



2 Applicazione

dell'Applicazione

Applicazioni

Attacchi possibili WhatsApp VS Signal VS Telegram

4 Signal

Storia dell'Applicazione

A seguito del nuovo rilascio delle applicazioni nel 2011 i due servizi assumono la

propria natura **open-source** che ancora oggi caratterizza l'applicazione Signal.

SIGNAL

Applicazione Signal

—Storia dell'Applicazione

- Applicazione Signal

Nel 2011 Twitter acquista Whisper Systems e Marlinspike diventa capo della cybersecurity del social media. Nel 2013 Marlinspike abbandona Twitter e fonda la OWS. Nello stesso anno inizia a lavorare al protocollo Signal insieme al fondatore di WhatsApp Trevor Perrin.

Applicazione Signal Starle dell'Applications





A sequito del nuovo rilascio delle applicazioni nel 2011 i due seguiti assumono li

propria natura open-source che ancora ossi caratterizza l'applicazione Signal









dell'Applicazione

Protocollo Signal

Applicazioni

4 Signal

Attacchi possibili

WhatsApp VS Signal VS Telegram

propria natura **open-source** che ancora oggi caratterizza l'applicazione Signal. Nel 2013 Marlinspike fonda il progetto open-source Open Whisper Systems, grazie a cui rilascia la prima versione di Signal nel 2015 (anche per PC come applicazione Chrome), per poi rilasciarlo anche per Windows, Mac e Linux nel 2017.

A seguito del nuovo rilascio delle applicazioni nel 2011 i due servizi assumono la

SIGNAL

Applicazione Signal

—Storia dell'Applicazione

Applicazione Signal Nel 2011 Twitter acquista Whisper Systems e Marlinspike diventa capo della cybersecurity del social media. Nel 2013 Marlinspike abbandona Twitter e fonda la OWS.

Nello stesso anno inizia a lavorare al protocollo Signal insieme al fondatore di WhatsApp Trevor Perrin.

Applicazione Signal Storia dell'Applicazione

A seguito del nuovo rilagrio delle applicazioni nel 2011 i due seguiti assumono li

propria natura open-source che ancora ossi caratterizza l'applicazione Signal Nel 2013 Marlinspike fonda il progetto open-source Open Whisper Systems

grazie a cui rilascia la prima versione di Signal nel 2015 (anche per PC come applicazione Chrome), per poi rilasciarlo anche per Windows. Mac e Linux nel 201



Applicazione Signal Storia dell'Applicazione Applicazione Signal

Nel febbrain 2018 Marlinsnike e il co-fondatore di WhatsAnn Brian Acton fondarono la Signal Foundation. il cui obiettivo è il supporto e l'accelerazione

2 Applicazione

dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia Applicazioni

4 Signal

Attacchi possibili

WhatsApp VS Signal VS Telegram

Nel febbraio 2018 Marlinspike e il co-fondatore di WhatsApp Brian Acton

della diffusione della comunicazione privata e sicura. [Lumer]

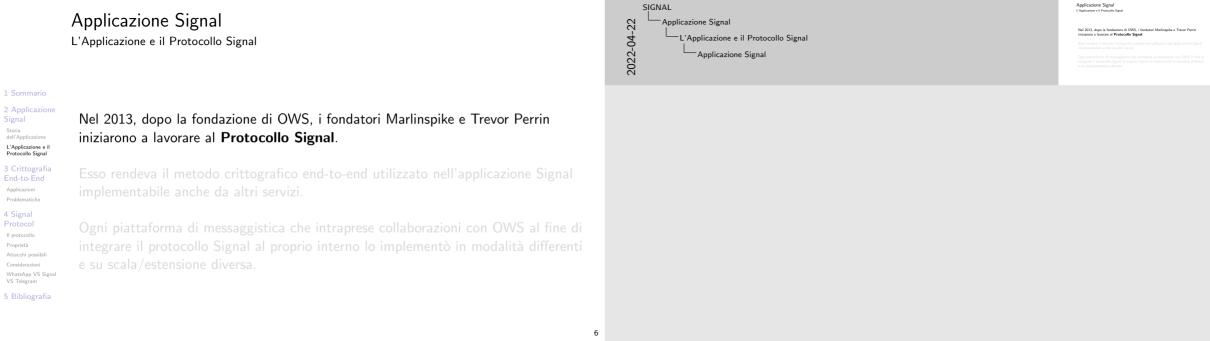
fondarono la **Signal Foundation**, il cui obiettivo è il supporto e l'accelerazione

SIGNAL

Applicazione Signal Storia dell'Apolicazione









SIGNAL

Applicazione Signal

L'Applicazione e il Protocollo Signal

Applicazione Signal

Applicazione Signal

iniziarono a lavorare al Protocollo Signal

Nel 2013, dono la fondazione di CWS, i fondatori Marlinsnike e Treure Perrin

Esso rendeva il metodo crittografico end-to-end utilizzato nell'applicazione Signal

Nel 2013, dopo la fondazione di OWS, i fondatori Marlinspike e Trevor Perrin

Esso rendeva il metodo crittografico end-to-end utilizzato nell'applicazione Signal

implementabile anche da altri servizi.

4 Signal

2 Applicazione

dell'Applicazione L'Applicazione e il Protocollo Signal 3 Crittografia

Applicazioni

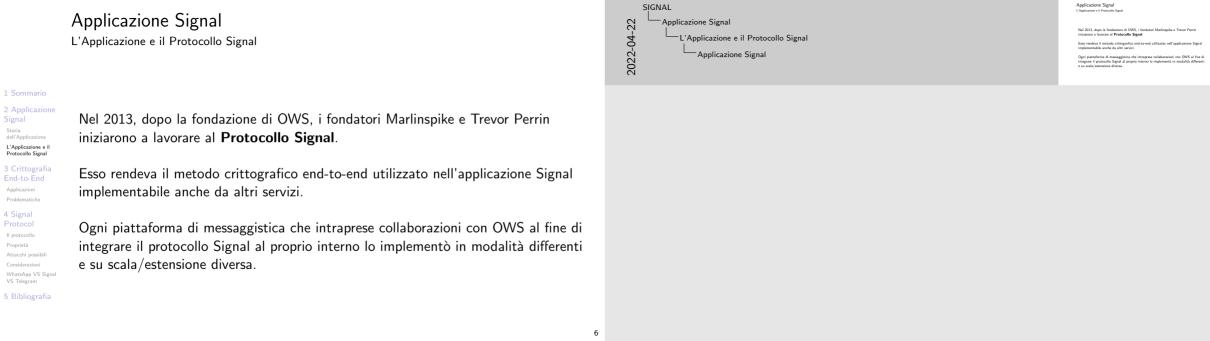
Protocol II protocollo Attacchi possibili

VS Telegram

WhatsApp VS Signal







L'Applicazione e il Protocollo Signal

- 2 Applicazione
- dell'Applicazione
- L'Applicazione e
- Protocollo Signal

- 4 Signal

- Attacchi possibili

- WhatsApp VS Signal

Tra le più note implementazioni (parziali) del Protocollo Signal troviamo:

