



2 Applicazione

Storia dell'Applicazione

Applicazioni

4 Signal

Difetti di progettazione WhatsApp VS Signal

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

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

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



Difetti di

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.

Nel 2013 Marlinspike fonda il progetto open-source Open Whisper Systems, Applicazioni grazie a cui rilascia la prima versione di Signal nel 2015 (anche per PC come 4 Signal applicazione Chrome), per poi rilasciarlo anche per Windows, Mac e Linux nel 2017.

SIGNAL

Applicazione Signal

—Storia dell'Applicazione

Applicazione Signal

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.

Nel 2011 Twitter acquista Whisper Systems e Marlinspike diventa capo della cybersecurity del social media.

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



fondarono la Signal Foundation. il cui obiettivo è il supporto e l'accelerazione Applicazione Signal

Nel febbrain 2018 Marlinsnike e il co-fondatore di WhatsAnn Brian Acton

Applicazione Signal Storia dell'Apolicazione

dell'Applicazione L'Applicazione e il Protocollo Signal 3 Crittografia Applicazioni 4 Signal Difetti di

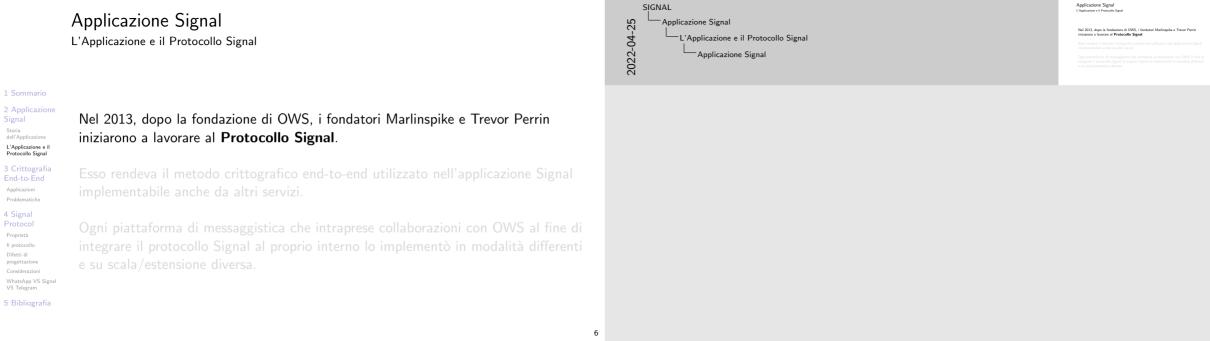
2 Applicazione

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 della diffusione della comunicazione privata e sicura. [Lumer] WhatsApp VS Signal

SIGNAL

Applicazione Signal

Storia dell'Applicazione





dell'Applicazione L'Applicazione e il Protocollo Signal

Applicazioni 4 Signal Protocol

Difetti di

WhatsApp VS Signal

Nel 2013, dopo la fondazione di OWS, i fondatori Marlinspike e Trevor Perrin iniziarono a lavorare al Protocollo Signal.

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

implementabile anche da altri servizi.

SIGNAL

Applicazione Signal

L'Applicazione e il Protocollo Signal

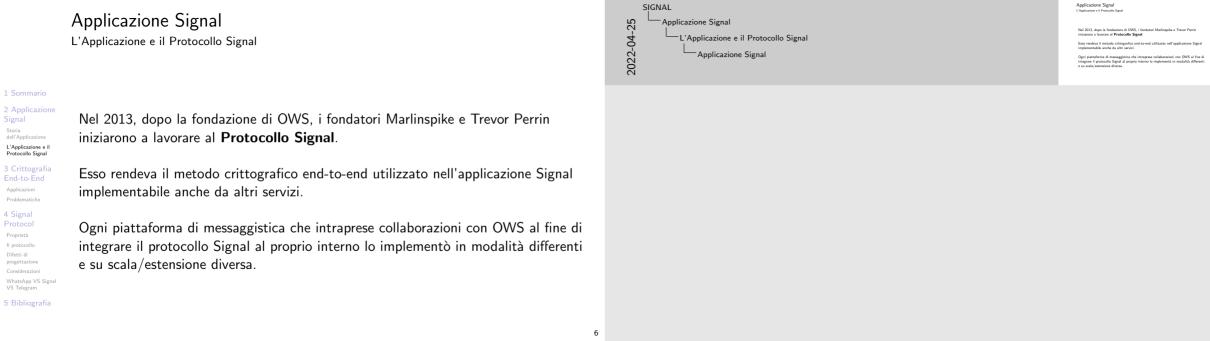
Applicazione Signal

Nel 2013 donn la fondazione di CWS i fondatori Marlinsnike e Travor Perrin

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

Applicazione Signal

iniziarono a lavorare al Protocollo Signal



L'Applicazione e il Protocollo Signal

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

- 4 Signal
- Difetti di

- WhatsApp VS Signal

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

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

Applicazione Signal L'Applicazione e il Protocollo Signal

SIGNAL

Applicazione 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

L'Applicazione e il Protocollo Signal

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

- 4 Signal
- Difetti di

- 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

Applicazione Signal

SIGNAL

- L'Applicazione e il Protocollo Signal Applicazione 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

Applicazione Signal

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

L'Applicazione e il Protocollo Signal

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

4 Signal

Difetti di

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

SIGNAL

Applicazione Signal 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 L'Applicazione e il Protocollo Signal ► Allo: rilasciata nel settembre 2016. sfruttava il Protocollo Signal se utilizzata Applicazione 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

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

- 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

L'Applicazione e il Protocollo Signal

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

4 Signal

Difetti di

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

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 3 Crittografia

4 Signal

Difetti di

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
- ▶ WhatsApp: tra le maggiori applicazioni che implementano Signal è l'unica

Applicazione Signal L'Applicazione e il Protocollo Signal Applicazione Signal Facebook: usa Signal solo nelle Secret Conversations

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

► Dup: protezione delle videochat

• 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

Difetti di progettazione 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
- ▶ 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

Facebook Messenger nel luglio 2016 L'Applicazione e il Protocollo Signal ► Allo: rilasciata nel settembre 2016. sfruttava il Protocollo Signal se utilizzata Applicazione Signal ► Skyne: conversazioni private dal 2018 ► WhatsApp: tra le mazziori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da [Gre29], [Lumer]

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

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

- 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 il Protocollo Signal

Applicazioni

4 Signal

WhatsApp VS Signal

3 Crittografia

"private" affinché sia possibile applicare la crittografia end-to-end su tutto il contenuto che viene scambiato

Ciascuna di queste features richiede che le conversazioni intraprese siano dichiarate

SIGNAL

Applicazione Signal L'Applicazione e il Protocollo Signal Applicazione Signal

i numeri a 60 cifre presentati.

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

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

Applicazione Signal

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

L'Applicazione e il Protocollo Signal

2 Applicazione

dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia

Applicazioni

Difetti di

WhatsApp VS Signal

4 Signal

"private" affinché sia possibile applicare la crittografia end-to-end su tutto il contenuto che viene scambiato

Inoltre, conversazioni già avvenute non possono essere protette applicando il protocollo ex post. [Mar16]

Ciascuna di queste features richiede che le conversazioni intraprese siano dichiarate

SIGNAL

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

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.

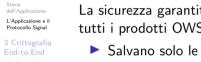
L'Applicazione e il Protocollo Signal

- 2 Applicazione

4 Signal

Difetti di

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

SIGNAL

Applicazione Signal

L'Applicazione e il Protocollo Signal Applicazione Signal

Applicazione Signal

L'Applicazione e il Protocollo Signal

- 2 Applicazione

3 Crittografia

4 Signal

Difetti di

WhatsApp VS Signal

La sicurezza garantita dall'implementazione del protocollo è relativa al fatto che dell'Applicazione L'Applicazione e Protocollo Signal

- 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]

SIGNAL

Applicazione Signal

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

2 Applicazione

dell'Applicazione

3 Crittografia

End-to-End Applicazioni

4 Signal

Difetti di progettazione

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.

SIGNAL Crittografia End-to-End 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.

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.

