



2 Applicazione

dell'Applicazione

Applicazioni

4 Signal

VS Telegram

II protocollo Attacchi possibili WhatsApp VS Signal

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

Storia dell'Applicazione

- Applicazione Signal

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

Protocol II protocollo

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

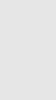
—Storia dell'Applicazione Applicazione Signal Nel 2011 Twitter acquista Whisper Systems e Marlinspike diventa capo della cybersecurity del social media. Nel 2013 Marlinspike abbandona Twitter e fonda la OWS. Nello stesso anno inizia a lavorare al protocollo Signal insieme al fondatore di WhatsApp Trevor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





SIGNAL

Applicazione Signal

Storia dell'Applicazione 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 Applicazione Signal

Applicazione Signal Storia dell'Apolicazione

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

3 Crittografia Applicazioni

4 Signal

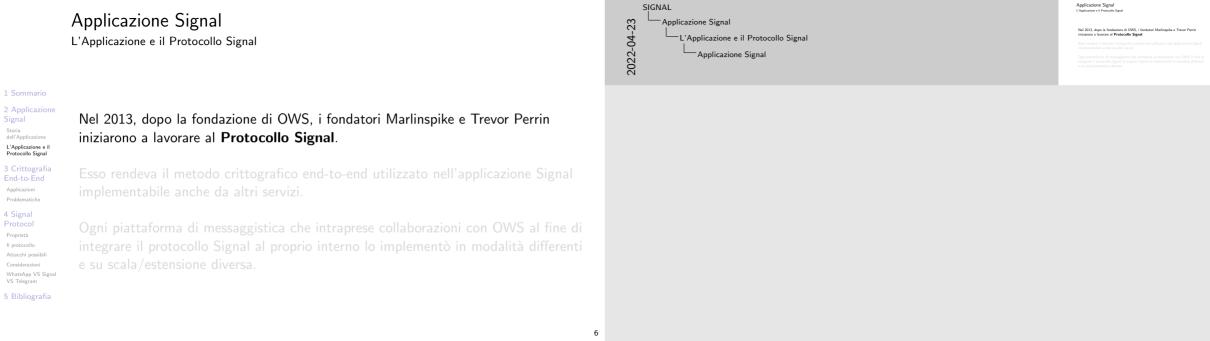
II protocollo Attacchi possibili

WhatsApp VS Signal VS Telegram

della diffusione della comunicazione privata e sicura. [Lumer]

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

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





L'Applicazione e il Protocollo Signal

SIGNAL

L'Applicazione e il Protocollo Signal Applicazione Signal

Applicazione Signal

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

Applicazione Signal

iniziarono a lavorare al Protocollo Signal

2 Applicazione

dell'Applicazione L'Applicazione e il Protocollo Signal

3 Crittografia Applicazioni

4 Signal Protocol

Attacchi possibili

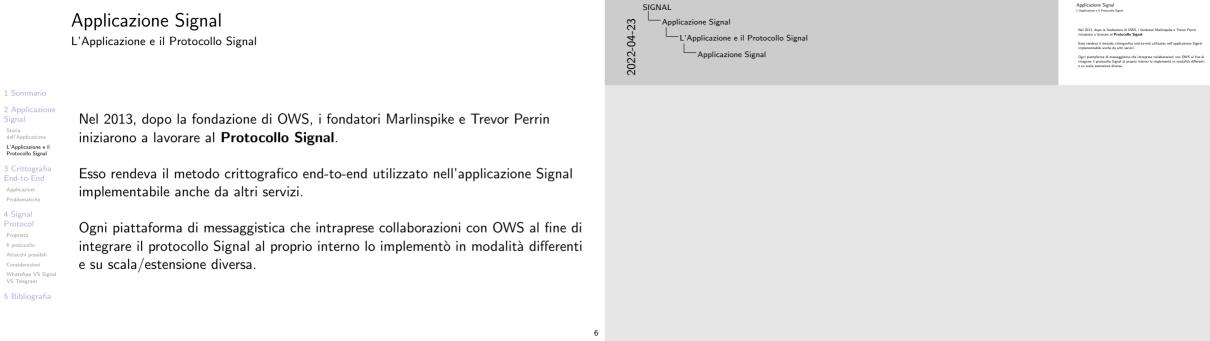
WhatsApp VS Signal VS Telegram

Esso rendeva il metodo crittografico end-to-end utilizzato nell'applicazione Signal implementabile anche da altri servizi.



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





L'Applicazione e il Protocollo Signal

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

- 4 Signal

- WhatsApp VS Signal

- Attacchi possibili

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

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

SIGNAL

Applicazione Signal

Applicazione Signal Facebook: usa Signal solo nelle Secret Conversations

Applicazione Signal

L'Applicazione e il Protocollo Signal

- 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
- L'Applicazione e

4 Signal

WhatsApp VS Signal

- dell'Applicazione Protocollo Signal
- ► Facebook: introdusse la feature Secret Conversations per gli utenti di

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

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

SIGNAL

Applicazione Signal

- 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
  - 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

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

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

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

4 Signal

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 L'Applicazione e il Protocollo Signal - Applicazione 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

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

- in modalità incognito
- 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
  - **Duo**: protezione delle videochat

  - **Skype**: conversazioni private dal 2018
  - ▶ WhatsApp: tra le maggiori applicazioni che implementano Signal è l'unica

Facebook Messenger nel luglio 2016 L'Applicazione e il Protocollo Signal ► Allo: rilasciata nel settembre 2016. sfruttava il Protocollo Signal se utilizzata ► Dup: protezione delle videochat Applicazione Signal Facebook: usa Signal solo nelle Secret Conversations

Applicazione Signal

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

Applicazione Signal

SIGNAL

- 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



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 aprile 2016)

[Gre29], [Lumer]

SIGNAL

Applicazione Signal

L'Applicazione e il Protocollo Signal

Facebook: usa Signal solo nelle Secret Conversations

Duo: applicazione per videochiamate e chat mobile di Google

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

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

Applicazione Signal

[Gre29], [Lumer]

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

WhatsApp VS Signal

4 Signal

2 Applicazione

dell'Applicazione

L'Applicazione e

Protocollo Signal

L'Applicazione e il Protocollo Signal

2 Applicazione

dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia

Applicazioni

4 Signal

II protocollo

VS Telegram

WhatsApp VS Signal

Attacchi possibili

contenuto che viene scambiato

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

Ciascuna di queste features richiede che le conversazioni intraprese siano dichiarate

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

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.

