Università degli Studi di Verona

FACOLTÀ DI SCIENZE E INGEGNERIA
Corso di Laurea in Informatica

Whatsapp Messenger

Candidato:
Alberto Marini
Matricola VR359129

Relatore:
Prof. Damiano Carra

Anno Accademico 2013 - 2014

Indice

Capitolo 1

Introduzione

Capitolo 2

Strumenti utilizzati

2.1 Whatsapp Messenger

2.1.1 Cos'è

WhatsApp Messenger è un'app di messaggistica mobile multi-piattaforma che consente di scambiarsi messaggi coi propri contatti senza dover pagare gli SMS. WhatsApp Messenger è disponibile per iPhone, BlackBerry, Android, Windows Phone e Nokia. La risposta è sì: tutti questi telefoni possono scambiarsi messaggi gli uni gli altri! Dato che WhatsApp Messenger si serve dello stesso piano dati Internet usato per le e-mail e la navigazione web, non vi sono costi aggiuntivi per mandare messaggi e restare in contatto coi propri amici.

Oltre alla messaggistica di base gli utenti di WhatsApp possono creare gruppi, scambiarsi messaggi illimitati, video e messaggi audio multimediali.

L'11 aprile 2014 e' arrivato il via libera all'acquisizione di WhatsApp da parte di Facebook dalla Federal Trade Commission (Ftc), l'ente governativo americano per la protezione dei consumatori.

2.1.2 Come funziona

Come funzionaCome funzionaCome funzionaCome funzionaCome funziona-Come funzionaCome funzionaCome funzionaCome funzionaCome funziona-Come funzionaCome funzionaCome funzionaCome funzionaCome funziona-Come funzionaCome funzionaCome funzionaCome funzionaCome funziona-Come funzionaCome

funzionaCome funzionaCome funzionaCome funzionaCome funzionaCome funzionaCome funzionaCome funzionaCome funzionaCome funzionaCome funzionaCome funzionaCome funzionaCome funzionaCome

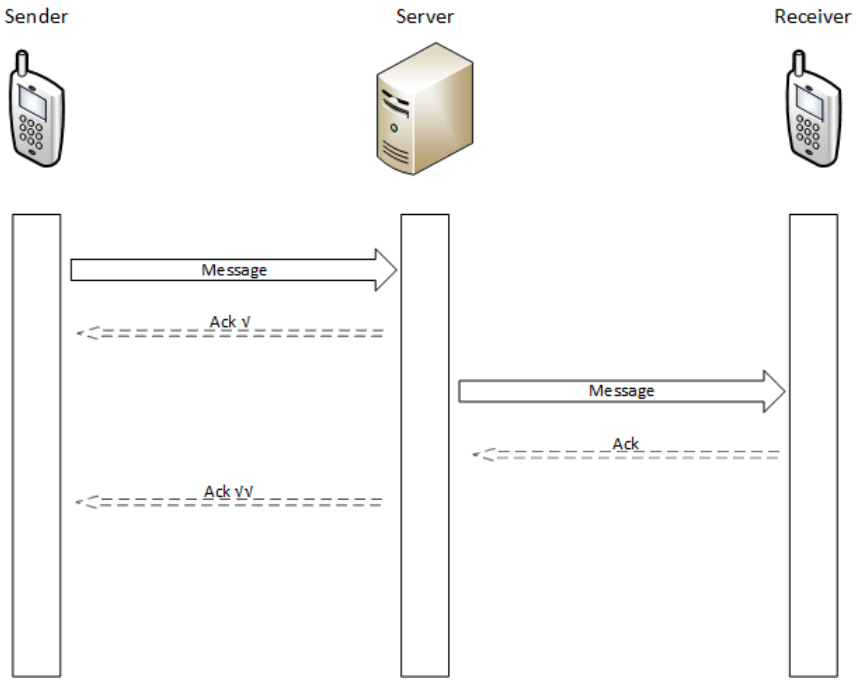

Figura 2.1: Funzionamento Whatsapp

2.2 Wireshark

2.2.1 Cos'è

Wireshark è un analizzatore di rete. It lets you interactively browse packet data from a live network or from a previously saved capture file. Inizialmente, il formato dei file catturati da Wireshark era l formato libpcap, che è il formato usato da tcpdump ed altri tools.

