Criptarea end-to-end, paznicul confidențialității noastre online

Introducere

Împărtășim zeci, sute sau mii de mesaje pe zi cu prietenii (și cu străinii, câteodată) care conțin de la "bună dimineața", lista de cumpărături sau "unde ești" până la, gânduri aleatorii, mesaje dornice, obscene, amuzante sau secrete, dar și poze jenante. Prezumția de la care plecăm e că aceste mesaje sunt doar ale noastre - ale mele și ale celui cu care vorbesc - și că nimeni altcineva, fără acces direct la dispozitivele mele, nu le poate vedea. Dar lucrurile pot fi altfel, în realitate.

Dacă ne dorim ca toate conversațiile noastre electronice să fie confidențiale, singura opțiune care ne poate garanta tehnic asta poartă denumirea de criptare end-to-end (adică de la un capăt la celălalt). Aceasta este o tehnologie care a evoluat de-a lungul anilor 2000 și nu a însemnat întotdeauna ce înseamnă astăzi.

Când spunem, acum, că mesajele dintr-un chat sunt criptate end-to-end, asta presupune că:

1. Doar participanții la conversație pot citi conținutul mesajelor.
2. Dacă cineva interceptează mesajele "pe drum", ele sunt neinteligibile.

De obicei, atunci când aplicațiile de chat securizează comunicarea utilizatorilor cu criptare end-to-end, implementarea poate să mai vină la pachet cu alte avantaje, precum:

1. Garanția că, dacă cineva modifică un mesaj "pe drum", destinatarul își poate da seama de asta.
2. Identitățile participanților la o conversație sunt garantate ca fiind corecte. Adică, dacă cineva vrea să se prefacă că e destinatarul, de pe un alt dispozitiv, nu va reuși să treacă de testul care confirmă identitatea.

Astăzi vorbim cel mai adesea de criptare end-to-end în contextul comunicării de tip chat, dar această tehnologie stă, de fapt, la baza a mai multor procese importante de pe internet. Atunci când vizualizăm un site - de exemplu, când citim feed-ul de Facebook în browser, sau căutăm ceva pe Google - toată informația care circulă între noi și serverele care găzduiesc aceste platforme este criptată end-to-end. Când folosim aplicații bancare, informația care circulă între aplicația de le telefon și serverele băncii este criptată end-to-end. Nu în ultimul rând, există servicii care ne permit să stocăm fișiere online care ne garantează faptul că serverul pe care sunt găzduite nu poate să vadă conținutul lor, pentru că folosesc criptare end-to-end.

Deși pare că avem, cu toții, numai de câștigat cu o securitate sporită de pe urma criptării end-to-end, există totuși multe entități care-și doresc să o slăbească sau să o elimine în totalitate. Eforturile acestea sunt suficient de mari și s-au întins pe mai mulți ani, astfel încât au căpătat titlul de război împotriva criptării.

De-a lungul istoriei, serviciile secrete de informații s-au bucurat de abilitatea legală de a monitoriza comunicarea cetățenilor, atunci când aveau motiv să o facă. Sau nu. Desigur, motivația lor, cât și modul în care au ales să facă această monitorizare au fost deseori puse la îndoială atunci când cetățenii au aflat despre acestea (uneori, de la avertizori de integritate precum Edward Snowden). Criptarea end-to-end face această monitorizare imposibilă tehnic, deoarece un serviciu de informații nu este unul dintre participanții la o conversație, deci nu poate să descifreze mesajele criptate.

Pe lângă autoritățile care ar vrea să aibă puterea de a monitoriza comunicațiile cetățenilor atunci când cred de cuviință (și, într-o societate democratică, când au un mandat judecătoresc să facă asta), unele companii ale căror profituri vin și din reclame sunt de asemenea împotriva criptării end-to-end. O bună parte din reclamele pe care le vedem în spațiul online ne sunt livrate în baza informațiilor pe care companiile le deduc despre noi. Dacă criptarea end-to-end ne protejează conținutul discuțiilor, atunci aceste companii au din ce în ce mai puține informații despre noi, ceea ce le poate dăuna modelului de afaceri bazat pe supravegherea activității online a utilizatorilor.