SIGNAL

L'Applicazione e il Protocollo Signal

2 Applicazione

dell'Applicazione L'Applicazione e

Protocollo Signal 3 Crittografia

Applicazioni

4 Signal Protocol

Il protocollo Attacchi possibili

WhatsApp VS Signal

[Mar16]

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

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

contenuto che viene scambiato

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

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.

Applicazione Signal

SIGNAL

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

SIGNAL

Applicazione Signal

L'Applicazione e il Protocollo Signal Applicazione Signal

Applicazione Signal

L'Applicazione e il Protocollo Signal

- 2 Applicazione

dell'Applicazione

4 Signal

II protocollo

VS Telegram

WhatsApp VS Signal

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

Attacchi possibili



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



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

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

► Salvano solo le informazioni strettamente necessarie

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

L'Applicazione e il Protocollo Signal

[Lumer]

2 Applicazione

L'Applicazione e i

3 Crittografia

4 Signal

Attacchi possibili

WhatsApp VS Signal

VS Telegram













II protocollo

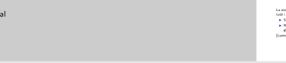






SIGNAL









Applicazione 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

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

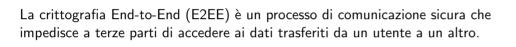
2 Applicazione

dell'Applicazione

### 3 Crittografia

End-to-End

4 Signal



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]

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 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

Crittografia End-to-End

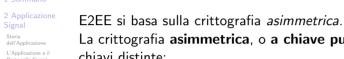
### 3 Crittografia

End-to-End

4 Signal

WhatsApp VS Signa





- 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
- 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

End-to-End Encryption

Crittografia End-to-End

dunque conservabili solo in ciphertext.

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

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

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

Storia dell'Applicazione

End-to-End

3 Crittografia

4 Signal



# 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

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

SIGNAL

Crittografia End-to-End

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 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.

End-to-End Encryption

# 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

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 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.

End-to-End Encryption

SIGNAL

Crittografia End-to-End

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

2 Applicazione Signal

dell'Applicazione

Protocollo Signal

3 Crittografia End-to-End

4 Signal

VS Telegram

WhatsApp VS Sign





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 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.

End-to-End Encryption

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

SIGNAL

Crittografia End-to-End

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

2 Applicazione

dell'Applicazione

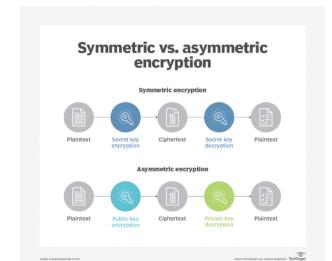
Protocollo Signal

3 Crittografia
End-to-End

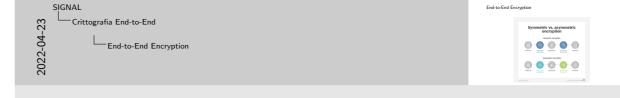
Applicazioni

4 Signal

Attacchi possibili Considerazioni WhatsApp VS Signal VS Telegram







Applicazioni

### 1 Commo

# 2 Applicazione

Storia dell'Applicazione L'Applicazione e

# Protocollo Signal 3 Crittografi

### 3 Crittogra End-to-En

Applicazioni

### Problema

### 4 Signal Protoco

Proprietà Il protocollo

Attacchi possibili

Considerazioni WhatsApp VS Signal VS Telegram

V J Telegranii

- ► 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:

[IDI



dai propri utenti. [Pou16]. [GM13]

 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 e in transit, proteggendo i dati degli utenti anche dall'acces

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]

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:

End-to-End Encryption 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

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

### 1 Sommari

### 2 Applicazion Signal

Storia dell'Applicazione L'Applicazione e

### 3 Crittogra

End-to-En

### Applicazioni

### 4 Signal

Protocol Proprietà

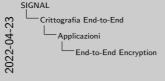
Il protocollo Attacchi possibili

Considerazioni 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:
- ▶ **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]



➤ Comunicazioni sicure: applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli trenti;

➤ Gestione passeword: in questo caso a entrambi gli endpoint della comunicazione si trova lo stesso utente, che il runica persona munita di chiave;

Data stronere, mi securi di strona in chul ondi noche ssorre aziantiti. ETEE

comminicazione si trova lo tesso utente, che à l'unica persona munita di c Data storage: nei servizi di storage in cloud può anche essere garantita in trannit, protroggendo i dati degli utenti anche dall'accesso da parte dei formitori del servizio in cloud;

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]

governo rederate in plaintext. [Sin 1]

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]

La E2EE non garantisce di per sé né la sicurezza né la privacy, in quanto i dati

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

SIGNAL

Crittografia End-to-End

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

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

che utenti non autorizzati e/o malintenzionati aventi accesso allo storage dei messaggi possano fare un uso improprio dei contenuti.

