una protezione che scansiona i programmi scaricati dall'utente e rileva eventuali virus e programmi dannosi, anche perché la fonte da cui si scaricano i file può essere sconosciuta e non sicura. Skype non presenta tale meccanismo di protezione, ma in questo caso lo scambio di file avviene con utenti specifici e, si suppone, noti.

4.1 Attacchi al sistema Skype

Un modo per testare la forza di un sistema è simulare vari tipi di attacchi ai protocolli e studiare la loro efficacia.
L'equipe Anagram Laboratories guidata dallo studioso Tom Berson [8], ha effettuato diversi test a riguardo.

4.1.1 Attacchi al protocollo

Alcuni attacchi mirano a forzare il protocollo di autenticazione di un sistema in modo che l'attaccante possa essere scambiato per un altro utente.
Un esempio è dato dall'attacco *Man In The Middle*, MITM, con lo scopo di impersonare la figura del chiamante o del chiamato per accedere all'intera conversazione. In questo modo le informazioni passeranno dal mittente all'attaccante e poi al destinatario, e viceversa.
Per raggiungere questo obiettivo, però, l'avversario incontra diversi ostacoli dati dai meccanismi di sicurezza imposti da Skype.

Innanzitutto è necessario convincere il mittente/destinatario di essere il destinatario/mittente. Per fare ciò, l'utente ostile deve procurarsi il Certificato d'Identità degli altri utenti. Tale documento può essere una copia di quello reale, oppure lo stesso Certificato autentico.
Inoltre l'attaccante deve essere in grado di intercettare e bloccare tutto il traffico Skype della comunicazione senza destare sospetti.
Il Man In The Middle va ad intaccare direttamente il protocollo di autenticazione di Skype. Come già accennato, l'autenticazione di un utente Skype avviene per mezzo di un Certificato d'Identità rilasciato solo dal Server Centrale di Skype. Ed è sempre il Server Centrale che ne garantisce l'autenticità con la sua chiave privata. Siccome non si fa uso di autorità di certificazione esterne, tutti i passaggi di identificazione di un utente rimangono all'interno del sistema Skype, per cui risulta difficile per un utente malevolo falsificare un Certificato d'Identità.

Altri attacchi cercano di aggredire il protocollo sulla comunicazione tra due utenti, in modo da ricavare la chiave per la cifratura dei messaggi.
L'*attacco replay* rappresenta un esempio di questa tipologia. Il suo nome deriva dalla sua strategia di attacco.
Nel sistema Skype, al momento dell'avvio della sessione di comunicazione, il software esegue una verifica per accertare l'identità degli utenti. Precisamente, l'utente A genera in modo casuale una sequenza da 64 bit, chiamata *challenge* e la invia al secondo utente B. Questo modifica l'informazione ricevuta seguendo un iter standard proprio di Skype e invia l'esito, chiamato *response*, ad A che ne verifica la correttezza. Questo meccanismo viene ripetuto diverse volte e, se viene rilevato anche un solo errore, la sessione viene interrotta.
Lo scopo dell'attaccante è quello di inserirsi proprio al momento dell'avvio della comunicazione. Per fare ciò l'aggressore osserva e registra gli scambi di dati e informazioni tra l'utente con cui vuole comunicare e uno dei nodi interessati. In questo modo ha accesso a molteplici valori di *challenge* e ai suoi corrispettivi *response*. Questa parte dell'attacco è passiva, ma una volta registrato un numero sufficiente di dati, ha inizio la parte attiva. L'attaccante invia un *challenge* all'utente che rimanda il corrispondente *response*. Questa parte dell'autenticazione è sicuramente valida. Ora, è l'utente ad inviare un *challenge* per effettuare la seconda parte dell'autenticazione. Se il *challenge* che l'attaccante riceve è uguale a uno di quelli che ha precedentemente registrato allora il nemico risponde con il corrispondente *response* registrato, altrimenti la comunicazione fallisce.
La probabilità che tale coincidenza si verifichi è molto bassa. Poiché il *challenge* è scelto casualmente e ha lunghezza di 64 bit, la probabilità su N osservazioni fatte è di $N/2^{64}$.
Tuttavia, anche se il numero delle osservazioni è abbastanza alto e viene verificata la corrispondenza tra challenge e response, l'attaccante non entra ancora in possesso della chiave AES di decifrazione. Per la costruzione della chiave, ogni utente deve contribuire con una sequenza di 128 bit casuali che viene condivisa con il secondo utente. I due contributi vengono poi assemblati con un procedimento cryptographically suond.
Quindi, solo se i 128 bit scelti casualmente dall'utente corrispondono ad una delle sequenze

registrate precedentemente dall'attaccante, questo ha la possibilità di conoscere la chiave di cifratura finale. Ma la probabilità che questo si verifichi su N osservazioni fatte è di $N/2^{128}$; una aspettativa ancora più bassa.

