Privacy e anonimato su smartphone Android

2014
LINUX
D A Y
I T A L I A

Mainardi Davide

- Ingegnere informatico laureato al Politecnico di Torino.
- Appassionato del mondo *open source* dal 2004.
- Primo *smartphone* acquistato nel 2008: **Nokia N73.**
- Primo *smarphone* senza tasti fisici acquistato nel 2013: **Google Nexus 5.**

Smartphone

La **rapida diffusione** degli *smartphone*, in grado di connettere gli individui in modo quanto mai personale, ha portato l'**informatica** al di **fuori dei confini** tradizionali.

Smartphone

Come è successo?

L'enorme **capillarità** dei cellulari, unita all'intrinseca **obsolescenza**, ha fatto sì che essi venissero via via **sostituiti** dagli *smartphone*.

Smartphone

- Le **app** (i software applicativi per dispositivi mobili) sono molto semplici da usare.
- Ogni app compie il suo dovere e **svolge al meglio** il compito per cui è stata progettata.
- Le app, semplicemente, **funzionano**; e bene!

Smartphone

- Gli ***smartphone***, in special modo i costosi modelli top di gamma, riescono a **risolvere** i più comuni **problemi** degli utenti.
  - Trovano le informazioni.
  - Permettono di comunicare con altre persone.
  - Ci guidano verso la destinazione.
  - Catturano (con foto e video) il mondo circostante.

Smartphone

- Lo ***smartphone*** è facile e veloce da usare, ed è **trendy**
- Gli utenti sono portati a **fidarsi ciecamente** del proprio *smartphone*.

Smartphone

Lo *smartphone* non è un **semplice telefono**, ma un vero e proprio **computer**.

- Molto più **personale**.
- Molto più **acceso**.
- Molto più **connesso**.

Privacy

Quali sono i **dati** che dallo *smartphone*, **inconsapevolmente**, vengono inviati all'esterno?

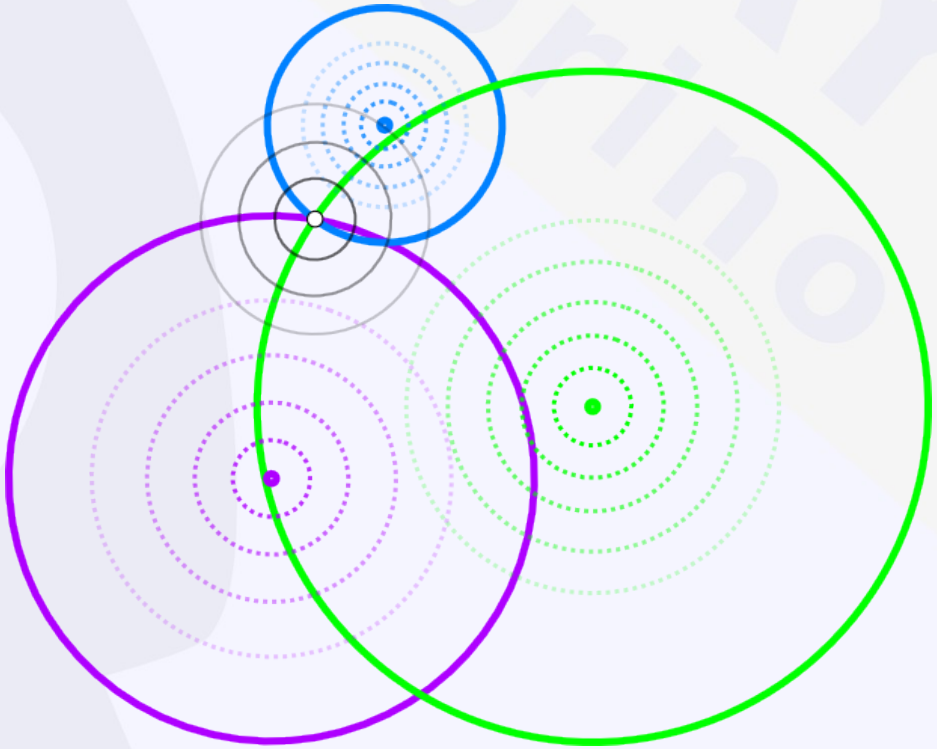
- Informazioni “telefoniche”
- Informazioni “internet”

Informazioni telefoniche

- **Chiamate vocali** in entrata e in uscita
  - Il numero di telefono del mittente
  - Il numero di telefono del destinatario
  - La durata della chiamata
- **Messaggi** (SMS) in entrata e in uscita
  - Il numero di telefono del mittente
  - Il numero di telefono del destinatario

Informazioni telefoniche

- Quanto spesso si accede alla **rete internet** o si controlla la casella e-mail.
- La **posizione** della cella (a volte molto precisa)



Informazioni telefoniche

A giugno 2014 il quotidiano **The Guardian** pubblica un articolo in cui commenta il comunicato ed il rapporto di trasparenza rilasciato da **Vodafone**. Nel rapporto sono presenti i dati delle intercettazioni telefoniche (**contenuto** e **metadati**).

