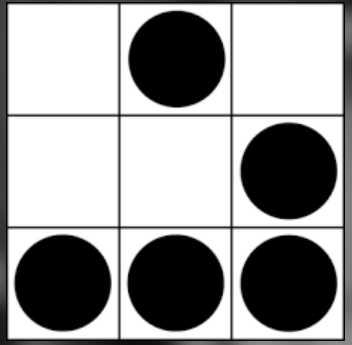


Analysis app. sms/voip for cellular – privacy by design

Fabio Carletti aka Ryuw E-Privacy 2021

PROGETTO WINSTON SMITH

WHOAMI

Strategic IT consultant

Membro Clusit e Onif

Relatore IPA (International Police Association)

cyber security researcher

I like Unix ;-)

analisi app for cellular

...deve proteggere le chat da cracker

PROGETTO WINSTON SMITH

la privacy online è un diritto di tutti, convinti che ogni individuo possa inviare un messaggio ad amici senza doversi preoccupare di poter essere spiato

PROGETTO WINSTON SMITH

E.Snowden

Quanto siete disposti a sacrificare della vostra vita privata per il beneficio di uno stato di sorveglianza globale?

PERCHE' ABBIAMO BISOGNO DI APP SICURE?

Electronic Frontier Foundation due anni fà condusse un test sulle principali applicazioni evidenziando che non vi erano standard di sicurezza accettabili (https://www.eff.org/pages/secure-messaging-scorecard)

PROGETTO WINSTON SMITH

EFF per i test usarono queste indicazioni



I dati vengono criptati in transito?
I dati vengono criptati in modo tale che neanche il fornitore del servizio possa leggerli?
È possibile risalire alla vera identità dei contatti?
Il fornitore del servizio mette in pratica quello che è conosciuto come perfect forward secrecy, in italiano “segretezza in avanti” (il che significa che le crypto-chiavi sono temporanee e una chiave rubata non decifrerà le comunicazioni esistenti)?
Il codice del service provider è open-source ed è disponibile ad un’analisi pubblica?
Le procedure di implementazione crittografiche e i relativi processi sono documentati?
Il servizio è stato sottoposto a un audit indipendente negli ultimi 12 mesi?

PROGETTO WINSTON SMITH

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
AIM	✓	✗	✗	✗	✗	✗	✗
BlackBerry Messenger	✓	✗	✗	✗	✗	✗	✗
BlackBerry Protected	✓	✓	✓	✗	✗	✓	✓
ChatSecure + Orbot	✓	✓	✓	✓	✓	✓	✓
Ebuddy XMS	✓	✗	✗	✗	✗	✗	✗
Facebook chat	✓	✗	✗	✗	✗	✗	✓
FaceTime	✓	✓	✗	✓	✗	✓	✓
Google Hangouts/Chat "off the record"	✓	✗	✗	✗	✗	✗	✓
Hushmail	✓	✗	✗	✗	✗	✗	✗
iMessage	✓	✓	✗	✓	✗	✓	✓

PROGETTO WINSTON SMITH

abbiamo bisogno di app di messaggistica sicura?

...ci sono vari settori in cui le app di messaggistica sicure sono indispensabili. Le aziende legali e di consulenza hanno bisogno delle app di messaggistica sicure migliori della categoria, perché non desiderano che le informazioni sensibili dei propri clienti vengano divulgate.

Cosè un Cryptosystem?