4.1.2 Attacchi alla password

Esistono vari metodi per tentare di scoprire la password di un utente: dall'ingegneria sociale, che attraverso le informazioni sulla vita dell'utente studia varie combinazioni possibili, al cosiddetto "attacco del dizionario", che consiste nel provare con ogni parola presente nel dizionario. Per questi motivi è necessario fare molta attenzione nella scelta della password, preferendo una combinazione di caratteri e numeri non facilmente ricavabile. Il Server Centrale di Skype, per prevenire questi attacchi, consente solo un numero limitato di tentativi.
Quando viene persa una password, si ha la possibilità di chiedere al sistema Skype una e-mail con la password recuperata. Ma questo servizio può risultare anche dannoso per un utente se la mail con il recupero della password viene intercettata da un utente nemico.
Skype fornisce anche un altro servizio: la memorizzazione della propria password nella piattaforma del computer che si sta utilizzando. Per esempio in piattaforme Windows, la password viene protetta con l'applicazione Windows CryptProtectData. Così, utilizzando quel computer, un utente può accedere a Skype senza dover digitare ogni volta la password. Tuttavia se il computer viene preso da terzi, questo avrà la possibilità di accedere all'account Skype dell'utente originario senza neanche inserire la password.
Un altro tipo di attacco che mira a ricavare la password di un utente è dato da programmi di keystroke loggers, che controllano costantemente la tastiera dell'utente memorizzando ogni digitalizzazione fatta. La difesa da questi attacchi, però, non compete a software come Skype ma dipende solo da una efficace protezione del computer.

4.1.3 Attacchi alla crittografia

Alcuni attacchi mirano a colpire direttamente l'apparato crittografico del sistema, cercando di sfruttarne i punti deboli.
Un esempio è dato dall'algoritmo di Controllo a Ridondanza Ciclica, CRC, che viene utilizzato per individuare in modo affidabile ed efficiente eventuali bit di errore che si possono presentare durante una comunicazione. Il CRC ha un approccio lineare e questo, se da una parte gli conferisce una maggiore semplicità, dall'altra può essere sfruttato da terzi per creare disordine inserendo intenzionalmente degli errori nei messaggi.
Questo problema è stato scoperto nel WEP, una parte dello standard IEEE 802.11 che specifica il protocollo per rendere sicure le trasmissioni delle reti Wi-Fi.
In molti aspetti, Skype utilizza il CRC in modo analogo al WEP e quindi anche i punti deboli sono simili.
Un altro punto debole è stato trovato dal gruppo di "code breakers"guidato da Sean O'Neil,

specialista nell'infrazione di codici segreti[11], che ha dichiarato di aver ricostruito l'implementazione dell'algoritmo RC4 utilizzato da Skype per la creazione di chiavi RSA. Il risultato è stato raggiunto grazie ad una sofisticata operazione di reverse-engineering che, procedendo a ritroso, consente di ricostruire passo dopo passo l'algoritmo in esame.
Ma nonostante questo, non si può di certo affermare che la sicurezza dell'intero sistema di comunicazione Skype sia compromessa. Infatti questi due algoritmi non sono direttamente responsabili della cifratura dei messaggi.
Ma può succedere che, in un sistema, un punto debole sia intrinseco al sistema stesso. Infatti, le implementazioni crittografiche consentono una trasmissione sicura dei messaggi, ma, possono anche creare dei danni al messaggio stesso. Per esempio possono andare persi dei bit del messaggio o della chiave. Contro tale inconveniente, che assale tutti i sistemi che usano la crittografia, non ci sono difese.
In più, un utente malevole potrebbe approfittare della situazione. Se nella piattaforma sulla quale lavora Skype è presente un programma maligno, questo potrebbe avere la possibilità di conoscere alcuni bit perfino della chiave privata dell'utente.
Tuttavia, bisogna precisare che un programma maligno può causare danni direttamente al client dell'utente, molto più gravi di quello appena descritto.