Criptarea end-to-end este o tehnologie interesantă și din cauza faptului că implementarea sa se bazează pe operații matematice care oferă niște garanții foarte puternice. Atunci când folosim cele mai recente tehnologii de criptare recomandate, nimeni nu poate să descifreze în timp util un mesaj decriptat dacă nu are o așa-numită cheie de decriptare. Cele mai performante sisteme de calcul din zilele noastre ar trebui să petreacă atât de mult timp pentru a descifra un singur mesaj, încât nimeni nu consideră că merită efortul.

În prezent, vedem mai multe inițiative de politici publice sau legislative, în țări diferite, care încearcă fie să forțeze companiile să descifreze mesajele schimbate pe platformele lor, fie să introducă o "ușă din spate" (backdoor), un mod de a accesa totuși conținutul mesajelor, la care ar avea acces doar "organismele competente" și nimeni altcineva. Unele dintre aceste proiecte de lege au trecut și sunt în vigoare în momentul de față, cum ar fi Online Safety Bill, în Marea Britanie.

Ce este cert, și a fost repetat timp de foarte mulți ani de comunitatea de experți în securitate și criptografie, este că nu există niciun mod de a oferi autorităților competente această "ușă din spate" la care să aibă acces doar ei. Dacă am crea un mod prin care autoritățile pot să descifreze și ele mesajele criptate dintr-o conversație, mai devreme sau mai târziu, hackerii și alte persoane rău-intenționate vor descoperi cum funcționează acest mecanism și vor abuza de el. Astfel, imediat ce creăm o "ușă din spate", putem fi siguri că, mai devreme sau mai târziu, ea va fi descoperită și folosită pentru a face rău.

Ce este criptarea?

Criptografia este o ramură a matematicii care își propune să garanteze o comunicare sigură, care nu poate să fie descifrată sau modificată de către altcineva în afara participanților la comunicare. Când spunem "criptare", ne referim la o aplicare a criptografiei.

Criptarea modernă a datelor are o istorie lungă și este, practic, un proces informatic prin care un text lizibil, care poate fi citit și înțeles de un om, este ascuns. În termeni tehnici conținutul acesta este codificat, adică devine ilizibil sau cifrat.

Un mesaj devine criptat atunci când trece printr-un proces matematic de conversie, de la text lizibil și descifrabil, la un text ilizibil care trebuie decodificat pentru a putea fi înțeles. Acest proces garantează că persoane terțe nu pot accesa conținutul mesajelor, decât dacă sunt dispuse să petreacă enorm de mult timp

pentru a încerca toate posibilitățile de a descifra mesajul - de exemplu, un miliard de ani, pentru un simplu mesaj criptat cu algoritmul AES și o cheie de 128 de biți.

Procesul invers, decodificarea, transformă mesajul din ilizibil (cifrat) în lizibil (descifrat).

Există mulți algoritmi de criptare și multiple utilizări ale lor.

Pe internet, cel mai adesea, vorbim despre o metodă de criptare care folosește o cheie privată și una publică. Aceste chei nu sunt nimic altceva decât șiruri de cifre, generate și folosite pentru a face operația matematică de criptare. Acest tip de criptare mai poartă numele de criptare asimetrică.

Cheia publică poate fi trimisă oricui și ea va fi folosită pentru a cripta un mesaj. Cheia privată care corespunde cheii publice folosite este necesară pentru a decripta mesajul. Dacă cineva a pierdut cheia privată, mesajul va rămâne veșnic neinteligibil.

Pe internet, noi vedem rareori aceste chei. Persoanele care folosesc tehnologia PGP pentru a cripta e-mail-uri, mesaje, sau fișiere, ajung să lucreze direct cu perechea proprie de chei. Dar, de cele mai multe ori, software-ul pe care îl folosim implementează deja tot procesul de a crea, folosi și proteja aceste chei. Chiar și atunci când mesaje sunt schimbate de internet între aplicații, mesajele lor sunt criptate (cel mai probabil, fiind vorba de trafic HTTPS).

A existat un moment în trecut în care doar unele website-uri de pe internet comunicau criptat cu utilizatorii care le vizitau. Aceasta era perioada în care protocolul HTTPS încă nu era adoptat la scară largă. Protocolul HTTP, precursorul său, care încă e folosit, însă la scară mult mai redusă, nu cripta mesajele și le trimitea "în clar" de la un capăt la celălalt. Astfel, comunicarea era vulnerabilă la multiple atacuri în care persoane rău-intenționate puteau intercepta sau modifica "pe drum" mesajele.