- ► Facebook: introdusse la feature Secret Conversations per gli utenti di

L'Applicazione e il Protocollo Signal Applicazione Signal

Applicazione Signal

SIGNAL

Facebook: usa Signal solo nelle Secret Conversations

• Duo: applicazione per videochiamate e chat mobile di Google

Google: introduce Signal di default nell'applicazione di messaggi su Android

• Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019

• Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016

L'Applicazione e il Protocollo Signal

- 2 Applicazione
- dell'Applicazione
- L'Applicazione e
- Protocollo Signal

- 4 Signal

- Attacchi possibili
- WhatsApp VS Signal

- - Facebook Messenger nel luglio 2016 Allo: rilasciata nel settembre 2016, sfruttava il Protocollo Signal se utilizzata

► Facebook: introdusse la feature Secret Conversations per gli utenti di

Tra le più note implementazioni (parziali) del Protocollo Signal troviamo:

SIGNAL

Applicazione Signal

L'Applicazione e il Protocollo Signal

• Duo: applicazione per videochiamate e chat mobile di Google

Google: introduce Signal di default nell'applicazione di messaggi su Android

Applicazione Signal Facebook: usa Signal solo nelle Secret Conversations • Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019

• Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016

Applicazione Signal

Tra le niù note implementazioni (narziali) del Protocollo Signal troviamo

L'Applicazione e il Protocollo Signal

- 2 Applicazione
- dell'Applicazione
- L'Applicazione e Protocollo Signal

4 Signal

Attacchi possibili WhatsApp VS Signal

Tra le più note implementazioni (parziali) del Protocollo Signal troviamo:

- ► Facebook: introdusse la feature Secret Conversations per gli utenti di Facebook Messenger nel luglio 2016
 - Allo: rilasciata nel settembre 2016, sfruttava il Protocollo Signal se utilizzata in modalità incognito
- **Duo**: protezione delle videochat

Applicazione Signal L'Applicazione e il Protocollo Signal Applicazione Signal

SIGNAL

Tra le niù note implementazioni (narziali) del Protocollo Signal troviamo Facebook Messenger nel luglio 2016 ► Allo: rilasciata nel settembre 2016. sfruttava il Protocollo Signal se utilizzata

- Facebook: usa Signal solo nelle Secret Conversations
- Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019
 - Duo: applicazione per videochiamate e chat mobile di Google
- Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016
- Google: introduce Signal di default nell'applicazione di messaggi su Android

L'Applicazione e il Protocollo Signal

- 2 Applicazione
- dell'Applicazione
- L'Applicazione e Protocollo Signal

4 Signal

Attacchi possibili WhatsApp VS Signal

- Tra le più note implementazioni (parziali) del Protocollo Signal troviamo:
 - ► Facebook: introdusse la feature Secret Conversations per gli utenti di Facebook Messenger nel luglio 2016
 - Allo: rilasciata nel settembre 2016, sfruttava il Protocollo Signal se utilizzata in modalità incognito
- **Duo**: protezione delle videochat
- **Skype**: conversazioni private dal 2018

SIGNAL

Applicazione Signal Tra le niù note implementazioni (narziali) del Protocollo Signal troviamo Facebook Messenger nel luglio 2016 L'Applicazione e il Protocollo Signal ► Allo: rilasciata nel settembre 2016. sfruttava il Protocollo Signal se utilizzata - Applicazione Signal

- Facebook: usa Signal solo nelle Secret Conversations
- Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019
- Duo: applicazione per videochiamate e chat mobile di Google
- Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016
- Google: introduce Signal di default nell'applicazione di messaggi su Android

L'Applicazione e il Protocollo Signal

- 2 Applicazione
- dell'Applicazione
- L'Applicazione e
- Protocollo Signal 3 Crittografia

4 Signal

Attacchi possibili WhatsApp VS Signal

VS Telegram

- Tra le più note implementazioni (parziali) del Protocollo Signal troviamo:
 - ► Facebook: introdusse la feature Secret Conversations per gli utenti di Facebook Messenger nel luglio 2016
 - Allo: rilasciata nel settembre 2016, sfruttava il Protocollo Signal se utilizzata in modalità incognito
- **Duo**: protezione delle videochat
- **Skype**: conversazioni private dal 2018
- ▶ WhatsApp: tra le maggiori applicazioni che implementano Signal è l'unica

L'Applicazione e il Protocollo Signal Applicazione Signal Facebook: usa Signal solo nelle Secret Conversations • Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019

- Tra le niù note implementazioni (narziali) del Protocollo Signal troviamo Facebook Messenger nel luglio 2016 ► Allo: rilasciata nel settembre 2016. sfruttava il Protocollo Signal se utilizzata ► Dup: protezione delle videochat

Applicazione Signal

SIGNAL

- Duo: applicazione per videochiamate e chat mobile di Google
- Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016
- Google: introduce Signal di default nell'applicazione di messaggi su Android



Tra le più note implementazioni (parziali) del Protocollo Signal troviamo:

- ► Facebook: introdusse la feature Secret Conversations per gli utenti di
- Facebook Messenger nel luglio 2016 Allo: rilasciata nel settembre 2016, sfruttava il Protocollo Signal se utilizzata
- in modalità incognito
- **Duo**: protezione delle videochat
- **Skype**: conversazioni private dal 2018
- ▶ WhatsApp: tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da

Attacchi possibili WhatsApp VS Signal aprile 2016)

2 Applicazione

dell'Applicazione

L'Applicazione e

Protocollo Signal

4 Signal

[Gre29], [Lumer]

SIGNAL

Duo: applicazione per videochiamate e chat mobile di Google

Applicazione Signal

Whatsapp: introdusse Signal per la prima volta nel 2014 per utenti Android, estendendolo a tutti gli utenti nel 2016

L'Applicazione e il Protocollo Signal

Facebook: usa Signal solo nelle Secret Conversations

Applicazione Signal

Google: introduce Signal di default nell'applicazione di messaggi su Android

• Allo: applicazione mobile di messaggistica istantanea di Google, non esiste più dal 12 marzo 2019

Tra le niù note implementazioni (narziali) del Protocollo Signal troviamo ► Facebook: introdusse la feature Secret Conversations per eli utenti di Facebook Messenger nel luglio 2016

► Skyne: conversazioni private dal 2018

► Allo: rilasciata nel settembre 2016. sfruttava il Protocollo Signal se utilizzata

► WhatsApp: tra le mazziori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da

Applicazione Signal

[Gre29], [Lumer]



L'Applicazione e il Protocollo Signal

contenuto che viene scambiato

2 Applicazione

dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia

Applicazioni

4 Signal

VS Telegram

Attacchi possibili

WhatsApp VS Signal



Ciascuna di queste features richiede che le conversazioni intraprese siano dichiarate "private" affinché sia possibile applicare la crittografia end-to-end su tutto il

SIGNAL

Applicazione Signal L'Applicazione e il Protocollo Signal Applicazione Signal

Ciascuna di queste features richiede che le conversazioni intraprese siano dichiarat "nrivate" affinché sia nossibile annicare la crittografia end-to-end su tutto il

Applicazione Signal

La dichiarazione delle conversazioni come "private" avviene in genere per selezione esplicita da parte dell'utente e non di default.

WhatsApp implementa automaticamente la crittografia end-to-end sia per le chat private che per quelle di gruppo, tuttavia se si vuole verificare che le conversazioni siano private è necessario che entrambe le persone che partecipano alla conversazione selezionino la chat di interesse, clicchino sul nome del contatto, selezionino l'opzione "Crittografia" e scannerizzino il codice QR che viene presentato sul dispositivo dell'altro utente oppure confrontino i numeri a 60 cifre presentati.