Informazioni telefoniche

Nazione	Metadati Vodafone	Contenuto Vodafone	Metadati Nazionali	Contenuto Nazionale
Belgio	2			
Rep. Ceca		7.677	195.504	
Francia	3			
Germania			18.026	23.687
Grecia			8.602 in totale	
Irlanda	4.124	Permesso di pubblicazione non concesso		
Italia	**605.601**			**140.577**
Portogallo	28.145		13.046	
Regno Unito			514.608	2.760
Spagna	48.679	24.212		

Informazioni internet

- Qualsiasi **foto** scattata o **video** registrato.
- Dettagli dei **messaggi** e delle **e-mail** che si inviano e si ricevono, compreso il contenuto.
- L'**identificativo** del chiamante e del chiamato (per chiamate vocali internet), compresi i dettagli come il **luogo** e la durata della chiamata.

Informazioni internet

- I contatti salvati
- ***Password***
- Dati finanziari
- Gli **appuntamenti** salvati nel calendario
- Il **luogo** abituale (residenza), età e genere

Sicurezza

Chi può prendere queste informazioni?

- Criminali
- Aziende pubblicitarie
- Governi

Glieli forniamo noi **inconsapevolmente**.

- "Accetto i termini e le condizioni del servizio"

Quali sono le ***privacy policies*** ?

Sicurezza

Come vengono **attaccati** gli ***smartphone*** ?

- Accesso fisico al dispositivo.
- Attraverso le connessioni (WiFi, Bluetooth).
- Ingegneria sociale.