Treptat, protocolul HTTPS a devenit folosit de cea mai mare parte a website-urilor foarte vizitate de pe internet. Însă problema comunicării criptate rămâne una foarte importantă când vine vorba de aplicații de mesagerie instantă.

Criptarea bună versus criptarea așa-și-așa

Singurul tip de criptare care protejează complet comunicarea online este criptarea end-to-end. Însă, din păcate, acest tip de criptare nu este implementat astăzi pe scară largă de către toate aplicațiile de mesagerie instantanee. Majoritatea nu o implementează, unele aplicații oferă criptare end-to-end ca variantă pentru care utilizatorul poate opta și destul de puține aplicații oferă doar acest tip de criptare.

> *O formă de criptare care ne protejează doar parțial se numește criptare "client-to-server" (adică mesajele sunt criptate doar între client și server). În materiale comerciale, acest tip de criptare mai poartă numele formal de "encryption in transit" (criptare care funcționează doar cât timp mesajele circulă de la o destinație la următoarea) sau "client-side encryption" (adică o criptare care funcționează doar pe partea clientului). Dat fiind că acest tip de criptare nu oferă garanții la fel de bune ca cea end-to-end, multe aplicații schimbă denumirea pe care o folosesc în materiale promoționale pentru a face produsul lor să pară mai sigur.*
>
> *Criptarea "client-to-server" protejează mesajele doar între expeditorul unul mesaj și serverul aplicației de mesagerie. Cum aproape orice aplicație foarte folosită de mesagerie va trimite mesajele printr-un server înainte ca ele să ajungă la destinatar, acesta e un punct în care e foarte important dacă mesajele rămân sau nu descifrabile doar de participanții la comunicare. În cazul criptării end-to-end, mesajele sunt criptate inclusiv pe server, deci compania care deține aplicația nu le poate citi. În cazul criptării "client-to-server", mesajele sunt lizibile pe server și pot fi citite de compania care deține aplicația.*

Aplicații care criptează end-to-end

Dintre aplicațiile de mesagerie instantanee cele mai folosite astăzi în România, singurele care implementează criptarea end-to-end sunt Signal și WhatsApp.

Facebook Messenger, TikTok, Instagram, Telegram folosesc din oficiu criptarea incompletă de tip "client-to-server". Facebook Messenger și Telegram permit utilizatorului să creeze așa-zise "secret chats", care sunt criptate end-to-end. Dar utilizatorul trebuie să își dorească să le creeze. Altfel, va folosi metoda mai puțin sigură de criptare.

Între Signal și WhatsApp nu sunt extrem de multe diferențe la nivelul implementării criptării, dar cele două aplicații diferă enorm când vine vorba de modul în care companiile care le dețin își tratează utilizatorii.

WhatsApp este deținut de Meta, compania care deține Facebook și Instagram. Atunci când schimbăm mesaje pe WhatsApp, compania le criptează end-to-end, dar alege să păstreze informații despre numerele de telefon care trimit mesaje între ele, sau numerele care sunt într-un chat comun. Aceste informații împreuna cu alte detalii ale conversației (cât vorbești, când (minut și secundă), numite și date de trafic sau metadate, nu îi oferă lui Meta nicio informație despre ce își spun oamenii, dar îi dă foarte multe de înțeles despre cine comunică cu cine. Și pot fi extrem de intruzive, cum am aflat deja în deciziile Curții de Justiție a Uniunii Europene și a ale Curții Constituționale din România.

Unul dintre foștii șefi ai NSA-ului, serviciile secrete de informații din America, a spus că guvernul american *ucide în baza metadatelor*. Ceea ce voia să transmită este că informația legată de legăturile dintre oameni, legate de când comunică și cât comunică sunt suficiente pentru a lua decizii critice legate de aceștia. De aceea, faptul că anumite companii rețin metadate în aplicațiilor pe care le oferă este foarte important, dat fiind că unii pot avea acces la aceste date, într-un regim democratic doar printr-un mandat de la o instanță judecătorească.

Signal, în schimb, este deținută de o organizație de tip non-profit axată pe confidențialitate, finanțată prin subvenții și donații. Ei nu rețin metadate și, deci, chiar și atunci când le-ar fi servit un mandat de percheziție, nu își pot pune în pericol utilizatorii, pentru că, tehnic, nu au cum.

Aplicația Signal este recomandată pentru orice fel de comunicare sigură, de la discuții cu amici, părinți sau colegi, până la discuțiile sensibile pe care, spre exemplu jurnaliștii le poartă cu sursele lor.