— Problematiche

sullo stesso database

14

Problematiche

2 Applicazione Signal

Storia dell'Applicazione

II protocollo

3 Crittografia

Attacchi possibil

WhatsApp VS Signal





### 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".











Problematiche

2 Applicazione Signal

dell'Applicazione

4 Signal

Il protocollo Attacchi possibil

VS Telegram

WhatsApp VS Sign







# Applicazioni Problematiche

provider di servizi.





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".

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

[int20], [IBM]

SIGNAL

 Problematiche End-to-End Encryption

Crittografia End-to-End

sullo stesso database

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

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] che utenti non autorizzati e/o malintenzionati aventi accesso allo storage dei messaggi possano fare un uso improprio dei contenuti.

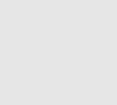
End-to-End Encryption

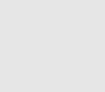
dati misliore della sola crittografia "in transit"

La EZEE non garantisco di ner sé né la sicurazza né la nrivary in quanto i dat trasmessi potrebbero essere protetti in modo poco sicuro sui dispositivi endpoint

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

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







14

Problematiche

### 2 Applicazione Signal

Storia dell'Applicazione

### Protocollo Signal

3 Crittogra

### End-to-En

Applicazioni

# Problematiche 4 Signal

Protocol Proprietà

Il protocollo Attacchi possi

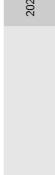
Attacchi possibili Considerazioni WhatsApp VS Signal

V J Telegram

### 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 crittografica di un dispositivo. Se non volute, possono essere introdotte tramite attacchi cyber e poi sfruttate per violare la sicurezza del sistema

[Gro15] [IR



SIGNAL

Crittografia End-to-End

Problematiche

End-to-End Encryption

End-to-

- 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. fingerorint numeriche o come QR code)

End-to-End Encryption

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

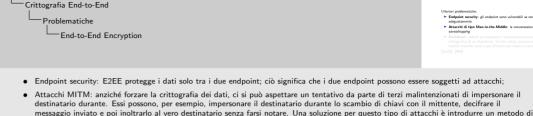
3 Crittografia

### 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
- 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 possibil WhatsApp VS Signa

Ulteriori problematiche:

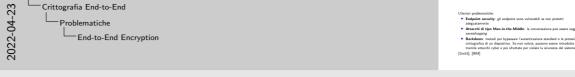
- ▶ Endpoint security: gli endpoint sono vulnerabili se non protetti adeguatamente
- ▶ Attacchi di tipo Man-in-the-Middle: la conversazione può essere soggetta a eavesdropping
- ▶ Backdoors: metodi per bypassare l'autenticazione standard o la protezione crittografica di un dispositivo. Se non volute,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

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

[Gre15], [IBM]



SIGNAL



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

Problematiche

4 Signal

II protocollo

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

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

SIGNAL

definire accuratamente eli estremi della trasmissione

End-to-End Encryption





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







Problematiche

- dell'Applicazione
- Protocollo Signal

Problematiche

Attacchi possibili

4 Signal

misure adeguate in caso di illeciti

Metadati visibili

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

Privacy "eccessiva": enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere

definire accuratamente gli estremi della trasmissione

Non vi è certezza che E2EE possa funzionare altrettanto bene con l'eventuale

WhatsApp VS Signal



SIGNAL

— Problematiche

Crittografia End-to-End

End-to-End Encryption

End-to-End Encryption

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

► Privacy "eccessiva": enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere

definire accuratamente eli estremi della trasmissione

Problematiche

- dell'Applicazione
- Protocollo Signal

Problematiche

4 Signal

Attacchi possibili WhatsApp VS Signal

misure adeguate in caso di illeciti

Metadati visibili

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

Privacy "eccessiva": enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere

Non vi è certezza che E2EE possa funzionare altrettanto bene con l'eventuale

definire accuratamente gli estremi della trasmissione

SIGNAL

Crittografia End-to-End — Problematiche End-to-End Encryption 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 misure adequate in caso di illeciti

Metadati visibili

► Complessità nel definire «li endonint: alcune implementazioni consentone

Problematiche

- dell'Applicazione
- Protocollo Signal

### Problematiche

4 Signal

II protocollo

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]

SIGNAL



► 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

Non vi è certezza che E2EE possa funzionare altrettanto bene con l'eventuale introduzione di quantum computer che rendano la crittografia obsoleta

End-to-End Encryption

Proprietà

### 2 Applicazione

dell'Applicazione

L'Applicazione e il Protocollo Signal

### 3 Crittografia

### 4 Signal

### Proprietà

II protocollo

Attacchi possibili

WhatsApp VS Signal VS Telegram

Protocol

- ambito crittografico:
- Integrità

Autenticità

Confidenzialità

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in

- Integrità: dati trasmessi non danneggiati e/o dispersi • Autenticità: possesso di una chiave da parte di due persone al fine di riconoscere e verificare l'identità dell'altro

SIGNAL

Signal Protocol

digitali

Confidenzialità: dati trasmessi non vengono diffusi a terzi non coinvolti nella conversazione

Signal Protocol

► Autenticità

Signal Protocol

ambito crittografico: Confidenzialiti ► Integrità

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in

- Non ripudiabilità: non deve essere possibile negare per es. la propria firma a un documento, per questo spesso è implementata tramite firme

# Proprietà

- 2 Applicazione

dell'Applicazione

Protocollo Signal

### Proprietà

II protocollo

4 Signal

3 Crittografia

Protocol

Attacchi possibili

WhatsApp VS Signal VS Telegram

ambito crittografico:

Confidenzialità

Integrità

Autenticità

Le proprietà CIA spesso vengono accompagnate dalla non ripudiabilità

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in

SIGNAL

Confidenzialità: dati trasmessi non vengono diffusi a terzi non coinvolti nella conversazione