2 Applicazione

dell'Applicazione

Applicazioni

Difetti di progettazione

WhatsApp VS Signal

4 Signal

3 Crittografia End-to-End

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.

Grazie alla E2EE è possibile proteggere i dati trasmessi da terze parti malintenzionate che possono includere i provider dei servizi di telecomunicazione

SIGNAL Crittografia End-to-End

--- End-to-End Encryption

Solamente eli utenti che sono in possesso della chiave segreta possono decifrare il

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

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

4 Signal Protocol

Difetti di progettazione

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]

SIGNAL

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] si tratta di dati presentati in un formato non leggibile

Dati protetti da crittografia sono tali per cui solamente le persone autorizzate possono leggerne il contenuto in chiaro, mentre per tutti gli altri utenti

Grazie alla E2EE è possibile proteggere i dati trasmessi da terze parti malintenzionate che possono includere i provider dei servizi di telecomunicazione

End-to-End Encryption

gli Internet provider e utenti malevoli

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

- 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

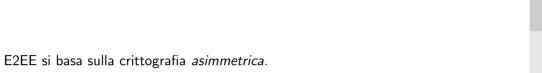
progettazione

WhatsApp VS Signal

VS Telegram



3 Crittografia End-to-End 4 Signal





SIGNAL

Crittografia End-to-End

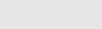
End-to-End Encryption I messaggi vengono crittografati dal mittente, pertanto, anche se intercettati da una terza persona, essi non le saranno visibili in plaintext e saranno

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

End-to-End Encryption







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

2 Applicazione Signal

Storia dell'Applicazione

- Difetti di

chiavi distinte:

- 2 Applicazione Signal

Storia dell'Applicazione

4 Signal

Difetti di progettazione

VS Telegram

3 Crittografia End-to-End

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

della chiave pubblica

E2EE si basa sulla crittografia asimmetrica.

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

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

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

End-to-End Encryption

SIGNAL

Crittografia End-to-End

End-to-End Encryption

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

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.

2 Applicazione Signal

dell'Applicazione

3 Crittografia

End-to-End

4 Signal

Difetti di progettazione

VS Telegram

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.

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

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.

E2EE si basa sulla crittografia asimmetrica.

- 2 Applicazione Signal
- dell'Applicazione

3 Crittografia End-to-End

4 Signal

Difetti di progettazione

VS Telegram

chiavi distinte: Protocollo Signal

- 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
- 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.

SIGNAL

Crittografia End-to-End

dunque conservabili solo in 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

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 du

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

2 Applicazione

dell'Applicazione

Protocollo Signal

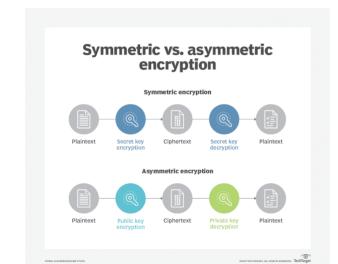
3 Crittografia
End-to-End

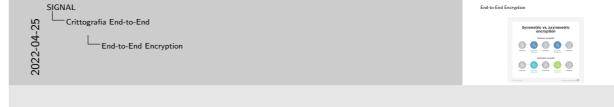
Applicazioni

4 Signal

Difetti di progettazione Considerazioni WhatsApp VS Signal

VS Telegram





Applicazioni

2 Applicazione

dell'Applicazione

Protocollo Signal

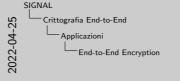
4 Signal

Difetti di

progettazione WhatsApp VS Signal



- ► 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



► Comunicazioni sicure: anniirazioni di messaggistica e nosta elettronica ne mantanam mirata la conversazioni deali utenti

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

1.0.....

2 Applicazio

dell'Applicazione L'Applicazione e Protocollo Signal

3 Crittogra

End-to-En

Applicazioni Problematici

4 Signal

Protoco

Il protocollo Difetti di progettazione

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:

ſΙΡ

SIGNAL

Crittografia End-to-End

Crittografia End-to-End

Applicazioni

End-to-End Encryption

End-to-End Encryption

Crittografia End-to-End Encryption

Applicazioni

End-to-End Encryption

Crittografia End-to-End Encryption

Applicazioni

End-to-End Encryption

(Applicazioni (Touris Sealing of the Applicazioni dala commissione (Touris Sealing of the Applicazioni (Touris Sealing of the

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]

13

dai propri utenti. [Pou16]. [GM13]

Applicazioni

dell'Applicazione

Applicazioni

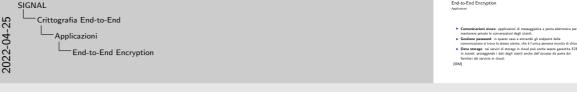
4 Signal

Difetti di

WhatsApp VS Signal

- ► 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]



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]

13

Problematiche

2 Applicazione Signal

Storia dell'Applicazione

Applicazioni

Problematiche

4 Signal

Difetti di

WhatsApp VS Signal

Tuttavia, l'implementazione della E2EE consente di applicare una protezione dei dati migliore della sola crittografia "in transit". 3 Crittografia

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.



SIGNAL

Crittografia End-to-End

— Problematiche 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 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

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

Storia dell'Applicazione

Applicazioni

Problematiche

4 Signal

Il protocollo Difetti di

WhatsApp VS Signa

[int20], [IBM]

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".

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

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.

SIGNAL

Crittografia End-to-End

 Problematiche Tuttavia l'implementazione della EZEE consente di applicare una protezione dei dati misliore della sola crittografia "in transit" End-to-End Encryption Per molti sistemi di messaggistica i messaggi passano attraverso un intermediario [int20], [IBM] 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.

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.

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

End-to-End Encryption

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

progettazione 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

Crittografia End-to-End ► Endonint security: eli endonint cono vulnerabili se non protetti — Problematiche End-to-End Encryption

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

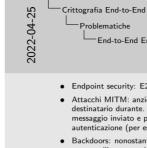
Problematiche

4 Signal

progettazione 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



SIGNAL

End-to-End Encryption

► Endonint security: eli endonint sono 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

1 C

2 Applicazione

Storia dell'Applicazione

Protocollo Signal

3 Crittografia End-to-End

Applicazioni

Problematiche

4 Signal

Proprietà
Il protocollo
Difetti di

Difetti di progettazione Considerazioni WhatsApp VS Signa VS Telegram

vs relegram

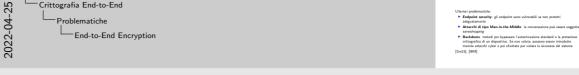
Ulteriori problematiche:

- ► 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. fingerorint 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

Difetti di progettazione

WhatsApp VS Signal



Metadati visibili

► Complessità nel definire gli endpoint: alcune implementazioni consentono

Privacy "eccessiva": enti governativi non hanno modo di verificare la natura

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

definire accuratamente gli estremi della trasmissione

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

SIGNAL

-- Problematiche End-to-End Encryption

Crittografia End-to-End

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

4 Signal

Difetti di





- ► 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 misure adeguate in caso di illeciti
- Metadati visibili
- 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

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

End-to-End Encryption













► Complessità nel definire «li endonint: alcune implementazioni consentone





Problematiche

- dell'Applicazione
- Protocollo Signal

Problematiche

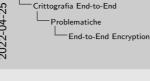
4 Signal

Difetti di

► 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

WhatsApp VS Signal



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 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

Difetti di

[LB21]

- ► 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

Crittografia End-to-End

End-to-End Encryption

— Problematiche

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 dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adequate in caso di illeciti

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

2 Applicazione Storia dell'Applicazione Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in

4 Signal

L'Applicazione e il Protocollo Signal

3 Crittografia

WhatsApp VS Signal

Proprietà

Protocol Proprietà

Autenticità

Integrità

ambito crittografico: Confidenzialità

SIGNAL

Signal Protocol

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

► Autenticità

Signal Protocol

ambito crittografico: Confidenzialiti ► Integrità

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in

2 Applicazione

4 Signal

Proprietà

WhatsApp VS Signal

Storia dell'Applicazione Protocollo Signal 3 Crittografia Autenticità Protocol

Proprietà

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in

Integrità

Le proprietà CIA spesso vengono accompagnate dalla non ripudiabilità

Confidenzialità

ambito crittografico:

SIGNAL

Signal Protocol

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

Le proprietà CIA spesso vengono accompagnate dalla non ripudiabilità

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in

Signal Protocol

ambito crittografico: Confidenzialiti ► Integrità

► Autenticità

• 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

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

Proprietà

2 Applicazione

4 Signal

WhatsApp VS Signal

Proprietà



















Ulteriori proprietà spesso richieste sono:

compromesso e non lo sono i precedenti

► Future Secrecy: se una chiave è compromessa solo un messaggio è

▶ Forward 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

Signal Protocol

compromesso e non lo sono i precedenti



Forward Secrecy: se una chiave è compromessa solo un messaggio



Ulteriori proprietà spesso richieste sono:

Proprietà

2 Applicazione

dell'Applicazione

Proprietà

Difetti di progettazione

3 Crittografia

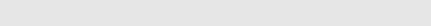
4 Signal

WhatsApp VS Signal

▶ 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





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

Signal Protocol

SIGNAL

Signal Protocol

vero o meno.