4.2 Intercettazioni

Sono stati studiati diversi attacchi alla sicurezza del sistema ed è stato osservato che tali attacchi non sono pienamente efficaci.
Questo, da una parte tutela la privacy degli utenti, ma dall'altra può essere sfruttata da malavitosi per organizzare i propri traffici in tutta sicurezza.
Infatti, dalle intercettazioni telefoniche di polizia ed FBI è risultato che i clan mafiosi utilizzano le classiche telefonate solo per decidere su account, banda larga e altre informazioni necessarie per collegarsi attraverso Internet, poi rimandano su Skype quelli che loro chiamano gli "altri discorsi". La frase simbolo che esprime la rivoluzione nelle comunicazioni anche di tipo mafioso è stata intercettata dagli uomini della Guardia di Finanza di Milano: "di quei due chili ne parliamo poi, su Skype" [12].
Un tecnico che collabora con la procura di Milano ha affermato che "Skype è riuscita a portare il proprio sistema di sicurezza a livelli militari, assolutamente lontani da quelli degli altri software creati per fare telefonate attraverso Internet. Ciò rende impossibile agli investigatori ogni tentativo di intercettazione" [12]. Inoltre sui tabulati non rimane traccia delle conversazioni Skype, così non si può sapere né quando né dove vengono fatte. È come se le chiamate Skype fossero invisibili.
La Direzione investigativa antimafia, insieme ad altri apparati, sta facendo diversi tentativi per cercare una soluzione a questo problema. Innanzitutto è stata chiesta la collaborazione di Skype. Ma la sua sede legale si trova in Lussemburgo, quindi la società non è soggetta alla normativa italiana del Codice di Comunicazione, che prevede su ordine della magistra-

tura, l'obbligo da parte degli operatori a violare la segretezza delle comunicazioni tra due privati cittadini.
Vista la mancanza di risultati, è stata intrapresa la via della rogatoria internazionale. Ma Stefano Aterno, docente di informatica forense e criminologia informatica all'Università la Sapienza di Roma, afferma che questa è "una strada impervia, in quanto capita spesso che Skype dica di non essere in grado o di non voler mettere a disposizione la tecnologia necessaria a decrittare le conversazioni. E il tutto si risolve in una grande perdita di tempo" [12].
Gli investigatori cercano, allora, di contenere i danni provocati da questa non collaborazione, utilizzando dei metodi alternativi. Per esempio, prima si ricorre alle intercettazioni ambientali che cercano di individuare i terminali utilizzati nella conversazione, poi, attraverso vari espedienti, vengono installate delle microspie nelle attrezzature, come cuffie, microfoni, tastiera, che permettono agli inquirenti di ascoltare le conversazioni che avvengono nell'ambiente circostante e non solo attraverso Skype.
Il problema è che non sempre è possibile individuare i terminali utilizzati perché, come detto, le chiamate Skype risultano invisibili sui tabulati. A volte anche se il terminale viene individuato, questo risulta essere un Internet Point oppure un cellulare.

Altre scorciatoie per intercettare le conversazioni Skype senza doversi confrontare con il sistema crittografico, sono state trovate dal programmatore Ruben Unteregger per conto dell'azienda svizzera ERA IT Solution [13].
Si tratta di due trojan, chiamati minipanzer e megapanzer, in grado di interfacciarsi con le API di Skype e registrare il flusso audio sia in entrata che in uscita, in un file MP3.
Il nodo cruciale sta in quel breve momento in cui le parole non sono ancora cifrate e, viceversa, appena le parole vengono decifrate. In quel frangente il cavallo di troia registra il flusso audio e lo comprime in formato MP3. L'operazione di registrazione non è rilevante in termini di prestazioni per il computer e lo scarso spazio occupato dai file MP3 fa sì che l'intero attacco non venga notato dall'utente. Inoltre il trojan, aprendo una backdoor, permette all'attaccante di scaricare i file audio ottenuti e anche di cancellare ogni traccia dell'infezione.
Questo programma però, ha efficacia solo in mancanza di antivirus.