L'Applicazione e il Protocollo Signal

contenuto che viene scambiato

2 Applicazione

dell'Applicazione

Protocollo Signal 3 Crittografia

Applicazioni

4 Signal

L'Applicazione e

[Mar16]

Attacchi possibili

WhatsApp VS Signal

Inoltre, conversazioni già avvenute non possono essere protette applicando il protocollo ex post.

"private" affinché sia possibile applicare la crittografia end-to-end su tutto il

Ciascuna di queste features richiede che le conversazioni intraprese siano dichiarate

SIGNAL

Applicazione Signal L'Applicazione e il Protocollo Signal - Applicazione Signal

Ciascuna di queste features richiede che le conversazioni intraprese siano dichiarat "nrivate" affinché sia nossibile annicare la crittografia end-to-end su tutto il Inoltre, conversazioni già avvenute non possono essere protette applicando i protocollo av post

Applicazione Signal

La dichiarazione delle conversazioni come "private" avviene in genere per selezione esplicita da parte dell'utente e non di default.

WhatsApp implementa automaticamente la crittografia end-to-end sia per le chat private che per quelle di gruppo, tuttavia se si vuole verificare che le conversazioni siano private è necessario che entrambe le persone che partecipano alla conversazione selezionino la chat di interesse, clicchino sul nome del contatto, selezionino l'opzione "Crittografia" e scannerizzino il codice QR che viene presentato sul dispositivo dell'altro utente oppure confrontino i numeri a 60 cifre presentati.

La sicurezza garantita dall'implementazione del protocollo è relativa al fatto che

tutti i prodotti OWS sono incentrati sulla privacy degli utenti, infatti:

L'Applicazione e il Protocollo Signal

- 2 Applicazione

dell'Applicazione

L'Applicazione e il Protocollo Signal 3 Crittografia

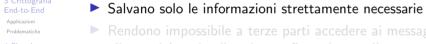
4 Signal

VS Telegram

WhatsApp VS Signal

▶ Rendono impossibile a terze parti accedere ai messaggi o ai file scambiati tra

Attacchi possibili







SIGNAL





L'Applicazione e il Protocollo Signal

2 Applicazione

dell'Applicazione L'Applicazione e i Protocollo Signal

3 Crittografia

4 Signal

Attacchi possibili

WhatsApp VS Signal

VS Telegram

La sicurezza garantita dall'implementazione del protocollo è relativa al fatto che tutti i prodotti OWS sono incentrati sulla privacy degli utenti, infatti:

- ► Salvano solo le informazioni strettamente necessarie
- ▶ Rendono impossibile a terze parti accedere ai messaggi o ai file scambiati tra gli utenti (grazie alla crittografia end-to-end)

[Lumer]

L'Applicazione e il Protocollo Signal Applicazione Signal

tutti i prodotti OWS sono incentrati sulla privacy deeli utenti. infatti

► Rendono impossibile a terze parti accedere ai messaggi o ai file scambiati tra

eli utenti (grazie alla crittografia end-to-end)

Applicazione Signal









SIGNAL

2 Applicazione

dell'Applicazione

3 Crittografia

End-to-End

Applicazioni

4 Signal

Attacchi possibil

WhatsApp VS Signal

La crittografia End-to-End (E2EE) è un processo di comunicazione sicura che impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro.

Crittografia End-to-End End-to-End Encryption

SIGNAL

End-to-End Encryption

La crittografia End-to-End (E2EE) è un processo di comunicazione sicura ch impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro.

Dati protetti da crittografia sono tali per cui solamente le persone autorizzate possono leggerne il contenuto in chiaro, mentre per tutti gli altri utenti si tratta di dati presentati in un formato non leggibile

Grazie alla E2EE è possibile proteggere i dati trasmessi da terze parti malintenzionate che possono includere i provider dei servizi di telecomunicazione. gli Internet provider e utenti malevoli

La E2EE si assicura inoltre che le comunicazioni tra due endpoint siano sicure.

2 Applicazione

dell'Applicazione

3 Crittografia

End-to-End

Applicazioni

4 Signal

Attacchi possibil

La crittografia End-to-End (E2EE) è un processo di comunicazione sicura che impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro.

Solamente gli utenti che sono in possesso della chiave segreta possono decifrare il testo cifrato e leggere il messaggio come plaintext.

Crittografia End-to-End La crittografia End-to-End (E2EE) è un processo di comunicazione sicura ch impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro. --- End-to-End Encryption Solamente eli utenti che sono in possesso della chiave segreta possono decifrare il Dati protetti da crittografia sono tali per cui solamente le persone autorizzate possono leggerne il contenuto in chiaro, mentre per tutti gli altri utenti

End-to-End Encryption

si tratta di dati presentati in un formato non leggibile

Grazie alla E2EE è possibile proteggere i dati trasmessi da terze parti malintenzionate che possono includere i provider dei servizi di telecomunicazione. gli Internet provider e utenti malevoli

La E2EE si assicura inoltre che le comunicazioni tra due endpoint siano sicure.

SIGNAL

2 Applicazione

dell'Applicazione

3 Crittografia

End-to-End

4 Signal

Attacchi possibil

La crittografia End-to-End (E2EE) è un processo di comunicazione sicura che impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro.

Solamente gli utenti che sono in possesso della chiave segreta possono decifrare il testo cifrato e leggere il messaggio come *plaintext*.

In linea di massima E2EE garantisce che potenziali eavesdroppers non possano accedere alle chiavi necessarie per decifrare la conversazione. [Gre15]

Crittografia End-to-End La crittografia End-to-End (E2EE) è un processo di comunicazione sicura ch impedisce a terze parti di accedere ai dati trasferiti da un utente a un altro End-to-End Encryption Solamente eli utenti che sono in possesso della chiave segreta possono decifrare il accedere alle chiavi necessarie per decifrare la conversazione. [Gre15]

End-to-End Encryption

Dati protetti da crittografia sono tali per cui solamente le persone autorizzate possono leggerne il contenuto in chiaro, mentre per tutti gli altri utenti si tratta di dati presentati in un formato non leggibile Grazie alla E2EE è possibile proteggere i dati trasmessi da terze parti malintenzionate che possono includere i provider dei servizi di telecomunicazione

gli Internet provider e utenti malevoli

La E2EE si assicura inoltre che le comunicazioni tra due endpoint siano sicure.

SIGNAL

E2EE si basa sulla crittografia asimmetrica.

- 2 Applicazione Signal

Storia dell'Applicazione

3 Crittografia

End-to-End

4 Signal



Al contrario, la crittografia simmetrica utilizza una sola chiave privata per cifrare il WhatsApp VS Signa

chiavi distinte: La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario

La crittografia asimmetrica, o a chiave pubblica, cifra e decifra i dati usando due

In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente

SIGNAL

dunque conservabili solo in ciphertext.

Crittografia End-to-End

End-to-End Encryption

Al contrario, il destinatario sarà in grado di ricevere i dati e decifrarli per sé.