• Integrità: dati trasmessi non danneggiati e/o dispersi

Signal Protocol

Signal Protocol

• Autenticità: possesso di una chiave da parte di due persone al fine di riconoscere e verificare l'identità dell'altro

• Non ripudiabilità: non deve essere possibile negare per es. la propria firma a un documento, per questo spesso è implementata tramite firme digitali

Signal Protocol

ambito crittografico: Confidenzialiti ► Integrità

► Autenticità





Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in

Le proprietà CIA spesso vengono accompagnate dalla non ripudiabilità

Proprietà

# 2 Applicazione

dell'Applicazione

### 3 Crittografia

### 4 Signal

### Proprietà

Attacchi possibili

WhatsApp VS Signal VS Telegram

Ulteriori proprietà spesso richieste sono:

- ▶ Forward Secrecy: se una chiave è compromessa solo un messaggio è compromesso e non lo sono i precedenti
- ► Future Secrecy: se una chiave è compromessa solo un messaggio è
- Cryptographic Deniability: l'esistenza di un file cifrato o di un messaggio è

SIGNAL

Signal Protocol

— Proprietà Signal Protocol

Forward Secrecy: se una chiave è compromessa solo un messaggio compromesso e non lo sono i precedenti

Signal Protocol

Cryptographic deniability in genere è più richiesta nelle applicazioni di messaggistica

Proprietà

# 2 Applicazione

dell'Applicazione

### 3 Crittografia

### 4 Signal

### Proprietà

Attacchi possibili

WhatsApp VS Signal VS Telegram

Ulteriori proprietà spesso richieste sono:

- ▶ Forward Secrecy: se una chiave è compromessa solo un messaggio è compromesso e non lo sono i precedenti
- ▶ Future Secrecy: se una chiave è compromessa solo un messaggio è compromesso e non lo sono i successivi
- Cryptographic Deniability: l'esistenza di un file cifrato o di un messaggio è

Signal Protocol — Proprietà Signal Protocol Cryptographic deniability in genere è più richiesta nelle applicazioni di messaggistica Signal Protocol

Forward Secrecy: se una chiave è compromessa solo un messaggio compromesso e non lo sono i precedenti

▶ Future Secrecy: se una chiave è compromessa solo un messaggio è commenmesso e non lo sono i successivi

SIGNAL

vero o meno.

Proprietà

dell'Applicazione

### Protocollo Signal 3 Crittografia

### 4 Signal

### Proprietà

Attacchi possibili WhatsApp VS Signal

VS Telegram

Ulteriori proprietà spesso richieste sono:

- ▶ Forward Secrecy: se una chiave è compromessa solo un messaggio è compromesso e non lo sono i precedenti
- ▶ Future Secrecy: se una chiave è compromessa solo un messaggio è compromesso e non lo sono i successivi
- ► 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

SIGNAL

Signal Protocol

—Propriet? ► Future Secrecy: se una chiave è compromessa solo un messaggio Signal Protocol

Signal Protocol

Forward Secrecy: se una chiave è compromessa solo un messaggio è compromesso e non lo sono i precedent

commenmesso e non lo sono i successivi ► Cryptographic Deniability: l'esistenza di un file cifrato o di un messaggio /

rinnerabile, nel senso che un altro utente non nuò dimostrare che i dati in plaintext esistono. Gli utenti possono negare che dei dati siano cifrati o anch negare di essere in grado di decifrarli, indipendentemente dal fatto che ciò si

Cryptographic deniability in genere è più richiesta nelle applicazioni di messaggistica

Il protocollo

2 Applicazione

dell'Applicazione

3 Crittografia

End-to-End

WhatsApp VS Signal VS Telegram

Attacchi possibili

II protocollo

4 Signal

Applicazioni

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).

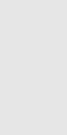
SIGNAL

Signal Protocol

Il protocollo 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) Signal Protocol

Signal Protocol

Il protocollo



19

II protocollo

### 1 Somma

### 2 Applicazione Signal

dell'Applicazione L'Applicazione e Protocollo Signal

### 3 Crittogra

End-to-En

Applicazioni

### 4 Signal

Protoc

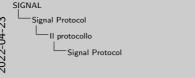
### II protocollo

Attacchi possibili Considerazioni WhatsApp VS Signal VS Telegram

5 Ribliografi

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.



II protocolio

Signal Protocol

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 funcioni X25519 e X448 di Diffici Aelibra su curv ellittiche. L'algoritmo VXEdDSA estende XEdDSA rendendolo verificabile.

basato e una chiave segreta condivisa.

➤ X3DH: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hello

- 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 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 ciò sia vero o meno.

Il protocollo

### 2 Applicazione

dell'Applicazione Protocollo Signal

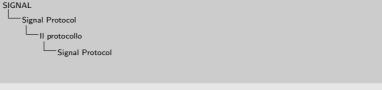
### 4 Signal

### II protocollo Attacchi possibili

WhatsApp VS Signal VS Telegram

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.



► XF4DSA e VXEdDSA: algoritmi per la creazione e verifica di signature: 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

Signal Protocol II austrontia

- 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 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 ciò sia vero o meno

Il protocollo

### 2 Applicazione

dell'Applicazione

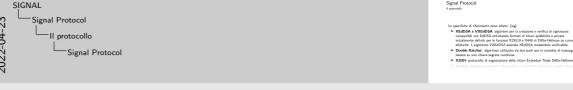
### 4 Signal

### II protocollo Attacchi possibili

WhatsApp VS Signal VS Telegram

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.