-Plaintext is what you want to protect

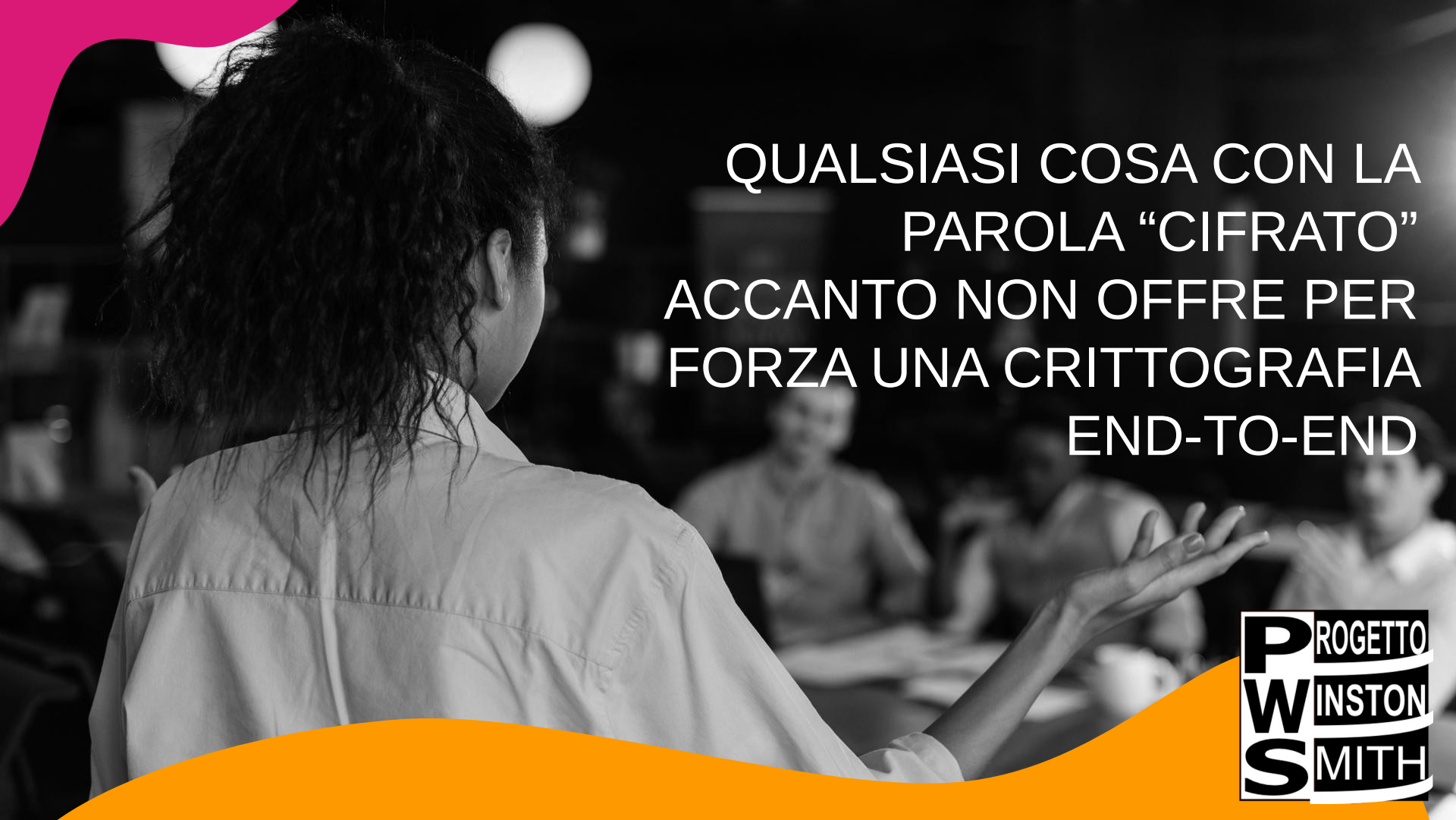
A cryptosystem is pair of algorithms that convert plaintext to ciphertext and back.

-Ciphertext is the encrypted version of the plaintext

criptaggio and-to-end

Verifica se l'app di messaggistica ha la disponibilità della crittografia end-to-end in modo che solo il mittente e il destinatario hanno le "chiavi" per leggerli. La crittografia incapsula il messaggio che non può essere letto da un cracker che riuscisse a intercettarlo nella rete internet. La crittografia end-to-end si basa sulla crittografia asimmetrica (detta "a chiave pubblica"), realizzata mediante la generazione di una coppia di chiavi, una "privata" e una "pubblica" che sono differenti, ma legate tra loro da un algoritmo che è stato inventato nel 1976 da Whitfield Diffie e Martin E.Hellman (si parla infatti di algoritmo Diffie-Hellman per lo scambio delle chiavi).

PROGETTO WINSTON SMITH


QUALSIASI COSA CON LA PAROLA “CIFRATO” ACCANTO NON OFFRE PER FORZA UNA CRITTOGRAFIA END-TO-END
PROGETTO WINSTON SMITH

App SEC MOBILE TELEPHONE

la crittologia..
- privact of stored data, messages and conversations
-Integrity of stored sdata, messages and conversations
-User and data authentication

cifrato

Alcuni servizi eseguono la crittografia del messaggio tra gli endpoint della trasmissione e, di conseguenza, le conversazioni sono conservate nei server della compagnia che fornisce il servizio, la quale, avendole cifrate, può anche decriptarle.Il punto debole può essere il dispositivo stesso e soprattutto l'uso che ne fa l'utente "fattore umano". Se una delle due estremità (endpoint) viene compromessa, se il nostro telefono viene rubato o violato (per esempio con uno spyware, o captatore informatico, come nel caso accaduto a Jeff Bezos) o fisicamente confiscato dalla polizia e sbloccato, la crittografia non serve più a nulla.