Proprietà

dell'Applicazione

Protocollo Signal 3 Crittografia

4 Signal

Proprietà Difetti di

WhatsApp VS Signal

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

► 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

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

Signal Protocol

compromesso e non lo sono i precedent

Cryptographic deniability in genere è più richiesta nelle applicazioni di messaggistica

SIGNAL

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 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)

Il protocollo

SIGNAL

19

Signal Protocol

Il protocollo

Signal Protocol

Il protocollo

2 Applicazione

dell'Applicazione

3 Crittografia

End-to-End

Applicazioni

WhatsApp VS Signal

II protocollo Difetti di





Il protocollo

dell'Applicazione

Protocollo Signal

4 Signal

II protocollo

Difetti di progettazione

WhatsApp VS Signal

Le specifiche di riferimento sono infatti: [sig]

- **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
- ▶ Double Ratchet: algoritmo utilizzato da due parti per lo scambio di messaggi
- Sesame: gestisce le sessioni crittografate in ambiente asincrono e multi-device.

Signal Protocol II protocollo Signal Protocol

SIGNAL

➤ X3DH: nestocollo di negoziazione delle chiavi Evtended Trinle Diffie Hellman 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 (grazie alla non invertibilità della funzione ratchet)

Signal Protocol

II austrontia

• 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

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

dell'Applicazione

Protocollo Signal

3 Crittografia

4 Signal

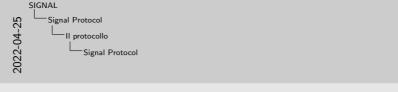
Difetti di

II protocollo

WhatsApp VS Signal



- **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman.
- ▶ Double Ratchet: algoritmo utilizzato da due parti per lo scambio di messaggi basato su una chiave segreta condivisa.



Le specifiche di riferimento sono infatti: [sig]

> X3DH: protocollo di negoziazione delle chiavi Extended Triple Diffie Hellman ► Double Ratchet: alsoritmo utilizzato da due parti per lo scambio di messassi

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 (grazie alla non invertibilità della funzione ratchet)
- 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

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

dell'Applicazione

Protocollo Signal

3 Crittografia

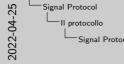
4 Signal

II protocollo Difetti di

WhatsApp VS Signal



- **X3DH**: protocollo di negoziazione delle chiavi Extended Triple Diffie-Hellman. ▶ Double Ratchet: algoritmo utilizzato da due parti per lo scambio di messaggi
- basato su una chiave segreta condivisa. **Sesame**: gestisce le sessioni crittografate in ambiente asincrono e multi-device.



SIGNAL

Le specifiche di riferimento sono infatti: [sig] ➤ X3DH: nentocollo di negoziazione delle chiavi Evtended Trinle Diffie.Hellman ► Double Ratchet: algoritmo utilizzato da due parti per lo scambio di message Signal Protocol ► Sesame: eestisce le sessioni crittografate in ambiente asincrono e multi-device

Signal Protocol II mentionelle

- 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 (grazie alla non invertibilità della funzione ratchet) • 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

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

Difetti di

4 Signal

progettazione



consentire di iniziare una conversazione mentre l'altro utente non è online

► KEY REGISTRATION: invio di numerose chiavi pubbliche al server per

CONVERSATION: Alice e Bob possiedono la chiave segreta condivisa e

- KEY AGREEMENT: Alice riceve le chiavi pubbliche di Bob dal server e le usa,

 - ► DH ratchet phase
 - Symmetric ratchet phase

- Il protocollo

SIGNAL

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

Signal Protocol

CONVERSATION

N.B. Symmetric ratchet phase e DH ratchet phase verranno meglio analizzati più avanti nel parlare dell'algoritmo Double Ratchet. Ad ogni modo, a livello generale, la loro combinazione permette di generare una nuova chiave.

Signal Protocol

Il protocollo: fasi di funzionamento [VD19]

- 2 Applicazione Signal
- dell'Applicazione Protocollo Signal

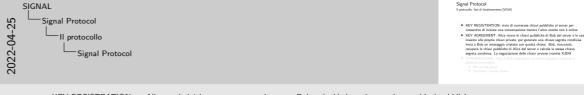
4 Signal

II protocollo

Difetti di

- ► 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

 - ► DH ratchet phase Symmetric ratchet phase



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

N.B. Symmetric ratchet phase e DH ratchet phase verranno meglio analizzati più avanti nel parlare dell'algoritmo Double Ratchet. Ad ogni modo, a livello generale, la loro combinazione permette di generare una nuova chiave.

Il protocollo: fasi di funzionamento [VD19]

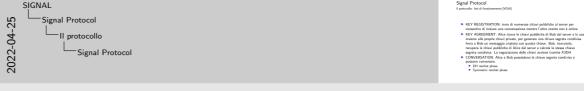
- 2 Applicazione Signal
- dell'Applicazione Protocollo Signal

4 Signal

II protocollo

Difetti di

- ► 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.
 - DH ratchet phase
 - Symmetric 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

N.B. Symmetric ratchet phase e DH ratchet phase verranno meglio analizzati più avanti nel parlare dell'algoritmo Double Ratchet. Ad ogni modo, a livello generale, la loro combinazione permette di generare una nuova chiave.

Il protocollo: fasi di funzionamento

Signal Protocol

Derivazione di una nuova chiave dalla chiave serreta condivisa.

2 Applicazione

Storia dell'Applicazione

Applicazioni

Protocol

Difetti di

progettazione WhatsApp VS Signal

II protocollo

4 Signal

3 Crittografia











Derivazione di una nuova chiave dalla chiave segreta condivisa.



Signal Protocol

Il protocollo

Signal Protocol

SIGNAL

Signal Protocol

Symmetric ratchet phase





Il protocollo: fasi di funzionamento

2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

Applicazioni

Difetti di

WhatsApp VS Signal

II protocollo

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.

Signal Protocol II protocollo Signal Protocol

SIGNAL

Symmetric ratchet phase

Signal Protocol

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 Protocol

Il protocollo: fasi di funzionament

Symmetric ratchet phase

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

SIGNAL

Signal Protocol

II protocollo

Signal Protocol

Il protocollo: fasi di funzionamento

Symmetric ratchet phase

chiave sia stata diffusa)

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

In questo modo solo Alice e Bob possono calcolarla (escludendo casi in cui la

2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

Applicazioni

Protocol

Difetti di

WhatsApp VS Signal

4 Signal

II protocollo















Il protocollo: fasi di funzionamento

Signal Protocol

Generazione di una nunva chiave segreta condivisa

Signal Protocol

2 Applicazione

dell'Applicazione

3 Crittografia

Applicazioni

Proprietà II protocollo

Difetti di

WhatsApp VS Signal

Diffie-Hellman ratchet phase

Generazione di una nuova chiave segreta condivisa.





SIGNAL

Signal Protocol

II protocollo

Signal Protocol

Il protocollo: fasi di funzionamento

2 Applicazione

dell'Applicazione

3 Crittografia

End-to-End

Applicazioni

4 Signal

Protocol II protocollo

Difetti di progettazione WhatsApp VS Signal

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

Generazione di una nunva chiave segreta condivisa 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.