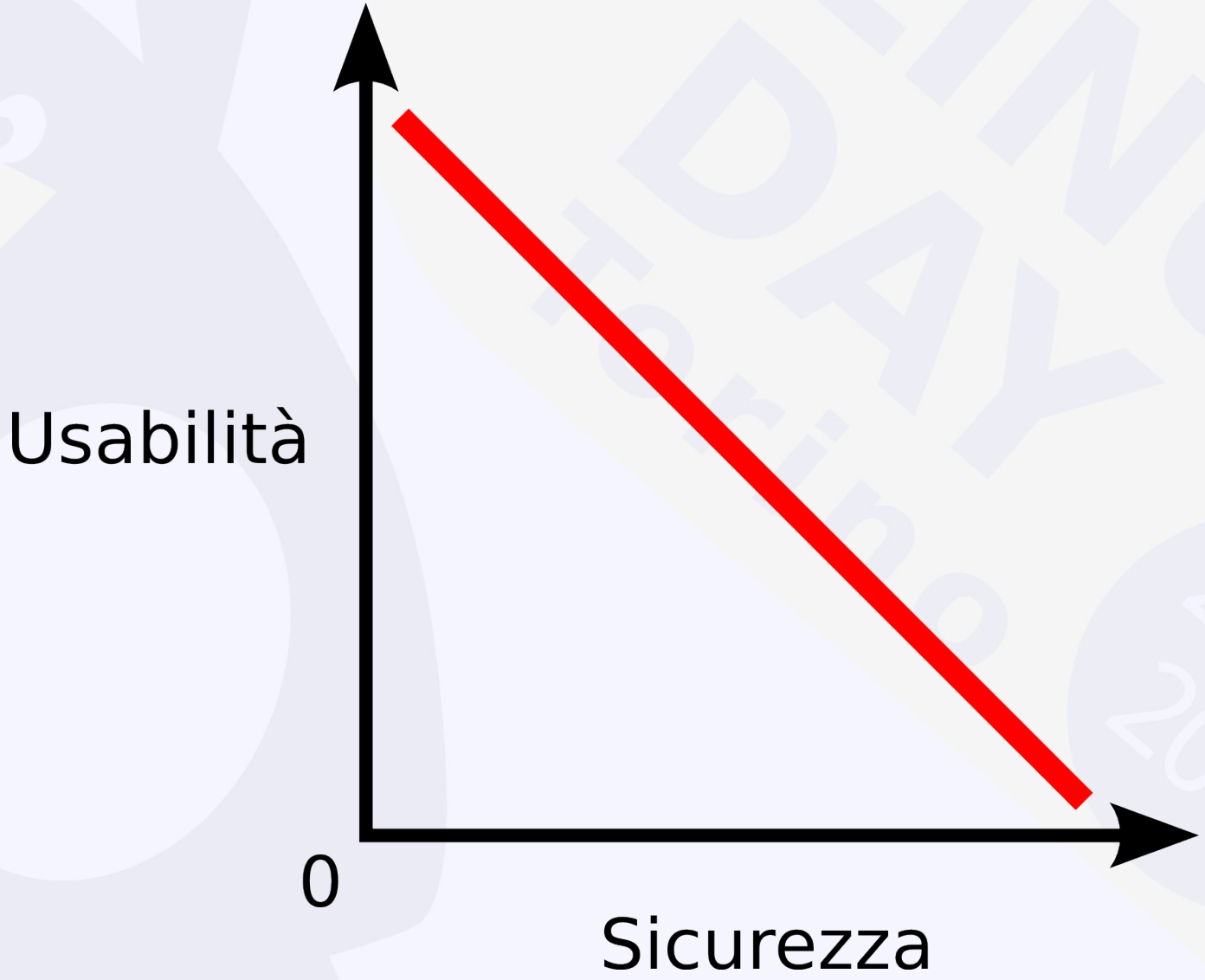
Soluzioni

Prima di tutto è necessario decidere il **livello di privacy** che vogliamo ottenere.

Un maggiore livello di privacy e sicurezza comporta necessariamente una **minore usabilità**.

Nell'uso comune, a volte, **usabilità** diventa un sinonimo di **comodità**.

Sicurezza vs. usabilità



Most secure - Blackphone

- È uno *smartphone* sviluppato dalla SGP Technologies (join venture tra GeeksPhone e Silent Cirle).
- In commercio a partire dal 30 giugno 2014.
- L'hardware e le prestazioni sono quelle comuni a uno *smartphone* commerciale di livello medio-alto.

Most secure - Blackphone

Caratteristiche:

- Operazioni di **cancellazione** e protezione dei dati attivabili da **remoto**.
- Navigazione e ricerca **sicure** (tramite VPN).
- Trasferimento e stoccaggio dei file **sicuri** (cifratura del dispositivo).
- Voce, video e messaggi **sicuri**.
- Centro di **sicurezza** Blackphone.

Most secure - Neo900

Il progetto **Neo900** punta alla realizzazione del successore del **Nokia N900**, con una CPU più veloce, un maggiore quantitativo di RAM ed un modem LTE. Lo sviluppo parte dalla piattaforma esistente **OpenPhoenux GTA04**: matura, stabile e libera. Tutto ciò seguendo lo **spirito di libertà** che ha caratterizzato i dispositivi Openmoko.

Most secure - Neo900

- Il Neo900 è una **piattaforma aperta** (*open hardware*).
- È possibile scaricare e visualizzare le **specifiche complete**, compresi gli schemi elettrici e le connessioni tra i componenti.

Most secure - Neo900

- La **privacy dell'utente**, insieme al pieno controllo della piattaforma, è una delle **priorità più elevate**.

More secure

- Usare dispositivi elettronici **senza accesso alla rete telefonica**.
- Tablet Nexus della Google
- Non usare la rete telefonica
  - Nessuna chiamata vocale
  - Nessun SMS

Secure

- Modificare il **software** dello smartphone, non l'**hardware**.
- Come facciamo ad essere sicuri che ciò che stiamo installando ci **protegga davvero**?

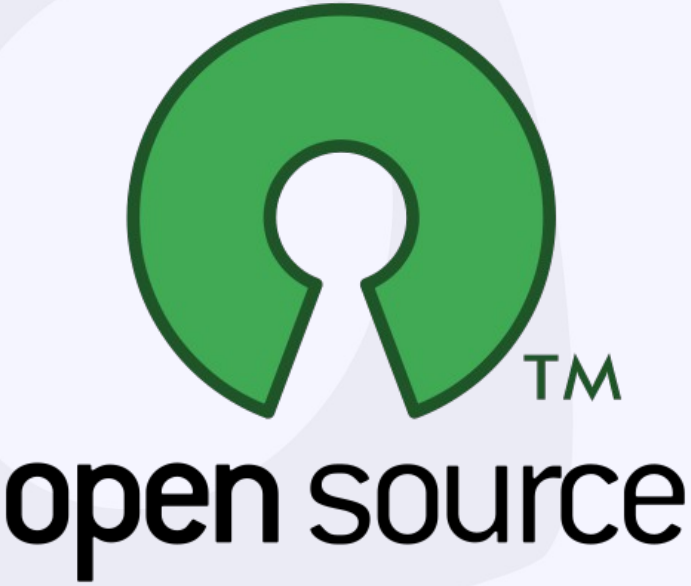
Che fare?