PROGETTO WINSTON SMITH

metadati

Informazioni come data e ora di invio, numero del mittente e del destinatario, la loro localizzazione generano fingerprint permette di capire con chi stiamo interagendo

L’asset intangibile che sta dietro al business sono i nostri dati, quelli che Tim Berners-Lee (l’inventore del World Wide Web) ha definito efficacemente “il petrolio del terzo millennio”.

PROGETTO WINSTON SMITH

aspetti per valutare la sicurezza delle app

- il business model: conoscere il modello di business sul quale queste applicazioni si reggono è fondamentale. Sono quasi tutte gratuite e questo ci obbliga a chiederci in che modo guadagnano o, quantomeno, su cosa si reggono. È persino superfluo richiamare qui la frase che “Se sul web qualcosa è gratis, tu sei il prodotto…”.
- la diffusione: un’applicazione molto diffusa sarà sicuramente più esposta ad ogni tipo di attacco: ci saranno molti gruppi di ricercatori, analisti e cyber attaccanti che continuamente ne ricercheranno vulnerabilità da sfruttare.
- i dati che vengono trasmessi e ricevuti: sarebbe opportuno definire una tassonomia dei dati, classificare il dato in funzione della sua importanza (pubblico, riservato). Potrebbe sembrare una misura ridondante ma diventa importante nel momento in cui nei nostri messaggi viaggiano informazioni importanti, aziendali e riservate. In un certo senso, le metodologie che applichiamo nella privacy (GDPR insegna) dovrebbero essere considerate anche quando abbiamo in mano lo smartphone.

PROGETTO WINSTON SMITH

WhatsApp

pro e contro

pro:
massima diffusione nel mondo;
grande facilità d’uso;
usa la crittografia end-to-end in automatico;
supporta le videochiamate;
il backup della chat permette agevolmente la migrazione su un altro dispositivo;
ha l’applicazione desktop (WhatsApp Web);
contro:
conserva molti metadati dei messaggi in forma non cifrata;
il codice sorgente è proprietario (non open source) quindi non è accessibile per audit di terze parti.

PROGETTO WINSTON SMITH

WhatsApp

ANONYMOUS

tweet del gruppo Anonymous, app. successivo (5 aprile 2016) all’introduzione della crittografia in WhatsApp, invita a riflettere su un servizio che è di proprietà di Facebook.

PROGETTO WINSTON SMITH

Telegram

bandita in Russia, perché non ha voluto consegnare le chiavi di crittografia alle autorità russe

pro:
molto diffuso nel mondo;
interfaccia semplice;
messaggi a scomparsa;
non è sottoposta alle logiche commerciali;
creazione di gruppi fino a 200 mila utenti, quasi un social network;
canali “broadcast” (invio “uno a molti”);
funzione di condivisione di file pesanti;
basata sul Cloud: non si deve esporre il numero di telefono per chattare;
il codice sorgente è open source;
contro:
le chat di default non sono cifrate end to end (c’è cifratura client-server e le chat passano dal cloud Telegram);
la crittografia end to end funziona solo per le chat segrete;
l’algoritmo di crittografia proprietario non è ritenuto molto sicuro;

PROGETTO WINSTON SMITH

Wickr Me/Wickr pro

“Questo messaggio si autodistruggerà entro X secondi“

pro:
garantire la sicurezza e la privacy delle comunicazioni tra i suoi utenti;
Durata dei messaggi 1s a 24 ore;
Senza banner pubblicitari;
Disponibile per pc;
Integrazione dei contatti già esistenti;
Non serve sim card per loggarsi;
Funziona invisibile;
Il codice sorgente è stato reso disponibile su GitHub.
Ha la funzione di Rilevamento degli screenshot e la funzionalità Secure Data Shredder per accertarsi che i file già eliminati non siano recuperabili con strumenti o tecnologie particolari (in pratica un “distruggi- documenti”)

PROGETTO WINSTON SMITH

Wire

“dichiara di rispettare le leggi europee sulla privacy (quindi il GDPR)

pro:

protocollo Proteus (che si basa su Axolotl ed è disponibile open source su GitHub) per la crittografia end-to-end.
Wire è il software di collaborazione e comunicazione più ampiamente verificato sul mercato.
100% opensource;