Non solo in Italia ma anche all'estero si registra la stessa emergenza sulle intercettazioni Skype.
Nel 2005 il Ministero Francese della Ricerca, su consiglio della Segreteria Generale della Difesa Nazionale, ha espresso la sua disapprovazione sull'uso di Skype sia in ambito lavorativo che in quello educativo. La Francia è caratterizzata da una forte campagna anti-Skype, tanto che il sito francese "IS Decisions" ha pubblicato SkypeKiller: un software gratuito che permette di bloccare l'applicazione Skype nei computer dove è installato.
Anche gli Stati Uniti hanno cercato di convincere Skype a cooperare con le autorità.
Nel Maggio 2006 la Federal Communications Commission, FCC, ha approvato l'applica-

zione di legge che consente le intercettazioni. Ma Skype ha rifiutato di aderire.
Tuttavia in Cina la politica adottata da Skype è diametralmente opposta. Qui, insieme ad altre compagnie, come Google, Microsoft e Yahoo, la società coopera con il governo cinese per ceare un sistema di censura di Internet. Per effettuare il controllo sulla comunicazione, la compagnia Internet cinese TOM Online installa un filtro a qualunque società voglia usufruire del servizio Internet offerto. Per questa scelta Skype è stata duramente criticata, ma, lo stesso Niklas Zennström, uno dei fondatori del software Skype, ha affermato che "queste sono le regole. Mi possono piacere oppure non piacere le leggi e le regole per fare business nel Regno Unito o in Germania o negli Stati Uniti, ma se io faccio affari lì allora scelgo di attenermi a quelle leggi e regole. Posso provare ad influenzarli per cambiare, ma ho bisogno di attenermi alle loro leggi. La Cina non fa eccezione" [5].

Ma il problema delle intercettazioni sembra aver preso una svolta decisiva.
Nel Giugno 2011 l'Ufficio Brevetti e Marchi degli Stati Uniti ha approvato il brevetto Legal Intercept di Microsoft [16], depositato nel 2009 due anni prima dell'acquisizione di Skype. Questo software dovrebbe permettere l'intercettazione delle comunicazioni VoIP e in particolare di quelle che avvengono con Skype. Precisamente, i dati vengono alterati in modo che seguano un percorso alternativo che include un agente di registrazione in grado di registrare silenziosamente la comunicazione.
Ma è nel Marzo 2012 che Microsoft rivoluziona la struttura della rete Skype.
In precedenza il numero di supernodi era, in media, di 48.000, e ognuno gestiva circa 800 utenti. Secondo uno studio effettuato da Kostya Kortchinsky e confermato parzialmente da Mark Gillet, un ingegnere Skype, attualmente si hanno poco più di 10.000 supernodi Linux controllati direttamente da Microsoft. Ognuno di questi supernodi supervisiona mediamente 4.100 utenti ma il limite massimo teorico raggiunge i 100.000 utenti.
Microsoft giustifica questa rivoluzionaria operazione col miglioramento del sistema a livello di prestazioni e disponibilità. Questa motivazione viene avvalorata dallo stesso Kortchinsky, secondo il quale la nuova architettura garantisce una maggiore sicurezza della rete. Infatti in un supernodo scelto casualmente può essere presente un software malevolo, ma questo sicuramente non si verifica se il supernodo è controllato. Di parere contrario sono alcuni esperti di sicurezza, che vedono in questa drastica riduzione del numero dei supernodi una maggiore opportunità per controllare e intercettare le comunicazioni.
Il 26 Luglio 2012 il Washington Post pubblica un articolo nel quale rivela la nuova politica di gestione della sicurezza Skype. Microsoft annuncia di voler cooperare con i governi, rendendo accessibili le conversazioni delle chat Skype, la cronologia dei messaggi e i dati personali degli utenti. Tuttavia, Microsoft garantisce che il contenuto delle chiamate audio e video rimarranno non intercettabili. Ma lo stesso Washington Post si interroga per quanto ancora le telefonate saranno inaccessibili, visto che Skype è tuttora un servizio in forte espansione.