Come facciamo ad essere sicuri che le varie soluzioni presenti in commercio **ci proteggano**?

- Possiamo fidarci e basta.
- Possiamo pagare e fidarci.
- Possiamo **controllare noi stessi** il funzionamento del software.

Soluzione

Il codice sorgente del ***free software*** (e del software ***open source***) è accessibile e modificabile liberamente da ognuno di noi.



Da dove iniziare?

- **PRISM break** prism-break.org
- **Reset the Net** www.resetthenet.org
- **Electronic Frontier Foundation** www.eff.org
- **The Digital First Aid Kit**
  digitaldefenders.org/digitalfirstaid
- **The Guardian Project** guardianproject.info

PRISM Break

prism-break.org è un sito che raccoglie tutte le tecnologie che ognuno di noi può utilizzare per tutelare la propria privacy su internet.

Reset the Net

Protesta attiva contro la sorvegliaza globale organizzato dall'associazione no-profit Fight for The Future al fine di ottenere una **maggiore privacy** nelle comunicazioni elettroniche

Electronic Frontier Foundation

*[...] è un'organizzazione internazionale non profit di avvocati e legali rivolta alla tutela dei **diritti digitali** e della **libertà di parola** nel contesto dell'odierna era digitale.*

Wikipedia

it.wikipedia.org/wiki/Electronic_Frontier_Foundation

EFF's SSD - ssd.eff.org

Il 23 ottobre 2014 la Electronic Frontier Foundation pubblica la **Surveillance Self Defense**.

La SSD è una guida (teorica e pratica) utile a coloro che vogliono difendersi dalla sorveglianza digitale.

The Digital First Aid Kit

L'obiettivo del Digital First Aid Kit è di dare un **primo supporto** alle persone che hanno a che fare con le minacce elettroniche più comuni.

Il Kit offre una serie di **strumenti** di auto-diagnosi utili ai difensori per i diritti umani, ai blogger, agli attivisti ed ai giornalisti; così come delle **linee guida** per assistere digitalmenete chi si trova sotto attacco.

The Guardian Project

The Guardian Project è una **comunità globale** di sviluppatori software, designer, avvocati, attivisti ed istruttori impegnati nella creazione o nel miglioramento di programmi per la **sicurezza in ambito mobile**.

THE GUARDIAN PROJECT
https://guardianproject.info

Internet “non va”? Mesh network

Una rete mesh è una rete **peer-to-peer decentralizzata**, ogni collegamento è controllato dall'utente ed è in genere wireless.

Ogni nodo trasmette i propri dati e serve come **ripetitore** per gli altri nodi.

Tutti i nodi dunque **cooperano** nella distribuzione delle informazioni all'interno della rete.

Internet “non va”? Mesh network

Nel fine settimana del 27-28 settembre 2014 il **governo cinese** ha deciso di **spegnere** la rete cellulare nell'area delle proteste in Honk Kong.

Internet “non va”? Mesh network

Gli studenti hanno potuto **comunicare ugualmente** grazie ad una applicazione che crea una **rete mesh**: Firechat.

Firechat però **non garantisce privacy**, le comunicazioni viaggiano in chiaro sulla rete.

In concreto

Quali sono i software che permettono di ottenere una **maggiore privacy** ed eventualemente l'anonimato sugli *smartphone*?

Cifratura dei dati, TOR, PGP, Cyanogenmod, Replicant, F-Droid, PasswdSafe, Orbot, Orweb, K-9, APG, ChatSecure, Xabber, Ostel, CSipSimple, OsmAnd.

CyanogenMod

CyanogenMod è una ROM basata sul sistema operativo *open source* **Android**. Offre funzionalità e opzioni **non disponibili sui firmware ufficiali.**

CyanogenMod

Alcune di queste funzionalità sono il supporto nativo per i temi, codec per il Free Lossless Audio Codec, cache compressa, un'estesa lista di APN, un client OpenVPN, un menu di reboot, supporto per Wi-Fi, Bluetooth e tethering USB e altro ancora.

CyanogenMod

Permette di installare solo il software **strettamente necessario** per il funzionamento del dispositivo.

La ***privacy policy*** spiega chiaramente quali siano e come vengano usate le informazione dell'utente.

Si veda cyngn.com/legal/privacy-policy/

Replicant

Replicant è un sistema operativo basato su **Android** caratterizzato da essere formato **esclusivamente da software libero**.