PROGETTO WINSTON SMITH

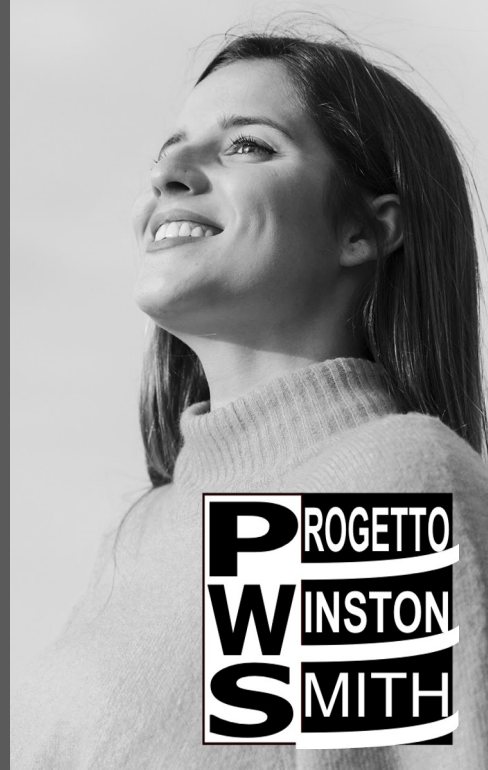
Signal

preferita da Edward Snowden e B. Schneier

pro:
è gestito da una fondazione non-profit e non ha fini di lucro;
algoritmo di crittografia molto sicuro;
messaggi a scomparsa;
consente telefonate e audio cifrati;
consente la creazione di gruppi;
non conserva i messaggi;
non conserva i metadati;
il codice sorgente è open source ed è stato oggetto di audit indipendente;
ha l'applicazione desktop;
contro:
non permette il backup delle chat ed il trasferimento su un altro dispositivo;
funzioni più limitate rispetto alle applicazioni più diffuse;
qualche perdita di segnale telefonico in assenza di Wi-Fi (qualità delle chiamate e videochiamate da migliorare).

PROGETTO WINSTON SMITH

SERVIZIO		DISCORD	KEYBASE	SIGNAL	SKYPE	TELEGRAM	WECHAT	WHATSAPP
Produttore		Discord	Keybase	Signal Foundation	Microsoft	Telegram	Tencent	Facebook
Giudizio		★★★★☆	★★★½☆	★★★★½	★★★★☆	★★★★½	★★★☆☆	★★★★☆
Sito Web		*www.discord.com*	*https://keybase.io*	*https://signal.org*	*www.skype.com*	*www.telegram.org*	*www.wechat.com*	*www.whatsapp.com*
DATI								
Anno di introduzione		2015	2017	2014	2003	2013	2011	2009
Licenza		Proprietaria	Open source	Open source	Proprietaria	Open source	Proprietaria	Proprietaria
Registrazione		Email	Account	Numero di telefono	Account	Numero di telefono	Numero di telefono	Numero di telefono
Piattaforme	Windows	●	●	●	●	●	●	●
	macOS	●	●	●	●	●	●	●
	Linux	●	●	●	●	●	✖	✖
	Web	●	Parziale	✖	●	●	●	●
	Android	●	●	●	●	●	●	●
	iOS	●	●	●	●	●	●	●
FUNZIONI								
Chat cifrate end to end	Due utenti	✖	●	●	●	Opzionali	✖	●
	Gruppi	✖	●	●	✖	✖	✖	●
Trasferimento file		●	●	●	●	●	●	●
Messaggi vocali		✖	✖	●	●	●	●	●
Chat vocale/video		●/●	✖/✖	●/●	●/●	●/●	●/●	●/●
Conferma di lettura		✖	●	●	●	●	✖	●
Modifica/Elimazione messaggi inviati		●/●	●/●	✖/Parziale	●/●	●/●	●/●	✖/Parziale
Emoji/Sticker		●/●	●/✖	✖/●	✖/●	●/●	✖/●	●/●
Autodistruzione messaggi		✖	●	●	✖	●	✖	Parziale



PROGETTO WINSTON SMITH

GDPR e sistemi di messaggistica

Per considerare adeguata, in termini di sicurezza dei dati, un'applicazione, non basta che gli sviluppatori ci dicano che la comunicazione è cifrata end-to-end in quanto questo impedisce solo che le informazioni vengano lette da terzi durante la trasmissione.
Nell'ambito delle applicazioni di messaggistica utilizzate sugli smartphone, esiste la possibilità concreta che, ad esempio, del codice malizioso consenta a terzi di sottrarre e, manipolare le informazioni trasmesse, specie se sono trasmesse in forma documentale.
Gli smartphone e i device che partecipano alla trasmissione dell'informazione in quanto il mittente e il ricevente hanno un terminale sottoposto ad alcun controllo.