Con l'apertura di Microsoft alle intercettazioni legali, viene meno la filosofia originaria di Skype. Questo innovativo sistema VoIP, nato per consentire chiamate private e a basso costo, attraverso varie acquisizioni da parte di importanti multinazionali, ha perso la battaglia sulla non intercettabilità delle comunicazioni cedendo alle pressioni dei Governi.
Nonostante ciò, Skype rimane un sistema estremamente sicuro da attacchi e intercettazioni da parte di malintenzionati, e il fatto che la Magistratura debba chiedere il consenso a Microsoft per ottenere le informazioni, conferma questa tesi.
Il grande merito di Skype rimane quello di aver introdotto un nuovo modo di comunicare, essendo il primo sistema VoIP con una rete peer-to-peer, ed il continuo e crescente successo ne dimostra la validità.

Appendice A

A.1 La distribuzione Heavy-Tailed

Una distribuzione di tipo heavy-tailed appartiene ad una famiglia di distribuzioni di probabilità le cui code sono più pesanti rispetto ad una distribuzione esponenziale, quindi, all'infinito, le code tendono a zero più lentamente.
Per avere una distribuzione heavy-tailed non è necessario che entrambe le code siano pesanti. In molte applicazioni è la coda destra della distribuzione, che è anche quella di maggiore interesse statistico, ad essere pesante, mentre in altri casi è la coda di sinistra a tendere a zero più lentamente.

Attraverso il grafico A.1 è possibile confrontare una distribuzione heavy-tailed, rappresentata da una distribuzione t di Student, con una distribuzione esponenziale, nello specifico una distribuzione normale standard.
In questo modo è possibile osservare direttamente le differenze tra le due distribuzioni. All'infinito, la distribuzione t di Student tende a zero più lentamente rispetto a quella normale, ed entrambe le code risultano più pesanti.

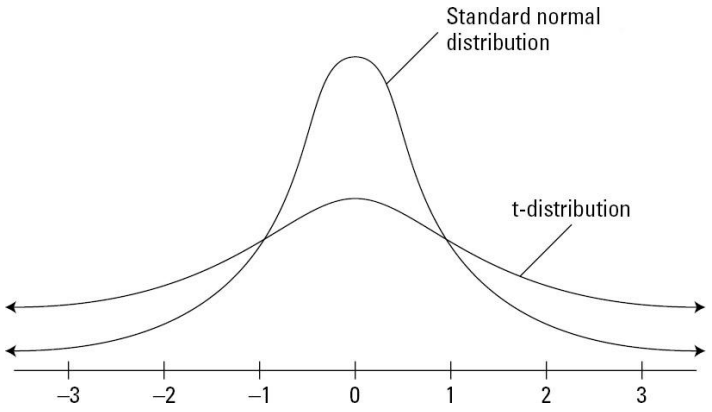

Figura A.1: Confronto tra una distribuzione haevy-tailed e una distribuzione esponenziale

Un esempio di distribuzione heavy-tailed, infatti, è la distribuzione t di Student. Questa è una distribuzione di probabilità continua che gestisce due variabili aleatorie, le quali presentano andamenti diversi: la prima variabile segue una distribuzione normale standard mentre la seconda è tale che il suo quadrato presenta distribuzione chi-quadro. Quindi, se considero Z e S^2 due variabili aleatorie indipendenti con, rispettivamente, distribuzione normale standard $N(0,1)$ e distribuzione chi-quadro $\chi^2(n)$, allora la distribuzione t di Student rappresenta la seguente variabile aleatoria:

$$T = \frac{Z}{\sqrt{\frac{S^2}{n}}}$$

A.2 La distribuzione di Poisson

La distribuzione di Poisson è una distribuzione di probabilità discreta che descrive una classe di eventi indipendenti in un dato intervallo di tempo.

Precisamente, sia X la variabile aleatoria che indica il numero di volte in cui si verifica un evento in un dato intervallo di tempo, ossia il numero di successi, allora la probabilità che X assuma il valore $k \in \mathbb{N}$ è data dalla distribuzione di Poisson:

$$f(k) = P(X = k) = e^{-\lambda} \frac{\lambda^k}{k!}$$

dove $\lambda > 0$ è il parametro della distribuzione e rappresenta il numero medio di successi nell'intervallo di tempo considerato.