- 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

Signal Protocol

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 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 ciò sia vero o meno

Il protocollo

### 2 Applicazione

dell'Applicazione Protocollo Signal

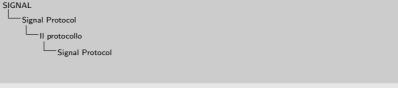
### 4 Signal

### 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.



- 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

Signal Protocol II austrontia

> ► XF4DSA e VXEdDSA: algoritmi per la creazione e verifica di signature: compatibili con EdDSA utilizzando formati di chiavi pubbliche e private

hasato su una chiave segreta condivisa ➤ X3DH: protocollo di neroziazione delle chiavi Extended Triple Diffie-Hellma ► Sesame: escripre le sessioni crittografate in ambiente acinconn e multi-devir

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

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 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 ciò sia vero o meno

Il protocollo: fasi di funzionamento [VD19]

- 2 Applicazione Signal
- dell'Applicazione

### 4 Signal

II protocollo

Attacchi possibili

WhatsApp VS Signal







- ► KEY REGISTRATION: invio di numerose chiavi pubbliche al server per consentire di iniziare una conversazione mentre l'altro utente non è online
- KEY AGREEMENT: Alice riceve le chiavi pubbliche di Bob dal server e le usa,
- ► CONVERSATION: Alice e Bob possiedono la chiave segreta condivisa e

  - Symmetric ratchet phase
  - ► DH ratchet phase

Signal Protocol • KEY REGISTRATION: se Alice vuole iniziare una conversazione con Bob può chiedere al server le sue chiavi pubbliche

Signal Protocol

► KEY RECISTRATION: invio di numerose chiavi pubbliche al server per consentire di iniziare una conversazione mentre l'altro utente non è online

SIGNAL

Signal Protocol

II protocollo

KEY AGREEMENT

CONVERSATION

Il protocollo: fasi di funzionamento [VD19]

- 2 Applicazione Signal
- dell'Applicazione

4 Signal

II protocollo

Attacchi possibili

WhatsApp VS Signal VS Telegram

► KEY REGISTRATION: invio di numerose chiavi pubbliche al server per consentire di iniziare una conversazione mentre l'altro utente non è online

- ▶ KEY AGREEMENT: Alice riceve le chiavi pubbliche di Bob dal server e le usa, insieme alle proprie chiavi private, per generare una chiave segreta condivisa. Invia a Bob un messaggio criptato con questa chiave. Bob. ricevutolo. recupera le chiavi pubbliche di Alice dal server e calcola la stessa chiave segreta condivisa. La negoziazione delle chiavi avviene tramite X3DH
- - ► DH ratchet phase



Signal Protocol

- KEY REGISTRATION: se Alice vuole iniziare una conversazione con Bob può chiedere al server le sue chiavi pubbliche
- KEY AGREEMENT
- CONVERSATION

SIGNAL

Il protocollo: fasi di funzionamento [VD19]

- 2 Applicazione
- dell'Applicazione
- Protocollo Signal

4 Signal

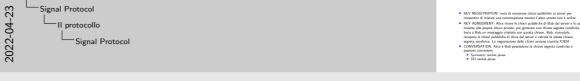
II protocollo

Attacchi possibili WhatsApp VS Signal

VS Telegram

► KEY REGISTRATION: invio di numerose chiavi pubbliche al server per consentire di iniziare una conversazione mentre l'altro utente non è online

- ▶ KEY AGREEMENT: Alice riceve le chiavi pubbliche di Bob dal server e le usa, insieme alle proprie chiavi private, per generare una chiave segreta condivisa. Invia a Bob un messaggio criptato con questa chiave. Bob. ricevutolo. recupera le chiavi pubbliche di Alice dal server e calcola la stessa chiave segreta condivisa. La negoziazione delle chiavi avviene tramite X3DH
- ► CONVERSATION: Alice e Bob possiedono la chiave segreta condivisa e possono conversare.
  - Symmetric ratchet phase
  - ► DH ratchet phase



• KEY REGISTRATION: se Alice vuole iniziare una conversazione con Bob può chiedere al server le sue chiavi pubbliche

Signal Protocol

- KEY AGREEMENT
- CONVERSATION

SIGNAL

Symmetric ratchet phase

Derivazione di una nuova chiave dalla chiave segreta condivisa.

Signal Protocol

Symmetric ratchet phase

Derivazione di una nuova chiave dalla chiave segreta condivisa

SIGNAL

Signal Protocol

Il protocollo

Signal Protocol

Il protocollo: fasi di funzionamento

### 2 Applicazione

Storia dell'Applicazione

4 Signal Protocol

VS Telegram





Signal Protocol

Symmetric ratchet phase

Derivazione di una nuova chiave dalla chiave segreta condivisa Se Aline invia nii) messaggi a Roh senza ringuere risnosta ngni messaggin sarb criptato con una nuova chiave calcolata in funzione della precedente.

SIGNAL

Signal Protocol

II protocollo

Signal Protocol

Il protocollo: fasi di funzionamento

Symmetric ratchet phase

Derivazione di una nuova chiave dalla chiave segreta condivisa.

criptato con una nuova chiave calcolata in funzione della precedente.

Se Alice invia più messaggi a Bob senza ricevere risposta ogni messaggio sarà

2 Applicazione

dell'Applicazione

Protocollo Signal

Applicazioni

II protocollo

VS Telegram

WhatsApp VS Signal









4 Signal

### Attacchi possibili

### 3 Crittografia

Il protocollo: fasi di funzionamento

2 Applicazione

dell'Applicazione Protocollo Signal

3 Crittografia

Applicazioni

Protocol

VS Telegram

WhatsApp VS Signal

II protocollo Attacchi possibili

4 Signal

Symmetric ratchet phase

Derivazione di una nuova chiave dalla chiave segreta condivisa. Se Alice invia più messaggi a Bob senza ricevere risposta ogni messaggio sarà criptato con una nuova chiave calcolata in funzione della precedente. In questo modo solo Alice e Bob possono calcolarla (escludendo casi in cui la chiave sia stata diffusa)

SIGNAL

Signal Protocol II protocollo Signal Protocol

Symmetric ratchet phase

Signal Protocol

Il protocollo: fasi di funzionament

Derivazione di una nuova chiave dalla chiave segreta condivisa

Se Aline invia niù messaggi a Roh senza ringuese risnosta ngni messaggin sari criptato con una nuova chiave calcolata in funzione della precedente. In questo modo solo Alice e Rob possono calcolada (escludendo casi in cui la









Il protocollo: fasi di funzionamento

2 Applicazione

dell'Applicazione

3 Crittografia

Applicazioni

Protocol Proprietà

II protocollo

Attacchi possibili

WhatsApp VS Signal

4 Signal

VS Telegram







Diffie-Hellman ratchet phase

Generazione di una nuova chiave segreta condivisa.