Replicant

Replicant nasce dal codice sorgente di CyanogenMod eliminandone **ogni sua componente proprietaria**. Infatti Android nonostante sia distribuito sotto una licenza libera contiene in realtà alcune parti proprietarie fra cui driver e librerie.

Cifratura dei dati

È consigliato **cifrare i dati** del proprio smartphone.

Sui sistemi operativi Android-based tale operazione può essere effettuata **senza app aggiuntive**.

In caso di **smarrimento**, tali dati saranno **illeggibili**, a meno che non si conosca la *password*.

F-Droid

F-Droid è un catalogo (***repository***) di applicazioni esclusivamente libere ed *open source* per Android. In poche parole è la versione **FOSS** di Google Play.

Permette di installare solo app libere od *open source*.

F-Droid - vantaggi

- Anonimato
- Evidenza delle anti-funzionalitá
- Comunitá e sviluppo
- Catalogo offline
- Retro-compatibilitá
- Sicurezza
- Condivisione

PasswdSafe

PasswdSafe è un'applicazione **FOSS** "portata" su Android. Permette di memorizzare le *password*, gli URL dei siti, gli indirizzi e-mail e molto altro all'interno di un file cifrato. In questo modo l'utente dovrà ricordarsi soltanto la ***password* principale di accesso**.

TOR

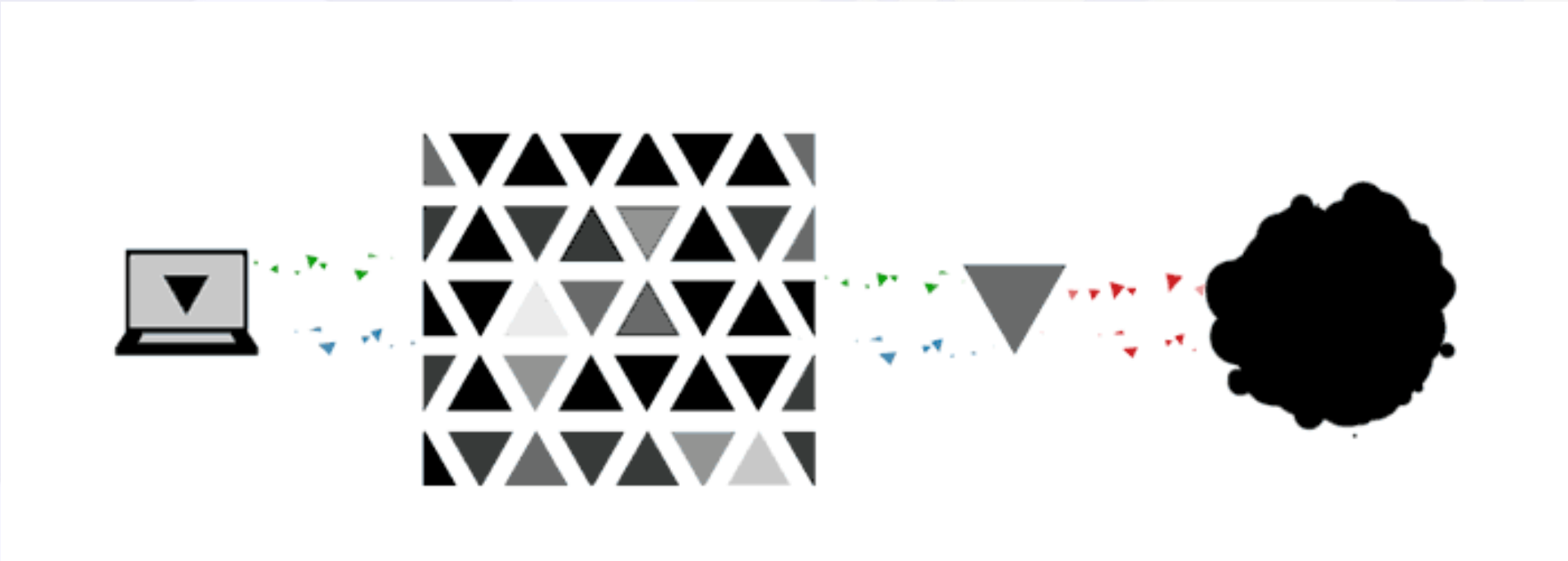
Tor (acronimo di The Onion Router) è un sistema di **comunicazione anonima** per Internet basato sulla seconda generazione del protocollo di *onion routing*. È possibile ottenere una connessione anonima ed accedere ai servizi nascosti grazie ad una **struttura stratificata** (a cipolla) ed alla **cifratura differente** nodo dopo nodo.