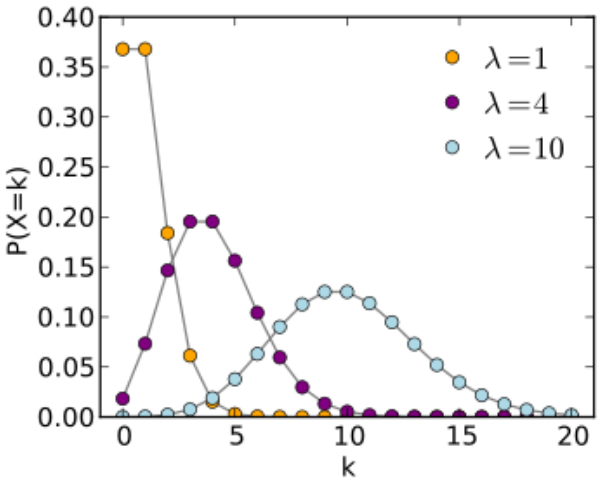

Figura A.2: Distribuzione di Poisson con diversi parametri λ

Appendice B

B.1 RC4

L'algoritmo RC4 è stato ideato nel 1987 da Ronald Rivest, il crittofrafo che ha contribuito anche alla creazione nel sistema RSA. Infatti, RC è semplicemente l'acronimo di Rivest Cipher.
L'RC4 è un algoritmo che genera un flusso di bit pseudo-casuali grazie alla combinazione di due algoritmi: RC4-KSA e RC4-PRGA.

Analizziamo il primo algoritmo.
L'RC4-KSA inizializza un vettore S da 256 elementi, composto dai valori crescenti da 0 a 255: $S[0] = 0; \quad S[1] = 1; \quad S[2] = 2; \quad \ldots \quad S[255] = 255$.
Il cuore dell'algoritmo scambia due elementi di S con l'ausilio di una chiave key fornita in input, la cui lunghezza (keylength) può variare da 40 a 256 bit. In totale vengono effettuati 255 scambi, ovvero swap.
Per maggiori dettagli si riporta lo pseudocodice [14].

```
for i = 0 to 255
   S[i] = i
next
j = 0
for i = 0 to 255
   j = (j + S[i] + key[i mod keylength]) mod 256
   swap (S[i], S[j])
next
```

L'RC4-KSA ha terminato il suo compito: la gestione della chiave, ovvero Key-Scheduling Algorithm (KSA).
Il vettore finale altro non è che un rimescolamento degli elementi di S, e costituirà l'input dell'algoritmo successivo.

Il secondo algoritmo, l'RC4-PRGA, si occupa della generazione dei numeri pseudo-casuali. Infatti, PRGA è l'acronimo di Pseudo-Random Generation Algorithm.
Lo speudocodice [14] seguente chiarisce gli swap e gli artifici usati per generare numeri pseudo-casuali a partire dal vettore S modificato dall'RC4-KSA.

```
for i = 0 to 255
   i = (i + 1) mod 256
   j = (j + S[i]) mod 256
   swap (S[i], S[j])
   return S[(S[i] + S[j]) mod 256]
next
```

L'algoritmo RC4 può essere utilizzato anche per cifrare un testo.
In questo caso il flusso di numeri pseudo-casuali viene combinato mediante l'operazione XOR con il testo in chiaro, ottenendo così il testo cifrato.
Poiché l'operatore XOR è simmetrico, il processo di decifrazione è analogo a quello di cifratura.

B.2 CRC

Il controllo a ridondanza ciclica, Cyclic redundancy check, è un metodo per il calcolo di checksum, cioè di sequenze di bit che, associate al pacchetto trasmesso, permettono di verificare la presenza di errori di trasmissione. Questo metodo risale al 1961 per opera di W. Wesley Peterson.

Il codice CRC è caratterizzato da un particolare polinomio chiamato polinomio generatore, che indico $g(x)$ con grado g. In base al polinomio utilizzato si distinguono diversi tipi di CRC:

- CRC-12: $g(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$
- CRC-16: $g(x) = x^{16} + x^{15} + x^2 + 1$
- CRC-16-CCITT: $g(x) = x^{16} + x^{12} + x^5 + 1$

In ogni caso il funzionamento del codice non subisce variazioni [15].
Al messaggio di n bit da trasmettere, viene associato un polinomio $b(x)$ di grado $n-1$.
Viene poi costruito il polinomio $p(x)$ mediante l'operazione: $p(x) = x \cdot g \cdot b(x)$
Sostanzialmente $p(x)$ si ottiene traslando a sinistra $b(x)$ di g posizioni, ovvero sommando ogni esponente del polinomio $b(x)$ con il valore di g. Il grado di $p(x)$ è dato da $h = n-1+g$.
Successivamente, grazie alla divisione modulo 2 tra $p(x)$ e $g(x)$, si definiscono altri due polinomi: il quoziente $q(x)$ e il resto $r(x)$.