Signal Protocol

Il protocollo: fasi di funzionamento

2 Applicazione

3 Crittografia

Applicazioni

4 Signal Protocol

II protocollo Difetti di

WhatsApp VS Signal

dell'Applicazione

Diffie-Hellman ratchet phase

generare nuove chiavi per i messaggi.

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 [MP16b]

3 Crittografia

4 Signal

II protocollo progettazione WhatsApp VS Signal

dell'Applicazione

- - ► 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

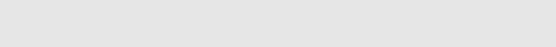
Signal Protocol

private (secret keys) sk.

ssk. [DH76], [JD16]

II protocollo Signal Protocol





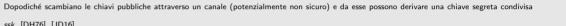


X3DH è stato quilunnato da OWS per connectare lo crambio acincrono delle chiau

Signal Protocol

II sestember Valle





► Identity key: chiave pubblica

► Ephemereal key: chiave utilizzabile una sola volta

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

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

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

[MP16b]

Definizioni:

II protocollo: X3DH

2 Applicazione Signal

Storia dell'Applicazione

3 Crittografia

4 Signal

II protocollo progettazione

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

WhatsApp VS Signal

SIGNAL

Signal Protocol

private (secret keys) sk.

ssk. [DH76], [JD16]

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

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

II sestember Valle

II protocollo: X3DH

- 2 Applicazione Signal

3 Crittografia

4 Signal

II protocollo progettazione

WhatsApp VS Signal

Definizioni: Storia dell'Applicazione

[MP16b]

► 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

private (secret keys) sk.

SIGNAL

Signal Protocol

ssk. [DH76], [JD16]

Il 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

Identity key: chiave pubblica

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





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







II protocollo: X3DH

- 2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

4 Signal

II protocollo Difetti di

WhatsApp VS Signal

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi. [MP16b] 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

—II protocollo Signal Protocol

Signal Protocol

SIGNAL

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

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

II sestember Valle

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]

Il protocollo: X3DH

2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

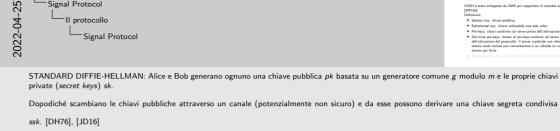
4 Signal

II protocollo

Difetti di progettazione WhatsApp VS Signal

X3DH è stato sviluppato da OWS per supportare lo scambio asincrono delle chiavi. [MP16b] 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 dell'attivazione del protocollo. Il server condivide una chiave ogni volta che un utente vuole iniziare una conversazione e ne richiede un nuovo insieme guando
- stanno per finire ► Signed pre-key: pre-key firmata con l'esponente dell'Identity key



dell'attivazione del protocollo. Il server condivide una chiave geni volta che u

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

► One-time pre-keys: insigmi di pre-keys condivisi col sepuer prima

Signal Protocol

II sestember Valle

Definizioni

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

SIGNAL

► Identity key: chiave pubblica

► Ephemereal key: chiave utilizzabile una sola volta

▶ 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.

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

Signal Protocol

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

► 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

II sestember Valle

Definizioni

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

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

SIGNAL

Signal Protoco

private (secret keys) sk.

ssk. [DH76], [JD16]

24

II protocollo

Signal Protocol

Il protocollo: X3DH

2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

II protocollo Difetti di progettazione

utente vuole iniziare una conversazione e ne richiede un nuovo insieme guando stanno per finire WhatsApp VS Signal

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

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

[MP16b]

Definizioni:

4 Signal

















II protocollo: X3DH

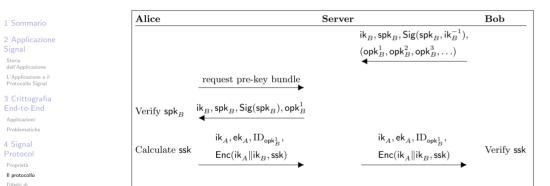


Figure: Funzionamento di X3DH semplificato

[VD19]

Signal Protocol SIGNAL I make and a Valley Signal Protocol (mk_mk_mk_....) $v_{(\alpha\beta)^{\prime},q_{\beta}k_{\beta}}=k_{\beta},q_{\beta}k_{\beta},S(g)(qk_{\beta}),c_{\beta}k_{\beta}$ Signal Protocol B_{ij} , B_{ij} , B_{ijkj} , B_{ijkj} Figure: Funzionamento di X3DH semplificato

Perché il protocollo possa funzionare offline ogni utente deve inviare le proprie chiavi pubbliche al server, inviando cioè ik, spk, Sig(spk, ik⁻¹ e $(opk^1, opk^2, opk^3, \ldots).$

La ik va inviata una sola volta, la spk va rinnovata periodicamente.

Se Alice vuole iniziare una conversazione richiede al server ik_B , spk_B , $Sig(spk_B, ik_B^{-1})$ e una delle one-time pre-keys opk_B^X di Bob. Il server poi elimina

 opk_{R}^{X} . Una volta finite le opk_{R} ad Alice verranno inviate solo le altre chiavi senza opk_{R} .

Ricevute le chiavi Alice verifica la firma di spko e se va a buon fine genera una coppia di chiavi effimere: poi calcola la ssk usando una Key Derivation

Function (KDF). Alla fine cancella ek_A^{-1} e tutti i valori k_i generati.

N.B. DH(x, y) è una funzione DH su curva ellittica che calcola una ssk basandosi su due chiavi, mentre KDF(x) è una funzione basata su RFC5869

[KE10].

Alice invia un messaggio iniziale a Bob contenente ik_A , ek_A , $ID_{opk_B^{\times}}$ (per fargli sapere quale opk_B^{\times} ha usato) e $Enc(ik_A||ik_B,ssk)$. Bob riceve il messaggio e calcola la ssk nello stesso modo di Alice. Bob decritta il messaggio inviato da Alice e controlla se il valore di ssk è corretto

e in questo caso cancella la opk utilizzata

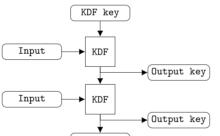
Alice e Bob possono ora riutilizzare la stessa ssk per messaggi futuri oppure usare chiavi da essa derivate. [VD19]

Il protocollo: Double Ratchet

Algoritmo utilizzato per il proseguimento della conversazione, dopo averla inizializzata tramite X3DH.

2 Applicazione

dell'Applicazione



4 Signal II protocollo Difetti di WhatsApp VS Signal KDF key

SIGNAL

Algoritmo utilizzato per il proseguimento della conversazione, dopo averla Signal Protocol Il protocollo Signal Protocol La catena KDF usa l'output di una KDF come input per un'altra applicazione della KDF.

Ogni output key può essere utilizzata per cifrare un messaggio. Tale catena garantisce: Resilienza: l'output appare randomico

- Forward secrecy: garantita dalla non-invertibilità della KDF
- Future secrecy: garantita se l'input della KDF i+1 non è il solo output della KDF i. Per garantire ciò è necessario usare un **DH** ratchet

Signal Protocol

Il protocollo: Double Ratchet

Signal Protocol Il protocollo: Double Ratchet

Algoritmo utilizzato per il proseguimento della conversazione, dopo averla inizializzata tramite X3DH.

2 Applicazione Signal [MP16a], [VD19]

dell'Applicazione

4 Signal

II protocollo

WhatsApp VS Signal

Difetti di

A differenza di X3DH usa una catena KDF, come mostrato in figura 2.

KDF key Input Output key Input ► Output key

KDF key

Figure: Catena KDF

La catena KDF usa l'output di una KDF come input per un'altra applicazione della KDF.

SIGNAL

Signal Protocol

Tale catena garantisce:

II protocollo

Signal Protocol

Ogni output key può essere utilizzata per cifrare un messaggio.