TOR

Il tuo computer
Il programma TOR viene eseguito sul tuo PC. Esso cifra tutti i dati e li manda nella rete TOR

Nella rete
Le informazioni cifrate, considerate indistruttibili, sono inviate alla rete TOR

Non rintracciabile
Le tue informazioni attraversano la rete TOR prendendo percorsi casuali, in questo modo l'orgine e la destinazione non sono rintracciabili

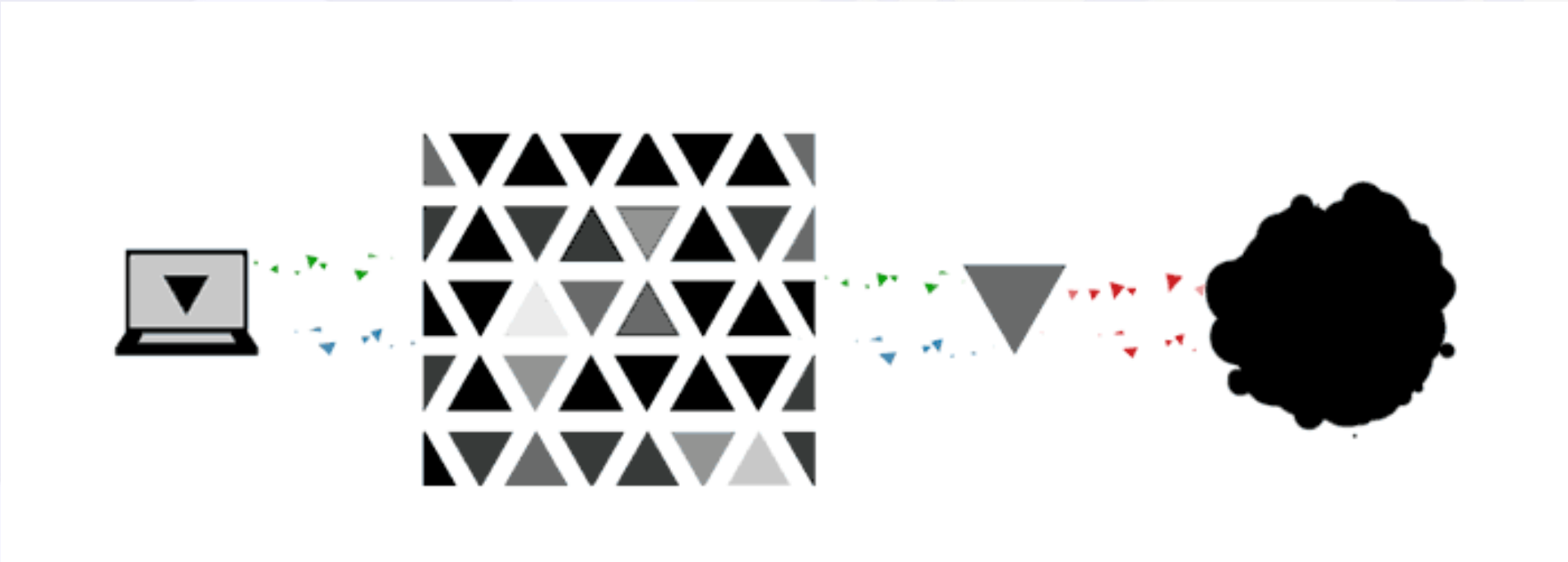


TOR

Decifratura dei dati
Il nodo di uscita decifra le informazioni non rintracciabili e le invia alla destinazione

In chiaro
Dal nodo di uscita, il flusso di dati decrifrati ma anonimi scorre dentro e fuori internet

In internet
Il sito web di destinazione non riesce a determinare la posizione dell'utente (risultando ogni volta diversa), rendendoti non identificabile



Orbot

Orbot è un client open source per la **rete Tor**, utilizzabile sui dispositivi Android. Il client permette il routing del traffico dal web browser del dispositivo, dal client e-mail, dal programma di mappe, ecc.. attraverso la rete Tor, fornendo l'**anonimato** all'utente.

Orweb

Orweb è un **browser web** per il sistema operativo Android. Esso viene usato in concomitanza con Orbot per offrire all'utente una **navigazione anonima**. Permette di raggiungere siti normalmente oscurati, monitorati, ed il web nascosto.

Firefox's Proxy Mobile Add-on

Proxy Mobile Add-on è un plug-in di Firefox (per Android) che permette all'utente di connettersi con la rete **Tor** tramite **Orbot**.

Attualmente non è più sviluppato attivamente.