Wireshark può leggere/importare i seguenti formati di file:

- *libpcap - captures from Wireshark/TShark/dumpcap, tcpdump, and various other tools using libpcap's/tcpdump's capture format*
- *pcap-ng - next-generation successor to libpcap format*
- *snoop and atmsnoop captures*
- *Shomiti/Finisar Surveyor captures*
- *Novell LANalyzer captures*
- *Microsoft Network Monitor captures*
- *AIX's iptrace captures*
- *Cinco Networks NetXRay captures*
- *Network Associates Windows-based Sniffer captures*
- *Network General/Network Associates DOS-based Sniffer (compressed or uncompressed) captures*
- *AG Group/WildPackets EtherPeek/TokenPeek/AiroPeek/EtherHelp/PacketGrabber captur*es
- *RADCOM's WAN/LAN analyzer captures*
- *Network Instruments Observer version 9 captures*
- *Lucent/Ascend router debug output*
- *files from HP-UX's nettl*
- *Toshiba's ISDN routers dump output*
- *the output from i4btrace from the ISDN4BSD project*
- *traces from the EyeSDN USB S0.*
- *the output in IPLog format from the Cisco Secure Intrusion Detection System*

- *pppd logs (pppdump format)*
- *the output from VMS's TCPIPtrace/TCPtrace/UCX$TRACE utilities*
- *the text output from the DBS Etherwatch VMS utility*
- *Visual Networks' Visual UpTime traffic capture*
- *the output from CoSine L2 debug*
- *the output from InfoVista's 5View LAN agents*
- *Endace Measurement Systems' ERF format captures*
- *Linux Bluez Bluetooth stack hcidump -w traces*
- *Catapult DCT2000 .out files*
- *Gammu generated text output from Nokia DCT3 phones in Netmonitor mode*
- *IBM Series (OS/400) Comm traces (ASCII Et UNICODE)*
- *Juniper Netscreen snoop files*
- *Symbian OS btsnoop files*
- *TamoSoft CommView files*
- *Textronix K12xx 32bit .rf5 format files*
- *Textronix K12 text file format captures*
- *Apple PacketLogger files*
- *Files from Aethra Telecommunications' PC108 software for their test instruments*

Non è necessario dire a Wireshark il formato dei file da leggere; lo determina automaticamente. Wireshark is also capable of reading any of these file formats if they are compressed using gzip. Wireshark recognizes this directly from the file; the '.gz' extension is not required for this purpose.

A differenza di altri analizzatori di protocolli, la finestra di Wireshark mostra 3 viste dei pacchetti. It shows a summary line, briefly describing what the packet is. A packet details display is shown, allowing you to drill down to exact protocol or field that you interested in. Finally, a hex dump shows you exactly what the packet looks like when it goes over the wire.

In aggiunta, Wireshark ha alcune features che lo rendono unico. Può assemblare tutti i pacchetti in una comversazione TCP e visualizzare i dati

ASCII (o EBCDIC, o hex) in questa conversazione. Display filters in Wireshark are very powerful; more fields are filterable in Wireshark than in other protocol analyzers, and the syntax you can use to create your filters is richer. As Wireshark progresses, expect more and more protocol fields to be allowed in display filters.

I pacchetti catturati sono conformi alla libreria pcap. I filtri applicabili ai pacchetti seguono le regole della libreria pcap. This syntax is different from the display filter syntax.

Compressed file support uses (and therefore requires) the zlib library. If the zlib library is not present, Wireshark will compile, but will be unable to read compressed files.

Il nome dei file catturati può essere specificato trmite l'opzione -r oppure come argomento da riga di comando. Wireshark and TShark share a powerful filter engine that helps remove the noise from a packet trace and lets you see only the packets that interest you. If a packet meets the requirements expressed in your filter, then it is displayed in the list of packets. Display filters let you compare the fields within a protocol against a specific value, compare fields against fields, and check the existence of specified fields or protocols.

2.3 Whois

Capitolo 3

Rilevazioni