I messaggi vengono crittografati dal mittente, pertanto, anche se intercettati da una terza persona, essi non le saranno visibili in plaintext e saranno

End-to-End Encryption





La crittografia asimmetrica, o a chiave pubblica, cifra e decifra i dati usando due

2 Applicazione Signal

Storia dell'Applicazione

3 Crittografia

End-to-End

4 Signal

WhatsApp VS Signa

E2EE si basa sulla crittografia asimmetrica.

La crittografia asimmetrica, o a chiave pubblica, cifra e decifra i dati usando due chiavi distinte:

- La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario
- della chiave pubblica In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente

Al contrario, la crittografia simmetrica utilizza una sola chiave privata per cifrare il

SIGNAL

Crittografia End-to-End End-to-End Encryption I messaggi vengono crittografati dal mittente, pertanto, anche se intercettati da una terza persona, essi non le saranno visibili in plaintext e saranno dunque conservabili solo in ciphertext.

La crittografia asimmetrica, o a chiave pubblica, cifra e decifra i dati usando due ► La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario

End-to-End Encryption

Al contrario, il destinatario sarà in grado di ricevere i dati e decifrarli per sé.

2 Applicazione Signal

dell'Applicazione

3 Crittografia

End-to-End

4 Signal

WhatsApp VS Signa

E2EE si basa sulla crittografia asimmetrica.

La crittografia asimmetrica, o a chiave pubblica, cifra e decifra i dati usando due chiavi distinte:

- La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario della chiave pubblica
- ▶ In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente chiave privata.

Al contrario, la crittografia simmetrica utilizza una sola chiave privata per cifrare il

I messaggi vengono crittografati dal mittente, pertanto, anche se intercettati da una terza persona, essi non le saranno visibili in plaintext e saranno

SIGNAL

Crittografia End-to-End

La crittografia asimmetrica, o a chiave pubblica, cifra e decifra i dati usando due --- End-to-End Encryption

► La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario

End-to-End Encryption

dunque conservabili solo in ciphertext.

Al contrario, il destinatario sarà in grado di ricevere i dati e decifrarli per sé.

dell'Applicazione

Protocollo Signal

3 Crittografia End-to-End

VS Telegram

WhatsApp VS Sign



2 Applicazione Signal

E2EE si basa sulla crittografia asimmetrica. La crittografia asimmetrica, o a chiave pubblica, cifra e decifra i dati usando due

chiavi distinte:

- La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario
- della chiave pubblica In seguito, il messaggio può essere decifrato solo utilizzando la corrispondente

chiave privata. Al contrario, la crittografia simmetrica utilizza una sola chiave privata per cifrare il plaintext e decifrare il ciphertext.

► La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario --- End-to-End Encryption In seguito, il messaggio può essere decifrato solo utilizzando la corrispondent Al contrario, la crittografia simmetrica utilizza una sola chiave privata per cifrare

End-to-End Encryption

La crittografia asimmetrica, o a chiave pubblica, cifra e decifra i dati usando du

I messaggi vengono crittografati dal mittente, pertanto, anche se intercettati da una terza persona, essi non le saranno visibili in plaintext e saranno dunque conservabili solo in ciphertext.

Al contrario, il destinatario sarà in grado di ricevere i dati e decifrarli per sé.

SIGNAL

Crittografia End-to-End

2 Applicazione

dell'Applicazione

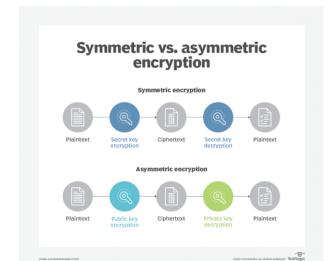
Protocollo Signal

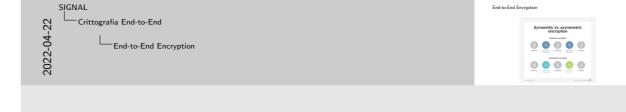
3 Crittografia
End-to-End

Applicazioni

4 Signal

Attacchi possibili Considerazioni WhatsApp VS Signal VS Telegram





Applicazioni

2 Applicazione

dell'Applicazione

Protocollo Signal

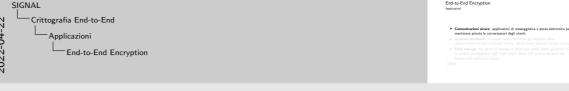
Applicazioni

4 Signal

Attacchi possibili WhatsApp VS Signal

VS Telegram

- ► Comunicazioni sicure: applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- ▶ **Gestione password**: in questo caso a entrambi gli endpoint della
- Data storage: nei servizi di storage in cloud può anche essere garantita E2EE



End-to-End Encryption

Alcuni sistemi, come ad esempio Lavabit e Hushmail, hanno in passato dichiarato di implementare la crittografia end-to-end nonostante ciò non fosse vero. [Gra 7]

Lavabit, servizio email in passato ritenuto sicuro e oggi non più attivo, nel 2014 consegnò al governo americano le chiavi che utilizzava per proteggere i dati dei propri utenti in occasione delle indagini sul caso Snowden. La controversia nacque dal fatto che la compagnia aveva in precedenza dichiarato che il proprio livello di sicurezza era tale che nemmeno gli amministratori della compagnia stessa avevano accesso al contenuto delle mail scambiate

Hushmail, altro email provider dichiarato sicuro, violò la privacy dei propri utenti utilizzandone le password per decrittare le email e consegnarle al governo federale in plaintext. [Sin 7]

Altri sistemi, come per esempio Telegram, non implementano la crittografia end-to-end di default e sono pertanto stati criticati.

In modo particolare Telegram non la implementa né per le chat di gruppo né per i client desktop. Tra le altre critiche mosse all'applicazione c'è quella di utilizzare il protocollo di crittografia non standard MTProto. [EPP 1]

dai propri utenti. [Pou16]. [GM13]

Applicazioni

dell'Applicazione Protocollo Signal

Applicazioni

4 Signal

WhatsApp VS Signal

VS Telegram

- ▶ Comunicazioni sicure: applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- ▶ **Gestione password**: in questo caso a entrambi gli endpoint della comunicazione si trova lo stesso utente, che è l'unica persona munita di chiave:

SIGNAL Crittografia End-to-End Ecomunicazioni sicure: annicazioni di messaggistica e nosta elettronica ner mantenere private le conversazioni degli utenti; -Applicazion ► Gostione nassword: in questo caso a entrambi eli endocint della End-to-End Encryption

End-to-End Encryption

Alcuni sistemi, come ad esempio Lavabit e Hushmail, hanno in passato dichiarato di implementare la crittografia end-to-end nonostante ciò non fosse vero. [Gra 7]

Lavabit, servizio email in passato ritenuto sicuro e oggi non più attivo, nel 2014 consegnò al governo americano le chiavi che utilizzava per proteggere i dati dei propri utenti in occasione delle indagini sul caso Snowden. La controversia nacque dal fatto che la compagnia aveva in precedenza dichiarato che il proprio livello di sicurezza era tale che nemmeno gli amministratori della compagnia stessa avevano accesso al contenuto delle mail scambiate dai propri utenti. [Pou16]. [GM13]

Hushmail, altro email provider dichiarato sicuro, violò la privacy dei propri utenti utilizzandone le password per decrittare le email e consegnarle al governo federale in plaintext. [Sin 7]

Altri sistemi, come per esempio Telegram, non implementano la crittografia end-to-end di default e sono pertanto stati criticati.