PGP

Pretty Good Privacy (PGP) è un programma che permette di ottenere **autenticazione** e **privacy crittografica**. Nelle sue varie versioni è probabilmente il crittosistema più usato al mondo.

Utilizza il sistema di **cifratura asimmetrica**.

PGP

Invio del documento
Il funzionamento di PGP si basa su una coppia di chiavi: una pubblica ed una privata. Queste due chiavi devono essere usate insieme (cifratura asimmetrica)

Cifratura del documento
Il mittente sceglie una password generata casualmente e con questa cifra il messaggio. Esso viene firmato con la chiave privata e la password viene cifrata con la chiave pubblica del destinatario

PGP

Il messaggio cifrato
Il messaggio e le chiavi vengono inviate al destinatario. PGP, al contrario di TOR, non garantisce l'anonimato del mittente, ma permette di ottenere una cifratura forte delle comunicazioni

Decifratura del documento
Il destinatario verifica la firma usando la chiave pubblica del mittente, e decifra la password con la propria chiave privata. Successivamente il messaggio viene decifrato con tale password

PGP

Messaggio consegnato
Il destinatario può quindi invertire il processo usando la propria chiave privata e la chiave pubblica del mittente

K-9

K-9 Mail è un'**applicazione mail** indipendente per il sistema operativo Android. Essa è resa disponibile come software libero/*open source* sotto la licenza Apache 2.0.

K-9

Il programma è pubblicizzato come un **sostituto** più funzionale dell'**applicazione predefinita** inclusa su molti smartphone. Supporta i protocolli POP3 ed IMAP, anche se le notifiche push sono supportate solo per IMAP.

APG

Android Privacy Guard (APG) è un'applicazione *Free Software* ed *Open Source* per il sistema operativo Android. L'applicazione fornisce una **cifrature forte** e personale compatibile con i programmi **PGP** e GPG. Questo permette di cifrare, decifrare, firmare e verificare le firme di testi, e-mail e file.

Off-the-Record Messaging

OTR è un **protocollo di cifratura** che fornisce conversazioni testuali (messaggi) cifrate. OTR usa una combinazione di:

- **AES-128** - algoritmo di cifratura simmetrico con chiave a 128 bit.
- **DH-1536** - algoritmo di scambio chiavi Diffie-Hellman a gruppi di 1536 bit.
- **SHA-1** - algoritmo di hashing con risultato a 160 bit.

Off-the-Record Messaging

In aggiunta alle funzioni di autenticazione e cifratura, OTR fornisce:

- **segretezza in avanti** (perfect forward secrecy);
- **autenticazione negabile** (deniable authentication).

XMPP

Extensible Messaging and Presence Protocol (XMPP) è un insieme di **protocolli aperti** di messaggistica istantanea e presenza basato su XML.

Il software basato su XMPP è diffuso su **migliaia di server** disseminati su Internet.

XMPP

I principali **punti di forza** sono riassumibili in:

- sistema decentralizzato;
- standard aperto;
- diffusione;
- sicurezza;
- flessibilità.

ChatSecure

ChatSecure è un client di **chat cifrata** *Free Software* ed *Open Source* per i sistemi operativi iOs e Android che supporta la cifratura OTR sul protocollo XMPP.

Xabber

Xabber è un client di **chat cifrata** *Free Software* ed *Open Source* per il sistema operativo Android che supporta la cifratura OTR sul protocollo XMPP.

ChatSecure vs. Xabber

Xabber è una realizzazione di **XMPP totalmente in Java**, sopporta la cifratura OTR e la rete Tor. La sua interfaccia grafica è più semplice di ChatSecure, e non fa uso di alcun componente nativo (che sono più vulnerabili rispetto al codice Java puro). Sfortunatamente **manca di alcune funzionalità** presenti in ChatSecure, come ad esempio il trasferimento di file ed i messaggi vocali.

Tox

Tox è un servizio libero, peer-to-peer e distribuito di **messaggistica multimediale**.

Facendo uso di tecnologie esistenti, come la **rete sparsa** e la **cifrature forte**, Tox è in grado di fornire un'esperienza di messaggistica istantanea superiore rispetto a quanto il mercato possa offrire.

Ostel

Ostel è uno strumento utile per creare **chiamate telefoniche cifrate** punto-punto. È un banco di prova pubblico per il progetto OSTN (*Open Secure Telephony Network*). Esso ha come obiettivo quello di promuovere l'uso di protocolli e standard, liberi ed *open*, per potenziare le comunicazioni vocali punto-punto sicure tra i dispositivi elettronici.

CSipSimple

CSipSimple è un'applicazione VoIP, distrubuita con licenza *open source*, per il Sistema operativo Android.