PROGETTO WINSTON SMITH

GDPR

Il singolo mezzo non è catalogabile come in compliance o meno al GDPR, ma è il mezzo nell’ambito del processo di trattamento che i dati personali subiscono che diventa più o meno critico.Non ci sono strumenti in assoluto “non in compliance” alla normativa a tutela dei dati personali ma esistono approcci sbagliati o non corretti al trattamento.

PROGETTO WINSTON SMITH

GDPR

Per considerare adeguata, in termini di sicurezza dei dati, un’applicazione, non basta che gli sviluppatori ci dicano che la comunicazione è cifrata end-to-end in quanto questo impedisce solo che le informazioni vengano lette da terzi durante la trasmissione. Nell’ambito delle applicazioni di messaggistica utilizzate sugli smartphone, esiste la possibilità concreta che, ad esempio, del codice malizioso consenta a terzi di sottrarre e, manipolare le informazioni trasmesse, specie se sono trasmesse in forma documentale.

UPDATE SOFTWARE

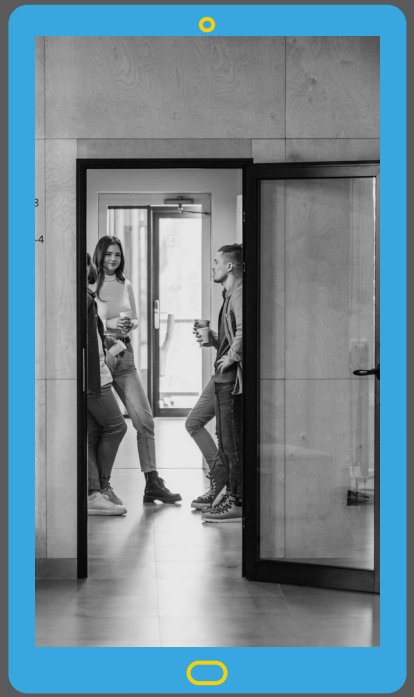
Gli smartphone e i device che partecipano alla trasmissione dell’informazione non sono sempre in sicurezza in quanto il mittente e il ricevente hanno un terminale sottoposto ad alcun controllo di aggioramenti di patch di sicurezza o di os

PROGETTO WINSTON SMITH

open source

sorgente aperto, in informatica si indica il suo modello di sviluppo o distribuzione

PROGETTO WINSTON SMITH



Edward Snowden

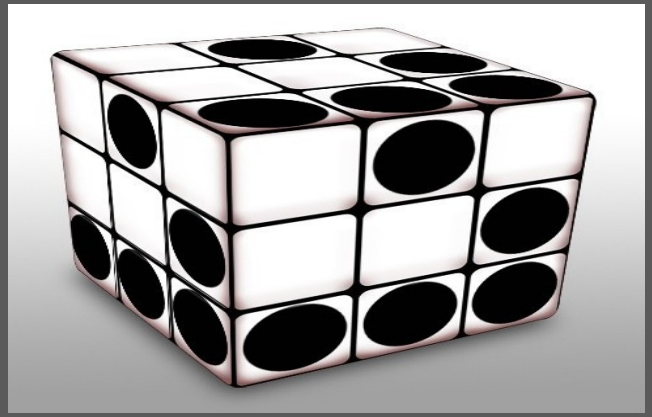
«Le persone che sostengono di non essere interessate alla privacy, perché non hanno niente da nascondere, non capiscono qual è la reale posta in gioco. È come se dicessero che non gli interessa la difesa di un loro diritto. Dire *“non mi interessa della privacy perché non ho nulla da nascondere”* è come dire “non mi interessa della libertà di espressione perché non ho niente da dire, né della libertà di stampa perché non ho niente da scrivere”.

PROGETTO WINSTON SMITH

THANKS!

Fabio Carletti aka Ryuw E-Privacy 2021

linkedin.com/in/fabio-carletti-53b38722



PROGETTO WINSTON SMITH