In modo particolare Telegram non la implementa né per le chat di gruppo né per i client desktop. Tra le altre critiche mosse all'applicazione c'è quella di utilizzare il protocollo di crittografia non standard MTProto. [EPP 1]

Applicazioni

- 2 Applicazion Signal
- dell'Applicazione L'Applicazione e
- 3 Crittogra

Applicazioni

Applicazioni Problematiche

4 Signal

- Il protocollo
 Proprietà
- Attacchi possibili Considerazioni
- Considerazioni WhatsApp VS Signal VS Telegram

V5 Telegram

- ► Comunicazioni sicure: applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- ► **Gestione password**: in questo caso a entrambi gli endpoint della comunicazione si trova lo stesso utente, che è l'unica persona munita di chiave:
- ▶ **Data storage**: nei servizi di storage in cloud può anche essere garantita E2EE *in transit*, proteggendo i dati degli utenti anche dall'accesso da parte dei fornitori del servizio in cloud:

[IBM]



dai propri utenti. [Pou16]. [GM13]

➤ Comunications sicure application of messaggistics a posts settomore per materiarie private is conversationi degli stanti;
➤ Gestione passanent in questo casa a settombi gli endopioti dalla comunicazionia e losso in siessa stettati, dell' intella pransia mentita di chiave; comunicazionia e losso in siessa stettati, dell' intella pransia mentita di chiave; con constituti della constituti della

End-to-End Encryption

Alcuni sistemi, come ad esempio Lavabit e Hushmail, hanno in passato dichiarato di implementare la crittografia end-to-end nonostante ciò non fosse vero. [Gra 7]

Lavabit, servizio email in passato ritenuto sicuro e oggi non più attivo, nel 2014 consegnò al governo americano le chiavi che utilizzava per proteggere i dati dei propri utenti in occasione delle indagini sul caso Snowden. La controversia nacque dal fatto che la compagnia aveva in precedenza dichiarato che il proprio livello di sicurezza era tale che nemmeno gli amministratori della compagnia stessa avevano accesso al contenuto delle mail scambiate

Hushmail, altro email provider dichiarato sicuro, violò la privacy dei propri utenti utilizzandone le password per decrittare le email e consegnarle al governo federale in plaintext. [Sin 7]

Altri sistemi, come per esempio Telegram, non implementano la crittografia end-to-end di default e sono pertanto stati criticati.

In modo particolare Telegram non la implementa né per le chat di gruppo né per i client desktop. Tra le altre critiche mosse all'applicazione c'è quella di utilizzare il protocollo di crittografia non standard MTProto. [EPP 1]

Problematiche

2 Applicazione Signal

Storia dell'Applicazione

3 Crittografia

Attacchi possibili

WhatsApp VS Signal









La E2EE non garantisce di per sé né la sicurezza né la privacy, in quanto i dati trasmessi potrebbero essere protetti in modo poco sicuro sui dispositivi endpoint. Tuttavia, l'implementazione della E2EE consente di applicare una protezione dei dati migliore della sola crittografia "in transit".

SIGNAL

Problematiche

Crittografia End-to-End

End-to-End Encryption

La EZEE non garantisco di nor sé né la sicusarza né la privacy in quanto i da trasmessi potrebbero essere protetti in modo poco sicuro sui dispositivi endpoint

Tuttavia l'implementazione della EZEE consente di applicare una protezione dei

End-to-End Encryption

In questo modo è possibile monitorare il contenuto dei messaggi (per esempio in cerca di contenuti offensivi o pericolosi) ma si corre anche il rischio che utenti non autorizzati e/o malintenzionati aventi accesso allo storage dei messaggi possano fare un uso improprio dei contenuti.

Nella crittografia "in transit" è possibile o salvare direttamente i messaggi decrittati oppure salvare i dati crittografati e la chiave con cui decrittarli sullo stesso database

14

Problematiche

2 Applicazione Signal

dell'Applicazione

4 Signal

Attacchi possibil WhatsApp VS Sign

Applicazioni Problematiche

VS Telegram

Tuttavia, l'implementazione della E2EE consente di applicare una protezione dei dati migliore della sola crittografia "in transit".

La E2EE non garantisce di per sé né la sicurezza né la privacy, in quanto i dati trasmessi potrebbero essere protetti in modo poco sicuro sui dispositivi endpoint.

Per molti sistemi di messaggistica i messaggi passano attraverso un intermediario che li conserva finché non vengono recuperati dal destinatario. Anche se protetti da crittografia, essi lo sono solamente in transito, quindi possono essere letti dai provider di servizi. [int20], [IBM]

SIGNAL

Crittografia End-to-End Problematiche End-to-End Encryption

trasmessi potrebbero essere protetti in modo poco sicuro sui dispositivi endpoint Tuttavia l'implementazione della EZEE consente di applicare una protezione dei dati misliore della sola crittografia "in transit" Per molti sistemi di messaggistica i messaggi passano attraverso un intermediario che E conserva finché non venzono recunerati dal destinatario. Anche se motetti d crittografia, essi lo sono solamente in transito, quindi nossono essere letti da provider di servizi. [int20], [IBM]

End-to-End Encryption

In questo modo è possibile monitorare il contenuto dei messaggi (per esempio in cerca di contenuti offensivi o pericolosi) ma si corre anche il rischio che utenti non autorizzati e/o malintenzionati aventi accesso allo storage dei messaggi possano fare un uso improprio dei contenuti.

La EZEE non garantisco di ner sé né la sicurazza né la nrivary in quanto i dat

Nella crittografia "in transit" è possibile o salvare direttamente i messaggi decrittati oppure salvare i dati crittografati e la chiave con cui decrittarli sullo stesso database

14

Problematiche

2 Applicazione Signal

dell'Applicazione

Protocollo Signal

Problematiche

4 Signal

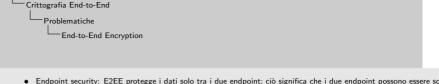
Attacchi possibili WhatsApp VS Signal

Ulteriori problematiche:

- **Endpoint security**: gli endpoint sono vulnerabili se non protetti adeguatamente
- ▶ Attacchi di tipo Man-in-the-Middle: la conversazione può essere soggetta a
- ▶ Backdoors: metodi per bypassare l'autenticazione standard o la protezione



SIGNAL



- ► Endonint security: eli endonint cono vulnerabili se non protetti

End-to-End Encryption

- Endpoint security: E2EE protegge i dati solo tra i due endpoint; ciò significa che i due endpoint possono essere soggetti ad attacchi:
- Attacchi MITM: anziché forzare la crittografia dei dati, ci si può aspettare un tentativo da parte di terzi malintenzionati di impersonare il destinatario durante. Essi possono, per esempio, impersonare il destinatario durante lo scambio di chiavi con il mittente, decifrare il messaggio inviato e poi inoltrarlo al vero destinatario senza farsi notare. Una soluzione per questo tipo di attacchi è introdurre un metodo di autenticazione (per es. certification authorities, web of trust, fingerprint numeriche o come QR code)
- Backdoors: nonostante le backdoors non siano sempre implementate volutamente, esse possono essere introdotte grazie a cyber-attacks e poi essere utilizzate per la negoziazione delle chiavi o per oltrepassare la protezione crittografica.