Forward secrecy: garantita dalla non-invertibilità della KDF

• Future secrecy: garantita se l'input della KDF i+1 non è il solo output della KDF i. Per garantire ciò è necessario usare un **DH** ratchet

Resilienza: l'output appare randomico

Signal Protocol

Il protocollo: Double Ratchet

inizializzata tramite X3DH

Algoritmo utilizzato per il proseguimento della conversazione, dopo averla

A differenza di X3DH usa una catena KDE come mostrato in figura 2

Isput - HEF

Figure: Cateria KDF

Il protocollo: Double Ratchet

Signal Protocol

Il protocollo Signal Protocol

Combinando una catena KDF con un DH ratchet otteniamo un algoritmo Double ratchet che garantisce sia forward servery che future servery

Signal Protocol

2 Applicazione

dell'Applicazione

L'Applicazione e i Protocollo Signal

Applicazioni

4 Signal

II protocollo Difetti di

WhatsApp VS Signal

Combinando una catena KDF con un DH ratchet otteniamo un algoritmo Double ratchet che garantisce sia forward secrecy che future secrecy. 3 Crittografia

SIGNAL

Signal Protocol

Il protocollo: Double Ratchet

2 Applicazione

dell'Applicazione

3 Crittografia

Difetti di



Combinando una catena KDF con un DH ratchet otteniamo un algoritmo Double

ratchet che garantisce sia forward secrecy che future secrecy.

DH ratchet infatti modifica gli input delle KDF in modo tale che, se anche una

chiave venisse recuperata da terzi, si sia in grado di ristabilire la segretezza

dall'applicazione successiva di una KDF.

Signal Protocol

Signal Protocol II protocollo

SIGNAL

Combinando una catena KDF con un DH ratchet otteniamo un algoritmo Double dall'applicazione successiva di una KDF

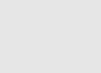
Signal Protocol

Il protocollo: Double Ratchet









Sia Alice che Bob hanno tre catene KDF da utilizzare:

Signal Protocol

► DH ratchet ► Sanding ratchet Receiving ratchet

Il protocollo: Double Ratchet

Sia Alice che Bob hanno tre catene KDF da utilizzare:

SIGNAL

Signal Protocol

II protocollo

Signal Protocol

Il protocollo: Double Ratchet

Signal Protocol

DH ratchet

Sending ratchet ► Receiving ratchet

2 Applicazione

dell'Applicazione

3 Crittografia

4 Signal Protocol

Proprietà

II protocollo Difetti di

WhatsApp VS Signal























Il protocollo: Double Ratchet

2 Applicazione

dell'Applicazione

3 Crittografia

4 Signal

II protocollo

Difetti di

WhatsApp VS Signal

Protocol

Sia Alice che Bob hanno tre catene KDF da utilizzare:

- DH ratchet
- Sending ratchet
- Receiving ratchet

Ogni volta che Alice vuole inviare un messaggio a Bob aggiornerà la catena sending ratchet producendo una nuova chiave di output e invierà a Bob il proprio messaggio cifrato con essa.

Signal Protocol Il protocollo Signal Protocol

SIGNAL

Il protocollo: Double Ratchet Sia Alice che Bob hanno tre catene KDF da utilizzare: ► DH ratchet

► Sanding ratchet Receiving ratchet Ogni volta che Alice vuole inviare un messaggio a Bob aggiornerà la catena sending

Signal Protocol

ratchet producendo una nuova chiave di output e invierà a Bob il proprio messaggio cifrato con essa

applicato prima del Double ratchet).

Il protocollo: Double Ratchet

2 Applicazione

dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia

Applicazioni

4 Signal

II protocollo

Difetti di

WhatsApp VS Signal



La catena di invio di Alice deve essere sincronizzata con quella di ricezione di Bob e viceversa e devono iniziare nella stessa posizione (caratteristica garantita da X3DH

SIGNAL

Signal Protocol

Il protocollo

Signal Protocol

Signal Protocol

Il protocollo: Double Ratchet

applicato prima del Double ratchet)

La catena di invin di Alice deve essere sincronizzata con muella di ricezione di Rob e viceversa e devono iniziare nella stessa posizione (caratteristica garantita da X3DF

Il protocollo: Double Ratchet

applicato prima del Double ratchet).

La catena di invio di Alice deve essere sincronizzata con quella di ricezione di Bob e

viceversa e devono iniziare nella stessa posizione (caratteristica garantita da X3DH

Signal Protocol

Il protocollo: Double Ratchet

applicate prima del Double ratchet)

La catena di invin di Alice deve essere sincronizzata con muella di ricezione di Rob e viceversa e devono iniziare nella stessa posizione (caratteristica garantita da X3DF

In queste condizioni tuttavia non è ancora garantita la future secrecy

SIGNAL

Signal Protocol

Il protocollo

Signal Protocol

2 Applicazione

dell'Applicazione

3 Crittografia

Applicazioni

WhatsApp VS Signal

Difetti di

II protocollo

In queste condizioni tuttavia non è ancora garantita la future secrecy

4 Signal

- Protocollo Signal

Il protocollo: Double Ratchet

dell'Applicazione L'Applicazione e il Protocollo Signal

Applicazioni

4 Signal

Protocol

II protocollo

Difetti di

WhatsApp VS Signal

Per garantire future secrecy Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.

SIGNAL Signal Protocol II protocollo Signal Protocol

Per garantire future secrecy Bob invierà come parte di uno dei suoi messaggi una

nuova chiave pubblica Diffie-Hellman.

Signal Protocol

Questo sistema di catene garantisce dunque:

- Forward security: grazie alle catene di invio e ricezione, caratterizzate da funzioni non invertibili, non è possibile retrocedere ai messaggi inviati in precedenza
- Future secrecy: grazie alla catena DH-ratchet se anche si riesce a intercettare un messaggio e decrittarlo si resettano le catene di invio e ricezione, rendendo impossibile generare in anticipo le chiavi che verranno utilizzate in futuro
- Funzionamento asincrono: se Alice invia dieci messaggi a Bob e lui non risponde man mano, egli comunque sarà in grado di ricostruire la seguenza di chiavi utilizzata da Alice e dunque leggere i messaggi
- In ogni messaggio viene indicato il numero di messaggi già inviati sulla stessa catena quindi se un messaggio va perso si può o aspettarne l'arrivo o far avanzare la catena di tante posizioni quanti messaggi sono andati persi,

Il protocollo: Double Ratchet

dell'Applicazione

Applicazioni

4 Signal

II protocollo

Difetti di

WhatsApp VS Signal

Per garantire future secrecy Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.

Alice userà questa chiave per far avanzare la catena DH-ratchet, imponendo così il reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata.

SIGNAL Signal Protocol II protocollo Signal Protocol

Per garantire future secrecy Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman Alice userà questa chiave ner far avanzare la catena DH-ratchet, imponendo così

reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di

Signal Protocol

Questo sistema di catene garantisce dunque:

- Forward security: grazie alle catene di invio e ricezione, caratterizzate da funzioni non invertibili, non è possibile retrocedere ai messaggi inviati in precedenza
- Future secrecy: grazie alla catena DH-ratchet se anche si riesce a intercettare un messaggio e decrittarlo si resettano le catene di invio e ricezione, rendendo impossibile generare in anticipo le chiavi che verranno utilizzate in futuro
- Funzionamento asincrono: se Alice invia dieci messaggi a Bob e lui non risponde man mano, egli comunque sarà in grado di ricostruire la seguenza di chiavi utilizzata da Alice e dunque leggere i messaggi
- In ogni messaggio viene indicato il numero di messaggi già inviati sulla stessa catena quindi se un messaggio va perso si può o aspettarne l'arrivo o far avanzare la catena di tante posizioni quanti messaggi sono andati persi,

Il protocollo: Double Ratchet

dell'Applicazione

Applicazioni

4 Signal

II protocollo

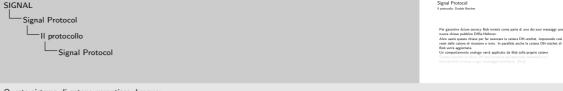
Difetti di

progettazione WhatsApp VS Signal

Per garantire future secrecy Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.

Alice userà questa chiave per far avanzare la catena DH-ratchet, imponendo così il reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata.

Un comportamento analogo verrà applicato da Bob sulle proprie catene.