Il messaggio trasmesso attraverso il canale di comunicazione sarà dato dai coefficienti di un ulteriore polinomio $m(x)$ ottenuto sottraendo a $p(x)$ il polinomio $r(x)$: $m(x) = p(x) – r(x)$

Vediamo il motivo per cui il polinomio $m(x)$ rappresenta il messaggio originario e permette di verificare la presenza di errori di trasmissione.
Il polinomio $p(x)$ si può rappresentare anche attraverso la divisione vista precedentemente:
$p(x) = q(x) \cdot g(x) + r(x)$
Sostituendo questa nuova scrittura nella definizione di $m(x)$ si ottiene:
$m(x) = q(x) \cdot g(x) + r(x) – r(x)$
Per le leggi dell'algebra sui campi finiti, sottraendo un polinomio a sé stesso si ottiene il polinomio nullo, quindi: $m(x) = q(x) \cdot g(x)$
Cioè il messaggio finale $m(x)$ è divisibile per il polinomio generatore $g(x)$ con resto nullo. Questa è la caratteristica fondamentale utilizzata per verificare la presenza di errori di trasmissione.
L'utente destinatario infatti, divide il messaggio ricevuto $m(x)$ con il polinomio generatore $g(x)$ del CRC utilizzato, e ne controlla il resto. Se la divisione modulo 2 produce resto allora il messaggio presenta degli errori dovuti al rumore di fondo del canale di trasmissione, altrimenti il messaggio è arrivato a destinazione integro. In quest'ultimo caso, per ottenere il messaggio originale, rappresentato da $b(x)$, è sufficiente traslare $m(x)$ verso destra del valore del grado g.

Il codice CRC è molto diffuso, in quanto è matematicamente semplice ed efficiente per la rilevazione di errori di trasmissione. Tuttavia, proprio la sua semplicità impedisce al codice CRC di riconoscere manomissioni intenzionali dovuti ad attacchi esterni.

Bibliografia

[1] http://www.telecompaper.com/news/skype-grows-fy-revenues-20-reaches-663-mln-users

[2] http://news.hitb.org/content/skype-tightening-security-reducing-supernodes

[3] S. Guha, N. Daswani e R. Jain (2006)
An Experimental Study of the Skype Peer-to-Peer VoIP System
http://saikat.guha.cc/pub/iptps06-skype

[4] http://en.wikipedia.org/wiki/Skype_protocol

[5] http://en.wikipedia.org/wiki/Skype_Technologies

[6] F. Risso
Introduzione alla rete Skype
http://netgroup.polito.it/teaching/tsr/Skype.pdf

[7] S. A. Baset e H. Schulzinne (2004)
An Analysis of the Skype Peer-to-Peer
http://www1.cs.columbia.edu/∼library/TR-repository/reports/reports-2004/cucs-039-04.pdf

[8] T. Berson (2005)
Skype Security Evaluation
http://www.anagram.com/berson/skyeval.pdf

[9] http://www.mail-archive.com/cryptography@c2.net/msg00613.html

[10] S. L. Garfinkel (2005)
VoIP and Skype Security
http://skypetips.internetvisitation.org/files/VoIP%20and%20Skype.pdf

[11] http://www.ilsole24ore.com/art/tecnologie/2010-07-15/codici-skype-mirino-maroni-080532.shtml?uuid=AYQAxw7B

[12] http://www.spysystem.it/portale/wi-fi/67-skype-rende-impossibili-le-intercettazioni.html

[13] http://punto-informatico.it/2700193/PI/News/skype-intercettare-si-puo.aspx

[14] http://it.wikipedia.org/wiki/RC4

[15] http://it.wikipedia.org/wiki/Cyclic_redundancy_check

[16] http://windows.digital.it/ microsoft-consentira-le-intercettazioni-su-skype-4053.html