# Signal Protocol

SIGNAL

### II protocollo Signal Protocol

Signal Protocol

Generazione di una nunva chiave segreta condivisa

Il protocollo: fasi di funzionamento

2 Applicazione

dell'Applicazione

End-to-End

Applicazioni

4 Signal

Protocol

II protocollo Attacchi possibili

WhatsApp VS Signal VS Telegram

3 Crittografia

Diffie-Hellman ratchet phase

Generazione di una nuova chiave segreta condivisa. Se Bob invia un nuovo messaggio ad Alice genera una nuova coppia di chiavi effimere. Bob usa questa chiave per calcolarne una nuova condivisa, inviando poi la

propria chiave effimera ad Alice per farle calcolare la chiave condivisa.

SIGNAL

Signal Protocol II protocollo Signal Protocol

Signal Protocol

Se Bob invia un nuovo messaggio ad Alice genera una nuova coppia di chiavi effimere. Boh usa muesta chiave ner calcolame una nuova condicisa, inviando noi l propria chiave effimera ad Alice per farle calcolare la chiave condivisa.

generare nuove chiavi per i messaggi.

Il protocollo: fasi di funzionamento

2 Applicazione

dell'Applicazione

3 Crittografia

Applicazioni

4 Signal

Protocol

II protocollo

Attacchi possibili

WhatsApp VS Signal

VS Telegram

Diffie-Hellman ratchet phase

Generazione di una nuova chiave segreta condivisa.

Se Bob invia un nuovo messaggio ad Alice genera una nuova coppia di chiavi effimere. Bob usa questa chiave per calcolarne una nuova condivisa, inviando poi la propria chiave effimera ad Alice per farle calcolare la chiave condivisa. La chiave così calcolata verrà usata in una nuova symmetric ratchet phase per

Signal Protocol II protocollo Signal Protocol

SIGNAL

Signal Protocol

Se Bob invia un nuovo messaggio ad Alice genera una nuova coppia di chiavi

II protocollo: X3DH

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi.

2 Applicazione Signal [MP16]

3 Crittografia

4 Signal

II protocollo Attacchi possibili WhatsApp VS Signal VS Telegram

dell'Applicazione

► Identity key: chiave pubblica

▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo ▶ One-time pre-keys: insiemi di pre-keys condivisi col server prima

► Signed pre-key: pre-key firmata con l'esponente dell'Identity key

► Ephemereal key: chiave utilizzabile una sola volta

SIGNAL

Signal Protocol

II protocollo Signal Protocol

STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi private (secret keys) sk. Dopodiché scambiano le chiavi pubbliche attraverso un canale (potenzialmente non sicuro) e da esse possono derivare una chiave segreta condivisa ssk. [DH76], [JD16]

Signal Protocol

II sestember Valle

X3DH è stato svilunnato da OWS per supportare lo scambio asincrono delle chia







II protocollo: X3DH

2 Applicazione Signal

Storia dell'Applicazione

4 Signal

VS Signal



Protoco
Proprietà
II protocol
Attacchi p
Considera:
WhatsApp VS Telegr
5 Biblio

# 3 Crittografia



[MP16]

- ► Identity key: chiave pubblica

  - ► Ephemereal key: chiave utilizzabile una sola volta
  - ▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo
  - ▶ One-time pre-keys: insiemi di pre-keys condivisi col server prima

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi.

- - ► Signed pre-key: pre-key firmata con l'esponente dell'Identity key

SIGNAL

private (secret keys) sk.

Signal Protocol

II protocollo

ssk. [DH76], [JD16]

Signal Protocol

Dopodiché scambiano le chiavi pubbliche attraverso un canale (potenzialmente non sicuro) e da esse possono derivare una chiave segreta condivisa

STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi

Signal Protocol

Identity key: chiave pubblica

II sestember Valle

X3DH è stato svilunnato da OWS per supportare lo scambio asincrono delle chia

II protocollo: X3DH

2 Applicazione Signal

Storia dell'Applicazione

3 Crittografia

4 Signal

II protocollo Attacchi possibili WhatsApp VS Signal

[MP16]

Definizioni:

► Identity key: chiave pubblica

► Ephemereal key: chiave utilizzabile una sola volta

▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo ▶ One-time pre-keys: insiemi di pre-keys condivisi col server prima

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi.

► Signed pre-key: pre-key firmata con l'esponente dell'Identity key

ssk. [DH76], [JD16]

SIGNAL

private (secret keys) sk.

Signal Protocol

II protocollo

Signal Protocol

STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi

Dopodiché scambiano le chiavi pubbliche attraverso un canale (potenzialmente non sicuro) e da esse possono derivare una chiave segreta condivisa

Signal Protocol

Identity key: chiave pubblica

II sestember Valle

X3DH è stato svilunnato da OWS per supportare lo scambio asincrono delle chia

II protocollo: X3DH

dell'Applicazione

Protocollo Signal

3 Crittografia

4 Signal

II protocollo

WhatsApp VS Signal

Attacchi possibili



### X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi. 2 Applicazione [MP16] Definizioni:

- ► Identity key: chiave pubblica
- ► Ephemereal key: chiave utilizzabile una sola volta
- ▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo ▶ One-time pre-keys: insiemi di pre-keys condivisi col server prima
- ► Signed pre-key: pre-key firmata con l'esponente dell'Identity key

SIGNAL

Signal Protocol

private (secret keys) sk.