Questo sistema di catene garantisce dunque:

• Forward security: grazie alle catene di invio e ricezione, caratterizzate da funzioni non invertibili, non è possibile retrocedere ai messaggi inviati in precedenza

Signal Protocol

- Future secrecy: grazie alla catena DH-ratchet se anche si riesce a intercettare un messaggio e decrittarlo si resettano le catene di invio e ricezione, rendendo impossibile generare in anticipo le chiavi che verranno utilizzate in futuro
- Funzionamento asincrono: se Alice invia dieci messaggi a Bob e lui non risponde man mano, egli comunque sarà in grado di ricostruire la seguenza di chiavi utilizzata da Alice e dunque leggere i messaggi
- In ogni messaggio viene indicato il numero di messaggi già inviati sulla stessa catena quindi se un messaggio va perso si può o aspettarne l'arrivo o far avanzare la catena di tante posizioni quanti messaggi sono andati persi,

Il protocollo: Double Ratchet

dell'Applicazione Protocollo Signal

4 Signal

II protocollo

Difetti di WhatsApp VS Signal

Per garantire future secrecy Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman.

Alice userà questa chiave per far avanzare la catena DH-ratchet, imponendo così il reset delle catene di ricezione e invio. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata.

Un comportamento analogo verrà applicato da Bob sulle proprie catene. Questo scambio di chiavi DH può avvenire ogniqualvolta necessario ma normalmente avviene a ogni messaggio scambiato. [Pou]



Per garantire future secrecy Bob invierà come parte di uno dei suoi messaggi una nuova chiave pubblica Diffie-Hellman Alice userà muesta chiave ner far avanzare la catena DH-ratchet, imponendo così

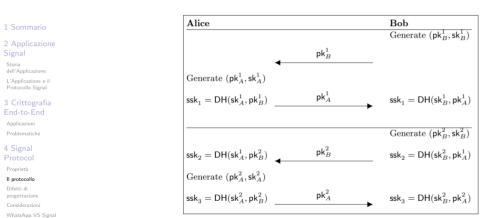
Un comportamento analogo verrà applicato da Bob sulle proprie catene. Questo scambio di chiavi DH può avvenire ornigualvolta necessario ma normalmente avviene a ogni messaggio scambiato. [Pou]

Signal Protocol

Questo sistema di catene garantisce dunque:

- Forward security: grazie alle catene di invio e ricezione, caratterizzate da funzioni non invertibili, non è possibile retrocedere ai messaggi inviati in precedenza
- Future secrecy: grazie alla catena DH-ratchet se anche si riesce a intercettare un messaggio e decrittarlo si resettano le catene di invio e ricezione, rendendo impossibile generare in anticipo le chiavi che verranno utilizzate in futuro
- Funzionamento asincrono: se Alice invia dieci messaggi a Bob e lui non risponde man mano, egli comunque sarà in grado di ricostruire la seguenza di chiavi utilizzata da Alice e dunque leggere i messaggi
- In ogni messaggio viene indicato il numero di messaggi già inviati sulla stessa catena quindi se un messaggio va perso si può o aspettarne l'arrivo o far avanzare la catena di tante posizioni quanti messaggi sono andati persi,

II protocollo: Double Ratchet



5 Bibliografia Figure: DH ratchet

Signal Protocol

II protocollo

Signal Protocol

Signal Protocol

Figure 10 to adde

Figure 10 to adde

Figure 10 to adde

Figure 10 to adde

Il protocollo: Sesame

2 Applicazione Signal

dell'Applicazione L'Applicazione e il Protocollo Signal

Applicazioni

4 Signal Protocol

II protocollo

Difetti di

WhatsApp VS Signal

L'algoritmo Sesame gestisce la creazione, eliminazione e utilizzo delle sessioni di comunicazione.

SIGNAL

Signal Protocol L'algoritmo Sesame gestisce la creazione, eliminazione e utilizzo delle sessioni d II protocollo Signal Protocol

Signal Protocol

Problemi che si possono generare:

- Alice e Bob possono avere ognuno più dispositivi quindi l'invio di un messaggio da parte di Alice richiede di inviarne una copia a tutti i dispositivi di Bob e a tutti i dispositivi di Alice per conoscenza.
- Alice e Bob possono aggiungere o rimuovere dispositivi, iniziando o terminando delle sessioni
- Alice e Bob possono iniziare una nuova sessione allo stesso tempo, così che si ottengano due sessioni. Per un funzionamento ottimale del Double Ratchet Alice e Bob devono usare la stessa sessione, quindi devono concordare su quella da utilizzare.
- Alice può resettare lo stato della sessione sul suo dispositivo o impostarla tramite backup, richiedendo a Bob di concordare nuovamente sulla sessione da utilizzare

32

Il protocollo: Sesame

dell'Applicazione Protocollo Signal

Applicazioni

4 Signal Protocol

II protocollo Difetti di

progettazione WhatsApp VS Signal

L'algoritmo Sesame gestisce la creazione, eliminazione e utilizzo delle sessioni di comunicazione.

Ogni dispositivo degli utenti deve tenere traccia di una sessione attiva per ogni altro dispositivo con cui sta comunicando e utilizzare quella sessione quando comunica con esso. Quando si riceve un messaggio su una sessione inattiva, essa

diventa attiva.

SIGNAL Signal Protocol II protocollo Signal Protocol

L'algoritmo Sesame gestisce la creazione, eliminazione e utilizzo delle sessioni d Ozni dispositivo deali utenti deve tenere traccia di una sessione attiva per peni altro dispositivo con cui sta comunicando e utilizzare quella sessione quando

Signal Protocol

Problemi che si possono generare:

- Alice e Bob possono avere ognuno più dispositivi quindi l'invio di un messaggio da parte di Alice richiede di inviarne una copia a tutti i dispositivi di Bob e a tutti i dispositivi di Alice per conoscenza.
- Alice e Bob possono aggiungere o rimuovere dispositivi, iniziando o terminando delle sessioni
- Alice e Bob possono iniziare una nuova sessione allo stesso tempo, così che si ottengano due sessioni. Per un funzionamento ottimale del Double Ratchet Alice e Bob devono usare la stessa sessione, quindi devono concordare su quella da utilizzare.
- Alice può resettare lo stato della sessione sul suo dispositivo o impostarla tramite backup, richiedendo a Bob di concordare nuovamente sulla sessione da utilizzare

Il protocollo: Sesame

dell'Applicazione Protocollo Signal

Applicazioni

4 Signal Protocol

II protocollo Difetti di

WhatsApp VS Signal

L'algoritmo Sesame gestisce la creazione, eliminazione e utilizzo delle sessioni di comunicazione.

Ogni dispositivo degli utenti deve tenere traccia di una sessione attiva per ogni altro dispositivo con cui sta comunicando e utilizzare quella sessione quando comunica con esso. Quando si riceve un messaggio su una sessione inattiva, essa

diventa *attiva*. In questo modo ogni dispositivo utilizza una sola sessione per ogni altro dispositivo remoto con cui comunica. [MP17]



Problemi che si possono generare:

• Alice e Bob possono avere ognuno più dispositivi quindi l'invio di un messaggio da parte di Alice richiede di inviarne una copia a tutti i dispositivi di Bob e a tutti i dispositivi di Alice per conoscenza.

Signal Protocol

L'algoritmo Sesame gestisce la creazione, eliminazione e utilizzo delle sessioni d

Ozni dispositivo deali utenti deve tenere traccia di una sessione attiva per peni altro dispositivo con cui sta comunicando e utilizzare quella sessione quando

- Alice e Bob possono aggiungere o rimuovere dispositivi, iniziando o terminando delle sessioni
- Alice e Bob possono iniziare una nuova sessione allo stesso tempo, così che si ottengano due sessioni. Per un funzionamento ottimale del Double Ratchet Alice e Bob devono usare la stessa sessione, quindi devono concordare su quella da utilizzare.
- Alice può resettare lo stato della sessione sul suo dispositivo o impostarla tramite backup, richiedendo a Bob di concordare nuovamente sulla sessione da utilizzare

2 Applicazione Signal

dell'Applicazione

3 Crittografia

4 Signal

II protocollo Difetti di

progettazione

WhatsApp VS Signal

Il protocollo: Sesame

Sesame è stato progettato per l'uso attraverso sessioni Double Ratchet create attraverso scambio di chiavi X3DH.