Chat Control și client-side scanning

În prezent, criptarea pare că evoluează pe două paliere.

Pe de o parte, cercetătorii și programatorii care lucrează pe probleme de criptografie caută să îmbunătățească acești algoritmi care ne garantează siguranța mesajelor și fișierelor.

Pe de altă parte, în rândul unor companii și unor guverne, există un efort susținut de a submina sau înlătura criptarea și de a avea acces la cât mai multe date despre cetățeni. Criptarea end-to-end este sub atac la scală globală. Statele Unite,

Australia, Anglia, și UE încearcă să submineze criptarea end-to-end prin intermediul legii.

> *O altă amenințare la adresa criptării vine din partea calculatoarelor cuantice. Aceste dispozitive sunt încă în stadiul unor modele foarte slabe, dar care, teoretic, execută programe într-un mod diferit față de calculatoarele pe care le folosim în prezent. Calculatoarele cuantice ar putea, în teorie, să descifreze mesaje criptate mult mai repede decât calculatoarele normale, ceea ce a determinat experții în domeniu să lucreze la algoritmi de criptare post-cuantici. Astfel, atunci când vom avea calculatoare cuantice care vor fi mai mult decât niște simple modele, vom avea și algoritmi de criptare care ne oferă aceleași protecții de care ne bucurăm acum.*
>
> *Avem deja exemple de algoritmi post-cuantici despre care putem spune că ne-ar putea proteja, în viitor. Însă, nu avem la fel de mult succes în a adresa problema cealaltă, a unor companii și guverne care vor să submineze criptarea. Pentru că, în acel caz, experții nu sunt puși în fața unei probleme matematice, ci a unei chestiuni politice sau de profit comercial.*

În Uniunea Europeană, o propunere de Regulament supra-numită Chat Control este cel mai recent exemplu al unui efort politic de a submina criptarea. Acest proiect de lege susține că, pentru a preveni distribuirea de material abuziv cu caracter sexual implicând minori, toate comunicațiile digitale ale tuturor cetățenilor Uniunii Europene vor fi verificate pe dispozitivele lor, de un algoritm de inteligență artificială. Acest algoritm decide dacă mesajele pe care cetățenii vor să le trimită conțin material abuziv și, dacă nu, mesajele vor fi criptate și trimise la fel ca până acum.

Comisia Europeană argumentează că proiectul lor de lege nu subminează criptarea în sine, pentru că mesajele vor fi în continuare criptate înainte de a fi trimise. Dar, ceea ce este extrem de important, este că mesajele vor fi procesate de încă o entitate, prin acest algoritm de inteligență artificială. Astfel, promisiunea criptării, că doar participanții la conversație văd conținutul mesajului, este încălcată.

Acest act legislativ a generat extrem de multe controverse despre către ApTI a scris în detaliu. În prezent, nu există semne clare dacă propunerea de Regulament va fi adoptată până la finalul legislaturii europene din 2024

În contextul culturii digitale de astăzi

Pe internet astăzi suntem, după cum spunea filosoful Byung Chul Han în cartea sa *Capitalism and the Death Drive*, o cultură de indivizi *hipercomunicativi* - adică comunicăm tot ce ne trece prin cap, tot timpul, cu cineva sau cu noi înșine (într-un fișier doc de tip jurnal), fiindcă media digitală contemporană încurajează un astfel de comportament. Alți cercetători din domeniul comunicării online au numit această tendință a comunicării mijlocite de calculatoare *comunicare hiperpersonală.*

Ne împărtășim și distribuim gânduri intruzive, secrete, poze jenante, și așa mai departe - asta e condiția omului digitalizat. Secretele dispar, încet și încet, din constituția noastră psihologică, sugerează B.C. Han. Această tendință tinde să se exacerbeze pe sine, nu să se diminueze în vreun mod considerabil, în era digitală.

Acest tip de cultură digitală nu o să dispară prea de curând - așa că doar criptarea end-to-end ne poate garanta o protecție tehnică *minimală* a hipercomunicării hiperpersonale online. Fără criptare end-to-end, orice gând împărtășit cu altcineva ar putea fi monitorizat, verificat și vândut mai departe unor entități cu diverse interese, de obicei maligne - și dăunătoare drepturilor noastre fundamentale.

Protecția criptării end-to-end înseamnă protecția tehnică a intimității și confidențialității noastre online.