Problematiche

2 Applicazione

dell'Applicazione

Protocollo Signal 3 Crittografia

Problematiche

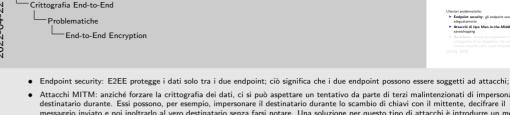
4 Signal

Attacchi possibili

WhatsApp VS Signal

Ulteriori problematiche:

- **Endpoint security**: gli endpoint sono vulnerabili se non protetti adeguatamente
- ▶ Attacchi di tipo Man-in-the-Middle: la conversazione può essere soggetta a eavesdropping
- ▶ Backdoors: metodi per bypassare l'autenticazione standard o la protezione



► Endonint security: eli endonint sono vulnerabili se non protetti

End-to-End Encryption

- Attacchi MITM: anziché forzare la crittografia dei dati, ci si può aspettare un tentativo da parte di terzi malintenzionati di impersonare il destinatario durante. Essi possono, per esempio, impersonare il destinatario durante lo scambio di chiavi con il mittente, decifrare il messaggio inviato e poi inoltrarlo al vero destinatario senza farsi notare. Una soluzione per questo tipo di attacchi è introdurre un metodo di autenticazione (per es. certification authorities, web of trust, fingerprint numeriche o come QR code)
- Backdoors: nonostante le backdoors non siano sempre implementate volutamente, esse possono essere introdotte grazie a cyber-attacks e poi essere utilizzate per la negoziazione delle chiavi o per oltrepassare la protezione crittografica.

SIGNAL

Problematiche

2 Applicazione

dell'Applicazione

Protocollo Signal 3 Crittografia

Problematiche 4 Signal

Attacchi possibili

WhatsApp VS Signa

Ulteriori problematiche:

- ▶ Endpoint security: gli endpoint sono vulnerabili se non protetti adeguatamente
- ▶ Attacchi di tipo Man-in-the-Middle: la conversazione può essere soggetta a eavesdropping
- ▶ Backdoors: metodi per bypassare l'autenticazione standard o la protezione crittografica di un dispositivo. Se non volute, possono essere introdotte

[Gre15], [IBM]

tramite attacchi cyber e poi sfruttate per violare la sicurezza del sistema

Crittografia End-to-End ► Endonint security: eli endonint sono vulnerabili se non protetti Problematiche End-to-End Encryption crittomofice of un disperition. So non-volute necessary errors introdutto • Endpoint security: E2EE protegge i dati solo tra i due endpoint; ciò significa che i due endpoint possono essere soggetti ad attacchi:

tramite attacchi coher e noi ofruttate ner violare la sicurezza del sistema

End-to-End Encryption

- Attacchi MITM: anziché forzare la crittografia dei dati, ci si può aspettare un tentativo da parte di terzi malintenzionati di impersonare il destinatario durante. Essi possono, per esempio, impersonare il destinatario durante lo scambio di chiavi con il mittente, decifrare il messaggio inviato e poi inoltrarlo al vero destinatario senza farsi notare. Una soluzione per questo tipo di attacchi è introdurre un metodo di autenticazione (per es. certification authorities, web of trust, fingerprint numeriche o come QR code)
- Backdoors: nonostante le backdoors non siano sempre implementate volutamente, esse possono essere introdotte grazie a cyber-attacks e poi essere utilizzate per la negoziazione delle chiavi o per oltrepassare la protezione crittografica.

SIGNAL

Problematiche

- 2 Applicazione
- dell'Applicazione

Problematiche

- 4 Signal
- Attacchi possibili WhatsApp VS Signal

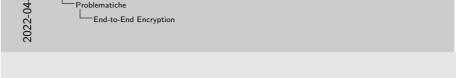
- ► Complessità nel definire gli endpoint: alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione
- Privacy "eccessiva": enti governativi non hanno modo di verificare la natura
- Metadati visibili Non vi è certezza che E2EE possa funzionare altrettanto bene con l'eventuale





SIGNAL

Crittografia End-to-End



End-to-End Encryption

► Complessità nel definire «li endonint: alcune implementazioni consentone di decodificare e ricodificare i dati lungo il percorso, quindi è necessario

definire accuratamente eli estremi della trasmissione

Problematiche

- dell'Applicazione
- Protocollo Signal

Problematiche

4 Signal

Attacchi possibili WhatsApp VS Signal

- ► Complessità nel definire gli endpoint: alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario
- definire accuratamente gli estremi della trasmissione Privacy "eccessiva": enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti
- Metadati visibili
- Non vi è certezza che E2EE possa funzionare altrettanto bene con l'eventuale

Crittografia End-to-End — Problematiche End-to-End Encryption

SIGNAL

End-to-End Encryption

di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente eli estremi della trasmissione ► Privacy "eccessiva": enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere

► Complessità nel definire «li endonint: alcune implementazioni consentone

Problematiche

- dell'Applicazione
- Protocollo Signal

Problematiche

4 Signal

Attacchi possibili

WhatsApp VS Signal

► Complessità nel definire gli endpoint: alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione

- Privacy "eccessiva": enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti
- Metadati visibili
- Non vi è certezza che E2EE possa funzionare altrettanto bene con l'eventuale

SIGNAL

Crittografia End-to-End

— Problematiche

End-to-End Encryption

► Complessità nel definire «li endonint: alcune implementazioni consentone di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente eli estremi della trasmissione ► Privacy "eccessiva": enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere

misure adequate in caso di illeciti Metadati visibili

End-to-End Encryption

Problematiche

- dell'Applicazione
- Protocollo Signal

Problematiche

4 Signal

Attacchi possibili

► Complessità nel definire gli endpoint: alcune implementazioni consentono di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione

- Privacy "eccessiva": enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti
- Metadati visibili
- Non vi è certezza che E2EE possa funzionare altrettanto bene con l'eventuale introduzione di quantum computer che rendano la crittografia obsoleta

WhatsApp VS Signal

[LB21]



End-to-End Encryption

di decodificare e ricodificare i dati lungo il percorso, quindi è necessario

introduzione di quantum computer che rendano la crittografia obsoleta

dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere

definire accuratamente eli estremi della trasmissione

misure adequate in caso di illeciti

SIGNAL

2 Applicazione

dell'Applicazione

3 Crittografia

Applicazioni

4 Signal Protocol

WhatsApp VS Signal VS Telegram

Attacchi possibili

II protocollo

End-to-End

Il protocollo Signal fornisce crittografia end-to-end a sistemi di messaggistica istantanea e di chiamate vocali, combinando l'algoritmo "Double Ratchet",

pre-chiavi e un triplo handshake Elliptic-curve Diffie-Hellman (3-DH).