- ▶ I dispositivi comunicano al server le proprie one-time pre keys, signed pre keys
- e identity public key. ▶ Il dispositivo mittente recupera dal server la identity public key del dispositivo
- ► X3DH usa queste chiavi per creare sia una chiave segreta che apre una

SIGNAL Signal Protocol Il protocollo Signal Protocol

Signal Protocol Il protocollo: Sesame

Secame è stato renesttato ner l'uso attraverso secsioni Double Ratchet create attraverso scambio di chiavi X3DH. ► I dispositivi comunicano al server le proprie one-time pre kevs, signed pre ke e identity public key.

33

Il protocollo: Sesame

2 Applicazione Signal

dell'Applicazione

Protocollo Signal

4 Signal

II protocollo

Difetti di progettazione

WhatsApp VS Signal

Sesame è stato progettato per l'uso attraverso sessioni Double Ratchet create attraverso scambio di chiavi X3DH.

- ▶ I dispositivi comunicano al server le proprie one-time pre kevs. signed pre kevs e identity public key.
- ▶ Il dispositivo mittente recupera dal server la identity public key del dispositivo
- destinatario, signed pre keys e una one-time pre key se disponibile. ► X3DH usa queste chiavi per creare sia una chiave segreta che apre una

SIGNAL Signal Protocol Il protocollo Signal Protocol Signal Protocol Il protocollo: Sesame

Secame è stato renesttato ner l'uso attraverso sessioni Double Ratchet create attraverso scambio di chiavi X3DH. ► I dispositivi comunicano al server le proprie one-time pre kevs, signed pre ke

- e identity public key. ► Il dispositivo mittente recupera dal server la identity public key del dispositivo
- destinatario, signed ore keys e una one time ore key se disponibile

Il protocollo: Sesame

2 Applicazione Signal

dell'Applicazione

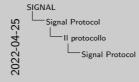
Protocollo Signal

Difetti di

WhatsApp VS Signal

Sesame è stato progettato per l'uso attraverso sessioni Double Ratchet create attraverso scambio di chiavi X3DH.

- ▶ I dispositivi comunicano al server le proprie one-time pre kevs. signed pre kevs
- e identity public key. ▶ Il dispositivo mittente recupera dal server la identity public key del dispositivo
- destinatario, signed pre keys e una one-time pre key se disponibile. ► X3DH usa queste chiavi per creare sia una chiave segreta che apre una sessione Double Ratchet sia un messaggio iniziale X3DH.



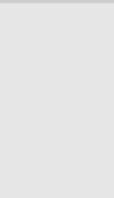
Signal Protocol Il protocollo: Sesame

Secame è stato renesttato ner l'uso attraverso secsioni Double Ratchet create attraverso scambio di chiavi X3DH. ► I dispositivi comunicano al server le proprie one-time pre keys, signed pre ker

- e identity public key.
 - ► Il dispositivo mittente recupera dal server la identity public key del dispositivo destinatario, signed ore keys e una one time ore key se disponibile
- X3DH usa queste chiavi per creare sia una chiave segreta che apre una sessione Double Ratchet sia un messaggio iniziale X3DH.

4 Signal

II protocollo



Il protocollo: Sesame

- 2 Applicazione

II protocollo Difetti di

progettazione



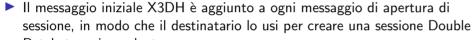




4 Signal

Protocol





SIGNAL

34

Signal Protocol

II protocollo

Signal Protocol

Signal Protocol

Il protocollo: Sesame

Il massaggio iniziale XRDH è aggiunto a neni messaggio di anertura di

sessione, in modo che il destinatario lo usi per creare una sessione Double

- Ratchet corrispondente.
- ▶ Ricevuto il messaggio di conferma di apertura della sessione il mittente smette

▶ I dispositivi comunicano solo con Double Ratchet.



- dell'Applicazione

Il protocollo: Sesame

- 2 Applicazione

dell'Applicazione

3 Crittografia

4 Signal Protocol

II protocollo Difetti di

WhatsApp VS Signal

- ► Il messaggio iniziale X3DH è aggiunto a ogni messaggio di apertura di sessione, in modo che il destinatario lo usi per creare una sessione Double Ratchet corrispondente.
- ▶ Ricevuto il messaggio di conferma di apertura della sessione il mittente smette
- di inviare il messaggio iniziale X3DH.
- ▶ I dispositivi comunicano solo con Double Ratchet.

SIGNAL

Signal Protocol Il protocollo Signal Protocol

Il massaggio iniziale XRDH è aggiunto a neni messaggio di anertura di sessione, in modo che il destinatario lo usi per creare una sessione Double ► Ricevuto il messaggio di conferma di apertura della sessione il mittente smette di inviare il messaggio iniziale X3DH.

Signal Protocol

Il protocollo: Sesame

Il protocollo: Sesame

[MP17], [VD19]

- 2 Applicazione

4 Signal

Protocol

II protocollo Difetti di

progettazione WhatsApp VS Signal

► Il messaggio iniziale X3DH è aggiunto a ogni messaggio di apertura di dell'Applicazione Protocollo Signal

sessione, in modo che il destinatario lo usi per creare una sessione Double Ratchet corrispondente.

▶ Ricevuto il messaggio di conferma di apertura della sessione il mittente smette

di inviare il messaggio iniziale X3DH.

▶ I dispositivi comunicano solo con Double Ratchet.

Il massaggio iniziale XRDH è aggiunto a neni messaggio di anertura di Il protocollo sessione, in modo che il destinatario lo usi per creare una sessione Double Signal Protocol [MP17], [VD19]

► Ricevuto il messaggio di conferma di apertura della sessione il mittente smette di inviare il messaggio iniziale X3DH. ► I dispositivi comunicano solo con Double Ratchet.

Signal Protocol

Il protocollo: Sesame

SIGNAL

Signal Protocol

Difetti di progettazione

Frosch analysis [FMB⁺16]

dell'Applicazione

Protocollo Signal

4 Signal

Difetti di

progettazione WhatsApp VS Signal

Export function [fixed]: la funzione esportava la password necessaria per inviare le *one-time pre-keys* al server in *plaintext* su dispositivi Android

► Vulnerabilità a UKS - Unknown kev-share attack

Signal Protocol Difetti di progettazione Difetti di progettazione

Export function [fixed]: la funzione esportava la password necessaria pe inviare le one-time pre-keys al server in plaintext su dispositivi Android ► Vulnerabilità a UKS - Unknown kev-share attack

Difetti di progettazione

Except explore (EME) 140

I difetti di implementazione individuati in questo paper sono stati ricavati da un'analisi di X3DH e di Double Ratchet separatamente, ma non da un'analisi dell'interazione dei due algoritmi come invece avviene nel protocollo Signal.

UKS Esempio

SIGNAL

Bob sa che Charlie lo inviterà a una festa. Per fare uno scherzo a Charlie. Bob sostituisce la propria chiave con quella di Dave.

Quando Charlie invita Bob alla festa. Bob inoltrerà il messaggio a Dave. Dal punto di vista di Dave, sembrerà che Charlie abbia inviato il messaggio.

Charlie penserà di aver invitato Bob, ma avrà in effetti invitato Dave.



4 Signal

progettazione WhatsApp VS Signal

2 Applicazione dell'Applicazione L'analisi effettuata è valida presupponendo che tutte le KDF si comportino come

oracoli che restituiscono un output simile a un output casuale. 3 Crittografia

Applicazioni

SIGNAL

Signal Protocol

Difetti di progettazione

Difetti di progettazione Il paper [CGCD+17] è il primo studio scientifico a riportare un'analisi formale dell'interazione tra X3DH e Double Ratchet.

L'analisi effettuata è valida presupponendo che tutte le KDF si comportino come

Difetti di progettazione

Cohn-Gordon analysis (CGCD*17)

36



dell'Applicazione L'analisi effettuata è valida presupponendo che tutte le KDF si comportino come oracoli che restituiscono un output simile a un output casuale.

3 Crittografia Applicazioni Definiamo questa condizione come random oracle model. 4 Signal

SIGNAL

Signal Protocol

Difetti di progettazione

Difetti di progettazione

Il paper [CGCD+17] è il primo studio scientifico a riportare un'analisi formale dell'interazione tra X3DH e Double Ratchet.