È il client per Android del progetto Ostel. Permette di effettuare **chiamate vocali cifrate** con altri utenti aderenti ad Ostel.

Redphone e Textsecure?

Redphone è un'applicazione FOSS che permette di effettuare chiamate VoIP cifrate.

Textsecure è un'applicazione FOSS che permette lo scambio di messaggi cifrati.

Benché tali app siano rilasciate sotto licenza free software GPLv3 **non sono presenti** nei repository di F-Droid.

OsmAnd

OsmAnd è un'applicazione mobile open source di **navigazione e visualizzazione mappe** (online e offline) per Android in veloce sviluppo e molto completa.

Utilizza il database **OpenStreetMap OSM** come fonte primaria per le mappe.

Vantaggi

- Lo *smartphone* diventa davvero un **dispositivo personale**.
- Le informazioni “escono” con maggiore difficoltà, ed è l'utente che deve darne il consenso.
- L'utente esercita un **maggiore controllo** sul proprio *smartphone*.

Svantaggi

- Moltissime *features* vengono **rimosse**.
- Gli utenti “assuefatti” alle app più comuni si sentono, inizialmente, **spaesati**.
- Quanta comodità si è disposti a **perdere** in favore di una maggiore privacy?

Privacy

"Chi non ha nulla da nascondere non ha nulla da temere."

Ne siamo sicuri?

Privacy, perché è importante?

Abbiamo tutti la necessità di uno **spazio personale**, nel quale comportarci liberamente **senza essere giudicati**.

Sentirsi “sotto sorveglianza” **altera il comportamento** di ognuno di noi. Si diventa maggiormente conformisti e accondiscendenti.

Domande?

- Domande
- Chiarimenti
- Approfondimenti

Sitografia e link utili

Articolo The Guardian su intercettazione metadati telefonici

www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance

Tipolgie di dati sorvegliabili su di uno smartphone

www.privacyrights.org/smartphone-cell%20phone-privacy

Sitografia e link utili

Comunicato Vodafone intercettazione metadati telefonici

www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

Report Vodafone intercettazione metadati telefonici

www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf

Sitografia e link utili

Blackphone

arstechnica.com/security/2014/06/exclusive-a-review-of-the-blackphone-the-android-for-the-paranoid/

arstechnica.com/security/2014/08/blackphone-goes-to-def-con-and-gets-hacked-sort-of

Sitografia e link utili

Neo 900

neo900.org

Rendere sicuro il proprio smartphone o tablet

blog.torproject.org/blog/mission-impossible-hardening-android-security-and-privacy

Reti mesh, caso reale ad Honk Kong

www.newscientist.com/article/dn26285-hong-kong-protesters-use-a-mesh-network-to-organise.html

Sitografia e link utili

PGP

it.wikipedia.org/wiki/Pretty_Good_Privacy

Animazioni TOR e PGP

www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/4

Cyanogenmod

it.wikipedia.org/wiki/CyanogenMod

Sitografia e link utili

Replicant

it.wikipedia.org/wiki/Replicant_%28sistema_operativo%29

F-Droid

it.wikipedia.org/wiki/F-Droid

PasswdSafe

prism-break.org/en/projects/passwdsafe/

Sitografia e link utili

Orbot

en.wikipedia.org/wiki/Orbot

Orweb

guardianproject.info/apps/orweb/

Firefox's Proxy Mobile Add-on

guardianproject.info/apps

K-9

en.wikipedia.org/wiki/K-9_Mail

Sitografia e link utili

APG

en.wikipedia.org/wiki/Android_Privacy_Guard

ChatSecure

chatsecure.org

ChatSecure vs. Xabber

blog.torproject.org/blog/mission-impossible-hardening-android-security-and-privacy

Sitografia e link utili

Tox

tox.im

wiki.tox.im/FAQ

Ostel

guardianproject.info/apps

CsipSimple

en.wikipedia.org/wiki/CsipSimple

Sitografia e link utili

RedPhone e TextSecure

whispersystems.org

RedPhone e TextSecure non presenti nei repository di F-Droid

f-droid.org/posts/security-notice-textsecure

f-droid.org/forums/topic/redphone-and-textsecure

Sitografia e link utili

OsmAnd

it.wikipedia.org/wiki/OsmAnd

Why privacy matters

www.ted.com/talks/glenn_greenwald_why_privacy_matters

Sitografia e link utili

XMPP

it.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol

OTR

en.wikipedia.org/wiki/Off-the-Record_Messaging

Grazie a tutti

Ing. Mainardi Davide

 @ingMainardi

 is.gd/05kWjX