17

Il protocollo Signal Protocol

SIGNAL

Signal Protocol

Signal Protocol

Il nenteralla Signal fornisco crittografia and to and a sistemi di mossaggistica istantanea e di chiamate vocali, combinando l'algoritmo "Double Ratchet" pre-chiavi e un trinlo handshake Ellintic-cupe Diffie-Hellman (3-DH)









1 Camanani

2 Applicazione Signal

dell'Applicazione L'Applicazione e Protocollo Signal

3 Crittogra

Applicazioni

4 Signal

Il protocollo

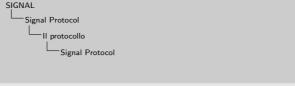
Proprietà Attacchi possibili Considerazioni

Considerazioni WhatsApp VS Signal VS Telegram

5 Bibliograf

Le specifiche di riferimento sono infatti: [sig]

- ➤ XEdDSA e VXEdDSA: algoritmi per la creazione e verifica di *signatures* compatibili con EdDSA utilizzando formati di chiavi pubbliche e private inizialmente definiti per le funzioni X25519 e X448 di Diffie-Hellman su curve ellittiche. L'algoritmo VXEdDSA estende XEdDSA rendendolo verificabile.
- ▶ Double Ratchet: algoritmo utilizzato da due parti per lo scambio di messaggi basato su una chiave segreta condivisa.
- **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
- ▶ **Sesame**: gestisce le sessioni crittografate in ambiente asincrono e multi-device.



messaggio corrente possa essere compromesso.

e specifiche di riferimento sono infatti: [sig]

> XEdDSA e VXEdDSA: algoritmi per la creazione e verifica di signatures compatibili con EdDSA utilizzando formati di chiavi pubbliche e private

compatibili con EdDSA utilizzando formati di chiavi pubbliche e private inizialmente definiti per le funzioni X25519 e X448 di Diffie-Hellman su curv ellittiche. L'algoritmo VXEdDSA estende XEdDSA rendendolo verificabile.

basato su una chiave segreta condivisa.

X3DH: nontroully di manyristime delle chiavi Evtended Triple Diffic.

Signal Protocol

X3DH: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellmi

- Double Ratchet: le due parti derivano nuove chiavi per ogni messaggio in modo tale che chiavi usate in precedenza non possano essere ricavate dalle chiavi successive.
- X3DH: stabilisce una chiave segreta condivisa da due parti che si autenticano a vicenda basandosi su chiavi pubbliche. X3DH fornisce forward secrecy e cryptographic deniability

Forward secrecy: un sistema di crittografia possiede la proprietà di forward secrecy se l'analisi in plaintext dei dati scambiati durante la fase di negoziazione delle chiavi durante l'inizializzazione della sessione di comunicazione non rivela la chiave utilizzata per cifrare il resto della sessione.

Si ottiene generando nuove chiavi di sessione per ogni messaggio e assicura che i messaggi scambiati in passato non siano decifrabili ma che al più il

Cryptographic deniability: l'esistenza di un file cifrato o di un messaggio è rinnegabile, nel senso che un altro utente non può dimostrare che i dati in plaintext esistono. Gli utenti possono negare che dei dati siano cifrati o anche negare di essere in grado di decifrarli, indipendentemente dal fatto che

- 2 Applicazione
- dell'Applicazione

4 Signal

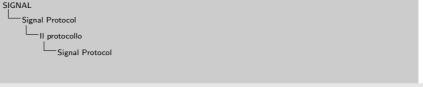
II protocollo

Attacchi possibili

WhatsApp VS Signal

Le specifiche di riferimento sono infatti: [sig]

- **XEdDSA** e **VXEdDSA**: algoritmi per la creazione e verifica di *signatures* compatibili con EdDSA utilizzando formati di chiavi pubbliche e private inizialmente definiti per le funzioni X25519 e X448 di Diffie-Hellman su curve ellittiche. L'algoritmo VXEdDSA estende XEdDSA rendendolo verificabile.
- ▶ Double Ratchet: algoritmo utilizzato da due parti per lo scambio di messaggi basato su una chiave segreta condivisa.
- ▶ X3DH: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
- **Sesame**: gestisce le sessioni crittografate in ambiente asincrono e multi-device.



compatibili con EdDSA utilizzando formati di chiavi pubbliche e private

Signal Protocol

inizialmente definiti per le funzioni X25519 e X448 di Diffie-Hellman su cury allitticha L'algoritmo VXEdDSA astenda XEdDSA randandolo varificabile ► Double Ratchet: algoritmo utilizzato da due narti ner lo scambio di messago

- Double Ratchet: le due parti derivano nuove chiavi per ogni messaggio in modo tale che chiavi usate in precedenza non possano essere ricavate dalle chiavi successive.
- X3DH: stabilisce una chiave segreta condivisa da due parti che si autenticano a vicenda basandosi su chiavi pubbliche. X3DH fornisce forward secrecy e cryptographic deniability

Forward secrecy: un sistema di crittografia possiede la proprietà di forward secrecy se l'analisi in plaintext dei dati scambiati durante la fase di negoziazione delle chiavi durante l'inizializzazione della sessione di comunicazione non rivela la chiave utilizzata per cifrare il resto della sessione.

Si ottiene generando nuove chiavi di sessione per ogni messaggio e assicura che i messaggi scambiati in passato non siano decifrabili ma che al più il

Cryptographic deniability: l'esistenza di un file cifrato o di un messaggio è rinnegabile, nel senso che un altro utente non può dimostrare che i dati in plaintext esistono. Gli utenti possono negare che dei dati siano cifrati o anche negare di essere in grado di decifrarli, indipendentemente dal fatto che ciò sia vero o meno

messaggio corrente possa essere compromesso.

1 Sommari

2 Applicazione Signal

dell'Applicazione L'Applicazione e

3 Crittogra

Applicazioni

4 Signal

Protocol Il protocollo

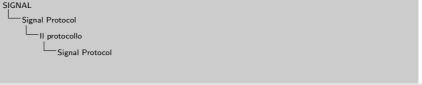
Proprietà Attacchi possibili Considerazioni

Considerazioni WhatsApp VS Signal VS Telegram

5 Bibliograf

Le specifiche di riferimento sono infatti: [sig]

- ➤ XEdDSA e VXEdDSA: algoritmi per la creazione e verifica di *signatures* compatibili con EdDSA utilizzando formati di chiavi pubbliche e private inizialmente definiti per le funzioni X25519 e X448 di Diffie-Hellman su curve ellittiche. L'algoritmo VXEdDSA estende XEdDSA rendendolo verificabile.
- ▶ Double Ratchet: algoritmo utilizzato da due parti per lo scambio di messaggi basato su una chiave segreta condivisa.
- **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
- ▶ **Sesame**: gestisce le sessioni crittografate in ambiente asincrono e multi-device.



ellstiche. L'algoritmo VXEGIDSA estande XEGIDSA enschediol verificabile.

Pouchle Rachtest: algoritmo utilizzato da deu parti per lo scambio di mossaggi
basato su una chiave segreta condivina.

* XIDH: protocollo di negoziazione della chiavi Extended Triple Diffie-Hellman.

compatibili con EdDSA utilizzando formati di chiavi pubbliche e private inizialmente definiti per le funzioni X25519 e X448 di Diffie-Hellman su curv

Signal Protocol

- Double Ratchet: le due parti derivano nuove chiavi per ogni messaggio in modo tale che chiavi usate in precedenza non possano essere ricavate dalle chiavi successive.
- X3DH: stabilisce una chiave segreta condivisa da due parti che si autenticano a vicenda basandosi su chiavi pubbliche. X3DH fornisce forward secrecy e cryptographic deniability

Forward secrecy: un sistema di crittografia possiede la proprietà di forward secrecy se l'analisi in plaintext dei dati scambiati durante la fase di negoziazione delle chiavi durante l'inizializzazione della sessione.