Difetti di progettazione

Cohn-Gordon analysis (CGCD*17)

L'analisi effettuata è valida presupponendo che tutte le KDF si comportino come Definismo muesta condizione come random oracle mode



progettazione WhatsApp VS Signal

36

SIGNAL Cohn-Gordon analysis (CGCD*17) Difetti di progettazione Signal Protocol Cohn-Gordon analysis [CGCD⁺17] Difetti di progettazione esso, come in effetti anche il nottocollo Signal, non differenzia gli identificatori di sessione (i.e. FID della sessione Alice-Bob è lo stesso ID della sessione Difetti di progettazione UKS è un attacco prevenibile a livello di applicazione (introducendo degli identificativi per gli utenti, e.g., il numero di telefono). 2 Applicazione N.B. Gli attacchi possono variare a seconda dell'implementazione fornita del protocollo, ma il protocollo in sé non presenta difetti rilevanti. Storia dell'Applicazione L'attacco UKS individuato in [FMB⁺16] non è valido in questo modello perché esso, come in effetti anche il protocollo Signal, non differenzia gli identificatori di sessione (i.e. l'ID della sessione Alice-Bob è lo stesso ID della sessione Alice-Charlie).

Difetti di progettazione

3 Crittografia Applicazioni 4 Signal Protocol Il protocollo progettazione WhatsApp VS Signal

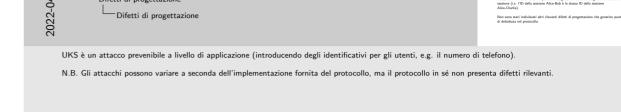
Difetti di progettazione Cohn-Gordon analysis [CGCD⁺17] 2 Applicazione L'attacco UKS individuato in [FMB⁺16] non è valido in questo modello perché esso. come in effetti anche il protocollo Signal, non differenzia gli identificatori di sessione (i.e. l'ID della sessione Alice-Bob è lo stesso ID della sessione Alice-Charlie). Non sono stati individuati altri rilevanti difetti di progettazione che generino punti di debolezza nel protocollo.

dell'Applicazione

3 Crittografia

Applicazioni 4 Signal

progettazione



Difetti di progettazione

Cohn-Gordon analysis (CGCD*17)

SIGNAL

Signal Protocol

Difetti di progettazione

Considerazioni

2022-04-25

38

SIGNAL

Signal Protocol

— Considerazioni Considerazioni Considerazioni

2 Applicazione Signal dell'Applicazione

L'Applicazione e il Protocollo Signal 3 Crittografia

End-to-End

4 Signal Protocol

Proprietà

VS Telegram 5 Bibliografia

Difetti di progettazione Considerazioni WhatsApp VS Signal

Applicazioni

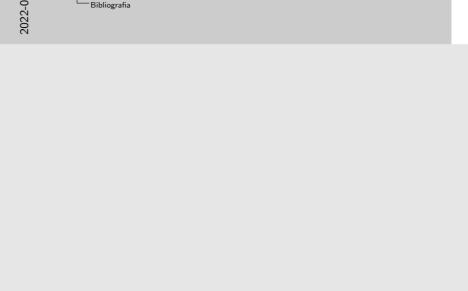
Bibliografia I Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and 2 Applicazione Douglas Stebila. A formal security analysis of the signal messaging protocol. In 2017 IEEE European Symposium on Security and Privacy (EuroS P), pages 451-466, 2017. W Diffie and M Hellman. New directions 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 WhatsApp VS Signal protect journalists. 5 Bibliografia 2016. May 1.

dell'Applicazione

Protocollo Signal

4 Signal

Difetti di



Ribliografia I

W Diffic and M Hellman New directions in cryptography.

Katrial Cohn, Gordon, Cas Cremers, Renjamin Douline, Luke Garratt, and

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

A formal security analysis of the signal messaging protocol

SIGNAL

- Bibliografia

Bibliografia II 2 Applicazione

Filman Frosch, Christian Mainka, Christoph Bader, Florian Bergsma, Jörg Schwenk, and Thorsten Holz. How secure is textsecure? In 2016 IEEE European Symposium on Security and Privacy (EuroS P), pages

457-472, 2016. Barton Gellman and Jerry Markon. Edward snowden says motive behind leaks was to expose 'surveillance state'. The Washington Post. June 10, 2013.

Difetti di Yael Grauer.

Mr. robot uses protonmail, but it still isn't fully secure. 2015. October 7.

— Bibliografia

SIGNAL

- Bibliografia

Ribliografia II

Yael Grauer.

How secure is textsecure?

Tilman Frosch, Christian Mainka, Christoph Bader, Florian Bergsma, Jöre

Mr. robot uses notonmail, but it still isn't fully secure

dell'Applicazione Protocollo Signal

3 Crittografia

4 Signal

WhatsApp VS Signal

5 Bibliografia



Bibliografia IV

Apr. 5, 2016.

Hugo Krawczyk and Pasi Eronen. Hmac-based extract-and-expand key derivation function (hkdf)'.

2 Applicazione 2010.

dell'Applicazione Protocollo Signal 3 Crittografia

4 Signal

Protocol Difetti di

WhatsApp VS Signal 5 Bibliografia

Ben Lutkevich and Madelyn Bacon. end-to-end encryption (e2ee). June 2021. David J Lumb. The story of signal. Increment, (7), 2018, October. Moxie Marlinspike. Whatsapp's signal protocol integration is now complete.

42

SIGNAL

- Bibliografia

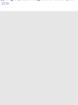
— Bibliografia

Moxie Marlinspike. Whatsapp's signal protocol integration is now complete.

Bibliografia IV

David J Lumb. The story of signal.

Hugo Krawryck and Paci Empen



Hmar-hased extract-and-exmand key derivation function (birdf) Ben Lutkevich and Madelyn Bacon end-to-end encryption (e2ee).



Bibliografia V

Moxie Marlinspike and Trevor Perrin. The double ratchet algorithm.

Technical report, Open Whisper Systems, 2016.

L'Applicazione e il Protocollo Signal 3 Crittografia

2 Applicazione

dell'Applicazione

Moxie Marlinspike and Trevor Perrin.

The x3dh key agreement protocol.

Technical report, Open Whisper Systems, 2016.

4 Signal Protocol

Moxie Marlinspike and Trevor Perrin.

The sesame algorithm: Session management for asynchronous message

Difetti di

encryption. WhatsApp VS Signal Technical report, Open Whisper Systems, 2017.

progettazione









SIGNAL

- Bibliografia

— Bibliografia

Bibliografia V

Movie Martinspike and Treum Parrin The double ratchet algorithm. Moxie Marlinspike and Trevor Perrin

The x3dh key agreement protocol. Technical report. Open Whisper Systems, 2016. Moxie Marlinspike and Trevor Perrin.

The sesame algorithm: Session management for asynchronous message

Bibliografia VI

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

- 4 Signal Protocol
- Proprietà Difetti di
- WhatsApp VS Signal 5 Bibliografia

- Video. K Poulsen.
- Mike Pound. Double ratchet messaging encryption - computerphile.
 - Snowden's email provider loses appeal over encryption keys.

Encrypted e-mail company hushmail spills to feds.

- 2014, April 16.
- Signal documentation. Ryan Singel.
 - 2007. November 7.

-Bibliografia

SIGNAL

- ____Bibliografia

Ribliografia VI

R K Poulsen.

Signal documentation Ryan Singel.

Mike Pound.

Double ratchet messaging encryption - computerabile

Encrypted e-mail company hushmail spills to feds.

Snowlen's amail requirer loses anneal over encountion leve



Bibliografia VII





Dion Van Dam.

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

protocol.

End-to-End

4 Signal

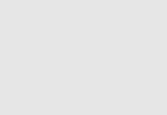
Protocol Difetti di WhatsApp VS Signal 5 Bibliografia

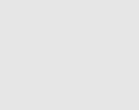
Master's thesis, Radboud University, 2019.

SIGNAL

-Bibliografia

Bibliografia



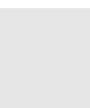




Bibliografia VII

Dion Van Dam.

Master's thesis Radboud University 2019



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