—II protocollo

Signal Protocol

ssk. [DH76], [JD16]

Dopodiché scambiano le chiavi pubbliche attraverso un canale (potenzialmente non sicuro) e da esse possono derivare una chiave segreta condivisa

STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi

Identity key: chiave pubblica Ephemereal key: chiave utilizzabile una sola volta Pre-keys: chiavi condivise col server prima dell'attivazione del protocoli

Signal Protocol

II sestember Valle

X3DH è stato quilunnato da OWS per curportare lo crambio acincrono delle chiau



► Identity key: chiave pubblica

Il protocollo: X3DH

[MP16]

Definizioni:

2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

4 Signal

II protocollo

Attacchi possibili

WhatsApp VS Signal



▶ One-time pre-keys: insiemi di pre-keys condivisi col server prima

▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo

dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un

utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando

► Ephemereal key: chiave utilizzabile una sola volta

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi.



SIGNAL

Identity key: chiave pubblica Ephemereal key: chiave utilizzabile una sola volta Signal Protocol STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi

 Pre-keys: chiavi condivise col server prima dell'attivazione del protocoli ► One-time pre-keys: insigmi di pre-keys condivisi col sepuer prima dell'attivazione del protocollo. Il server condivide una chiave geni volta che u

X3DH è stato quilunnato da OWS per curportare lo crambio acincrono delle chiau

Signal Protocol

II sestember Valle

Dopodiché scambiano le chiavi pubbliche attraverso un canale (potenzialmente non sicuro) e da esse possono derivare una chiave segreta condivisa

Il protocollo: X3DH

- 2 Applicazione

dell'Applicazione

Protocollo Signal

II protocollo

Attacchi possibili WhatsApp VS Signal

dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un

4 Signal

3 Crittografia



X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi. [MP16] Definizioni:

- ► Identity key: chiave pubblica
- ► Ephemereal key: chiave utilizzabile una sola volta
- ▶ Pre-keys: chiavi condivise col server prima dell'attivazione del protocollo ▶ One-time pre-keys: insiemi di pre-keys condivisi col server prima
- utente vuole iniziare una conversazione e ne richiede un nuovo insieme quando stanno per finire
- ► Signed pre-key: pre-key firmata con l'esponente dell'Identity key

ssk. [DH76], [JD16]

private (secret keys) sk.

SIGNAL

II protocollo Signal Protocol

Signal Protoco

STANDARD DIFFIE-HELLMAN: Alice e Bob generano ognuno una chiave pubblica pk basata su un generatore comune g modulo m e le proprie chiavi

 Pre-keys: chiavi condivise col server prima dell'attivazione del protocoli ► One-time pre-keys: insigmi di pre-keys condivisi col sepuer prima dell'attivazione del protocollo. Il server condivide una chiave geni volta che u Signed pre-key pre-key firmata con l'esponente dell'Identity key

Signal Protocol

Identity key: chiave pubblica

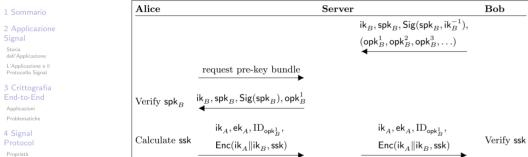
II sestember Valle

X3DH à state quillenate da OWS per connectare le crambio aciermen delle chiau

Dopodiché scambiano le chiavi pubbliche attraverso un canale (potenzialmente non sicuro) e da esse possono derivare una chiave segreta condivisa

24

Il protocollo: X3DH



Verify ssk

Figure: Funzionamento di X3DH semplificato

SIGNAL

Signal Protocol Il protocollo report proky hradie Yorky age or the safe, Signal or only Signal Protocol

h , sph., Sig(sph., h., l). (985.985.985....) Figure: Funzionamento di X3DH semplificato

Signal Protocol

Il protocollo: X3DH

[VD19]