Si ottiene generando nuove chiavi di sessione per ogni messaggio e assicura che i messaggi scambiati in passato non siano decifrabili ma che al più il messaggio corrente possa essere compromesso.

Cryptographic deniability: l'esistenza di un file cifrato o di un messaggio è rinnegabile, nel senso che un altro utente non può dimostrare che i dati in plaintext esistono. Gli utenti possono negare che dei dati siano cifrati o anche negare di essere in grado di decifrarli, indipendentemente dal fatto che

2 Applicazione

dell'Applicazione

4 Signal

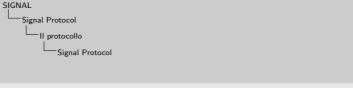
II protocollo

Attacchi possibili

WhatsApp VS Signal

Le specifiche di riferimento sono infatti: [sig]

- **XEdDSA** e **VXEdDSA**: algoritmi per la creazione e verifica di *signatures* compatibili con EdDSA utilizzando formati di chiavi pubbliche e private inizialmente definiti per le funzioni X25519 e X448 di Diffie-Hellman su curve ellittiche. L'algoritmo VXEdDSA estende XEdDSA rendendolo verificabile.
- ▶ Double Ratchet: algoritmo utilizzato da due parti per lo scambio di messaggi basato su una chiave segreta condivisa.
- **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
- **Sesame**: gestisce le sessioni crittografate in ambiente asincrono e multi-device.



messaggio corrente possa essere compromesso.

compatibili con EdDSA utilizzando formati di chiavi pubbliche e private inizialmente definiti per le funzioni X25519 e X448 di Diffie-Hellman su cury allitticha L'algoritmo VXEdDSA astenda XEdDSA randandolo varificabile ► Double Ratchet: algoritmo utilizzato da due narti ner lo scambio di messago

➤ X3DH: protocollo di neroziazione delle chiavi Extended Triple Diffie-Hellma

Signal Protocol

► Sesame: escripre le sessioni crittografate in ambiente acinconn e multi-devir

 Double Ratchet: le due parti derivano nuove chiavi per ogni messaggio in modo tale che chiavi usate in precedenza non possano essere ricavate dalle chiavi successive.

 X3DH: stabilisce una chiave segreta condivisa da due parti che si autenticano a vicenda basandosi su chiavi pubbliche. X3DH fornisce forward secrecy e cryptographic deniability

Forward secrecy: un sistema di crittografia possiede la proprietà di forward secrecy se l'analisi in plaintext dei dati scambiati durante la fase di negoziazione delle chiavi durante l'inizializzazione della sessione di comunicazione non rivela la chiave utilizzata per cifrare il resto della sessione.

Si ottiene generando nuove chiavi di sessione per ogni messaggio e assicura che i messaggi scambiati in passato non siano decifrabili ma che al più il

Cryptographic deniability: l'esistenza di un file cifrato o di un messaggio è rinnegabile, nel senso che un altro utente non può dimostrare che i dati in plaintext esistono. Gli utenti possono negare che dei dati siano cifrati o anche negare di essere in grado di decifrarli, indipendentemente dal fatto che ciò sia vero o meno

Signal Protocol XEdDSA e VXEdDSA

2 Applicazione Signal dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End Applicazioni 4 Signal Protocol Il protocollo Proprietà Attacchi possibili WhatsApp VS Signal VS Telegram

SIGNAL

Signal Protocol

☐ II protocollo

Signal Protocol

2022-04-22

Signal Protocol

Signal Protocol Double Raschet

SIGNAL

2022-04-22

20

Signal Protocol

☐ II protocollo

Signal Protocol

Double Ratchet

2 Applicazione Signal

dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End Applicazioni

4 Signal

Protocol Il protocollo Proprietà Attacchi possibili

WhatsApp VS Signal VS Telegram

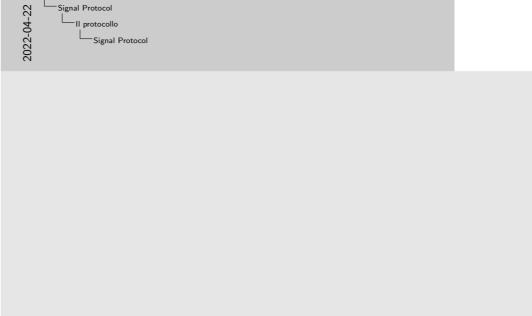
Signal Protocol X3DH 2 Applicazione Signal dell'Applicazione L'Applicazione e il Protocollo Signal 3 Crittografia End-to-End Applicazioni 4 Signal Protocol II protocollo Proprietà Attacchi possibili WhatsApp VS Signal VS Telegram 21



Signal Protocol

SIGNAL

Signal Protocol Sesame 2 Applicazione Signal dell'Applicazione L'Applicazione e il Protocollo Signal 3 Crittografia End-to-End Applicazioni 4 Signal Protocol II protocollo Proprietà Attacchi possibili WhatsApp VS Signal VS Telegram



Signal Protocol

SIGNAL

Bibliografia I

- 2 Applicazione
- dell'Applicazione
- 3 Crittografia

4 Signal

Protocol

Attacchi possibili

WhatsApp VS Signal

5 Bibliografia

CPJ Middle East, North Africa Program, and CPJ Technology Program.

- Why telegram's security flaws may put iran's journalists at risk committee to protect journalists. 2016. May 1.
- Barton Gellman and Jerry Markon.
 - Edward snowden says motive behind leaks was to expose 'surveillance state'.
- The Washington Post, June 10, 2013.

2015, October 7.

- Yael Grauer.
 - Mr. robot uses protonmail, but it still isn't fully secure.

Bibliografia I

Barton Gellman and Jerry Markon Mr. robot uses protonmail, but it still isn't fully secure

TP I Middle Fast, North Africa Program, and CPJ Technology Program. Why telegram's security flaws may put iran's journalists at risk - committee t

SIGNAL

- Bibliografia

Bibliografia

23



Bibliografia III

- 2 Applicazione
- dell'Applicazione

4 Signal Protocol

Attacchi possibili WhatsApp VS Signal

VS Telegram







3 Crittografia







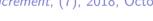




David J Lumb.

The story of signal.







Whatsapp's signal protocol integration is now complete.

Apr. 5, 2016.

K Poulsen.

Snowden's email provider loses appeal over encryption keys.

Signal documentation.

2014, April 16.

SIGNAL

Bibliografia

____Bibliografia

Whatsapp's signal protocol integration is now complete. R K Poulsen. Signal documentation

Bibliografia III

David Llumb The story of signal. Movie Martinonike

Bibliografia IV Ryan Singel. Encrypted e-mail company hushmail spills to feds.

L'Applicazione e il Protocollo Signal 3 Crittografia

Applicazioni

4 Signal

Protocol

Proprietà Attacchi possibili

WhatsApp VS Signal

VS Telegram

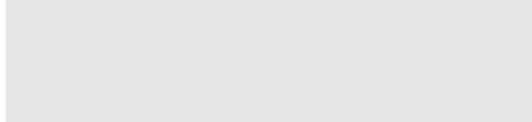
2 Applicazione

2007, November 7.

dell'Applicazione

End-to-End





Bibliografia IV

Ryan Singel.

Encrypted e-mail company hushmail spills to feds.

SIGNAL

2022-04-22

-Bibliografia

Bibliografia