Suportul de comunicatie pentru cross-platform,

 WhatsApp

**Ce este WhatsApp?**

WhatsApp este o aplicație de mesagerie multiplatformă pentru telefoanele mobile, ce permite atât expedierea mesajelor, imaginilor, fisierelor audio sau video între utilizatori, precum și realizarea de apeluri video prin intermediul conexiunii la serviciul de date mobile.În ciuda faptului că, începând din ianuarie 2016, aplicația a devenit gratuită pentru toți utilizatorii, aceasta încă se diferențiază prin faptul că nu publică reclame în cadrul interfeței de utilizator.

Lansat în anul 2009 pentru dispozitivele iPhone, WhatsApp a ajuns să fie disponibil de-a lungul anilor, pentru o gama largă de platforme, precum Symbian, Android, Windows Phone și BlackBerry. În anul 2015, aplicația a fost făcuta disponibilă pentru PC printr-un web client numit WhatsApp Web. Aceasta rulează pe majoritatea browserelor, cu excepția Internet Explorer, sincronizând conversațiile și contactele de pe dispozitivele mobile.

**Protocoale folosite**

Aplicația folosește o variantă modificată a protocolului XMPP (Extensible Messaging and Presence Protocol). Bazat pe XML, XMPP este un protocol de nivel de aplicație, folosit pentru schimbul de date, într-un timp cât mai scurt, între două sau mai multe dispozitive. Spre deosebire de majoritatea protocoalelor de mesagerie rapidă, XMPP este definit de un standard deschis, permițând oricărui individ să implementeze un astfel de serviciu și să se folosească de alte implementări ale sale.

Pe lângă avantajul unui standard deschis, XMPP conține facilități pentru sporirea siguranței precum autentificarea prin SASL (Simple Authentication and Security Layer) și criptarea datelor prin protocolul TSL(Transport Layer Security).

TSL, unul dintre cele mai folosite protocoale pentru securizarea datelor, permite aplicațiilor să comunice într-un mod ce împiedică interceptarea conversației, folosind o procedură de tip handshake, astfel:

* Un client se conectează la un server ce folosește TSL, solicitând o conexiune securizată și oferind o listă cu cifrele și funcțiile hash suportate
* Serverul alege din listă un cifru și o funcție hash și înștiințează clientul aupra deciziei făcute
* Serverul trimite înapoi informațiile de identificare sub forma unui certificat digital, ce conține numele serverului, cheia publică de criptare a serverului și numele entității care a emis certificatul digital
* Clientul confirmă validitatea certificatului
* Pentru generarea cheilor folosite pentru o conexiune securizată clientul criptează cheia publică a serverului și îi trimite acestuia rezultatul, urmând să îl folosească ambele entități pentru criptarea/decriptarea datelor în timpul sesiunii

**Mod de funcționare**

Aplicația funcționează pe baza numărului de telefon al utilizatorului, creând un cont de forma „[numar\_de\_telefon]@s.whatsapp.net”, odată cu instalarea pe dispozitiv. Programul compară automat toate numerele din agenda utilizatorului cu o bază de date centrală pentru a adăuga persoane în lista de contacte WhatsApp.

Versiunile anterioare se foloseau fie de o variantă codificată a codului IMEI al telefonului, fie de adresa MAC a modulului Wi-Fi pe post de parolă. Începând cu 2012, parola a fost generată în mod aleator de către server.

Mecanismul de transmitere al unui mesaj între două dispozitive este de tip „store and formward”. Atunci când un utilizator trimite un mesaj, acesta ajunge, mai întâi, la serverul WhatsApp, unde este memorat. Dupa aceea, serverul trimite mai departe mesajul către destinație și trimite, în mod repetat, cererea pentru înștiințarea primirii mesajului (acknowledge). De îndată ce înștiințarea a fost primită, serverul șterge mesajul din memorie. În cazul neprimirii mesajului de acknowledge, serverul va șterge automat mesajul după 30 de zile.

**Evoluția soluțiilor tehnice folosite**

Una dintre marile probleme cu care s-au confruntat dezvoltatorii aplicației WhatsApp a fost legată de securitate. Cu toate că aplicația se folosea de protocolul XMPP, conversațiile utilizatorilor nu erau criptate, datele trimise și recepționate putând fi ușor interceptate și citite. Diverși indivizi au făcut publice diverse metode prin care exploatau această slăbiciune, precum: schimbarea statusului unui utilizator, cunoscându-i doar numărul de telefon sau terminarea aplicației pe telefonul destinatarului printr-un mesaj special codificat. Problemele au fost rezolvate definitiv în 2014, când, după multe update-uri ale aplicației în care s-a încercat introducerea de metode de criptare a datelor, dezvoltatorii au realizat un parteneriat cu One Whisper Systems în urma căruia avea să se introducă protocolul de criptare folosit de aplicația TextSecure.

**Concluzii**

În concluzie, Whatsapp reprezintă o bună alternativă la serviciile SMS ale operatorilor de telefonie mobilă, mesajele fiind trimise rapid si la un cost redus utilizând conexiunea de date a dispozitivului. De asemenea, introducerea de noi funcționalități de-a lungul timpului pentru sporirea securității, precum și îmbunătățirea interfeței grafice, au ajutat la creșterea numărului de utilizatori, ajuns până în acest moment la un miliard. Cu toate acestea, după cumpărarea de către Facebook, s-a renunțat la tarifarea anuală a utilizatorilor cu 1$, aceasta fiind singura metodă de valorificare a aplicației, din moment ce reclamele nu sunt folosite pentru a produce venituri.

**Bibliografie**

<https://en.wikipedia.org/wiki/WhatsApp#Platform_support>

<https://en.wikipedia.org/wiki/XMPP>

<https://en.wikipedia.org/wiki/Transport_Layer_Security>

<https://www.whatsapp.com/>