II protocollo Attacchi possibili

25

Signal Protocol
Il protocollo: Double Ratchet

2 Applicazione Signal

dell'Applicazione

Protocollo Signal 3 Crittografia End-to-End

Applicazioni

4 Signal Protocol Proprietà

II protocollo Attacchi possibili

WhatsApp VS Signal VS Telegram

SIGNAL

2022-04-23

Signal Protocol

☐ II protocollo

Signal Protocol

26

Signal Protocol

Signal Protocol
Il protocollo: Double Ratchet

2 Applicazione Signal

dell'Applicazione

Protocollo Signal 3 Crittografia End-to-End

Applicazioni

4 Signal Protocol Proprietà

II protocollo Attacchi possibili

WhatsApp VS Signal VS Telegram

SIGNAL

2022-04-23

Signal Protocol

☐ II protocollo

Signal Protocol

Signal Protocol

# 27

Signal Protocol
Il protocollo: Sesame

2 Applicazione Signal

dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni

4 Signal Protocol Proprietà

II protocollo

VS Telegram

Attacchi possibili WhatsApp VS Signal

28

SIGNAL

2022-04-23

Signal Protocol

☐ II protocollo

Signal Protocol

Signal Protocol

Signal Protocol II protocollo: XEdDSA e VXEdDSA

2 Applicazione

dell'Applicazione

L'Applicazione e il Protocollo Signal 3 Crittografia

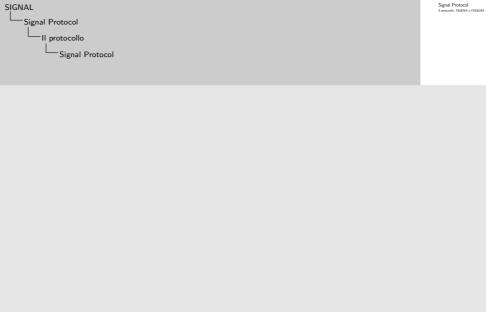
End-to-End Applicazioni

4 Signal

Protocol Proprietà

II protocollo Attacchi possibili

WhatsApp VS Signal VS Telegram



### Considerazioni

2022-04-23

dell'Applicazione L'Applicazione e il Protocollo Signal

2 Applicazione Signal

3 Crittografia

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

30

Considerazioni

SIGNAL

Signal Protocol

— Considerazioni Considerazioni

# Bibliografia I

W Diffie and M Hellman.

- 2 Applicazione
- dell'Applicazione
- 3 Crittografia

- 4 Signal
- Protocol II protocollo
- Attacchi possibili WhatsApp VS Signal VS Telegram
- 5 Bibliografia
- Edward snowden says motive behind leaks was to expose 'surveillance state'.
- - - Barton Gellman and Jerry Markon.

The Washington Post. June 10, 2013.

- protect journalists. 2016. May 1.
- New directions in cryptography.
- In IEEE Transactions on Information Theory, pages 644–654, 1976.
- CPJ Middle East, North Africa Program, and CPJ Technology Program.

  - Why telegram's security flaws may put iran's journalists at risk committee to

31

- Bibliografia

SIGNAL

Bibliografia

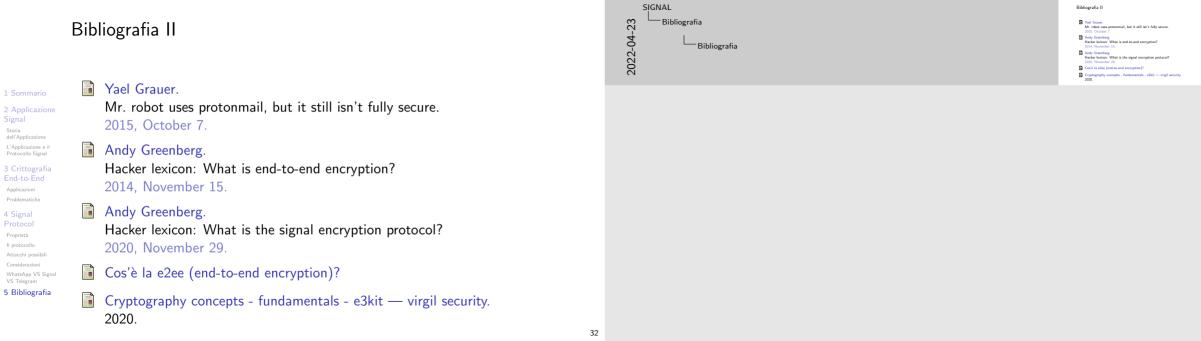
- Rarton Gellman and Jerry Markon Edward snowden says motive behind leaks was to expose 'surveillance state'

New directions in cryptography.

Bibliografia I

CP | Middle Fast North Africa Program and CP | Technology Program

Why telegram's security flaws may put iran's journalists at risk - committee



# Bibliografia III

2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

4 Signal Protocol

II protocollo

VS Telegram

Attacchi possibili WhatsApp VS Signal 5 Bibliografia

David J Lumb. The story of signal.

Computer security: Public key crypto.

2016.

B Jacobs and J Daemen.

Ben Lutkevich and Madelyn Bacon.

end-to-end encryption (e2ee). June 2021.

Increment, (7), 2018, October.

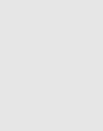
Moxie Marlinspike. Whatsapp's signal protocol integration is now complete. Apr. 5, 2016.

end-to-end encryption (e2ee). David J Lumb. The story of signal. Moxie Marlinspike. Whatsapp's signal protocol integration is now complete.

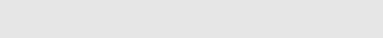
Bibliografia III

B R Jambs and J Daemen Computer security: Public key crusto

Ben Lutkevich and Madelyn Bacon







33

SIGNAL

2022-04-

- Bibliografia

Bibliografia

## Bibliografia IV

- Moxie Marlinspike and Trevor Perrin.

The x3dh key agreement protocol.

Technical report, Open Whisper Systems, 2016.

Snowden's email provider loses appeal over encryption keys.

- 2 Applicazione
- dell'Applicazione
- 3 Crittografia
- 4 Signal
- Protocol
- II protocollo Attacchi possibili
- WhatsApp VS Signal

5 Bibliografia

- Signal documentation.

K Poulsen.

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

2014, April 16.

2007. November 7.

34

- Bibliografia

SIGNAL

- -Bibliografia

Bibliografia IV

Moxie Marlinspike and Trevor Perrin. The v3dh key agreement rentoral K Poulsen

Signal documentation Ryan Singel.

Snowden's email provider loses appeal over encryption keys

Encrypted e-mail company hushmail spills to feds. 2007, November 7.

# Bibliografia V

Dion Van Dam.

Master's thesis, Radboud University, 2019.

protocol.

Analysing the signal protocol - a manual and automated analysis of the signal

### 2 Applicazione dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

# Protocol

Attacchi possibili WhatsApp VS Signal

VS Telegram

II protocollo

5 Bibliografia

4 Signal

SIGNAL

-Bibliografia

Bibliografia

Ribliografia V

Dion Van Dam.

Master's thesis Radboud University 2019

Analysing the signal protocol - a manual and automated analysis of the signal

