

2 Applicazione

Storia dell'Applicazione

Applicazioni

4 Signal

Difetti di

Signal VS WhatsApp

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.

Storia dell'Applicazione

SIGNAL

Applicazione Signal

Storia dell'Applicazione

- Applicazione Signal

Nel 2013 Marlinspike abbandona Twitter e fonda la OWS.

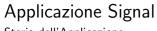
Nel 2011 Twitter acquista Whisper Systems e Marlinspike diventa capo della cybersecurity del social media.

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



Storia dell'Applicazione

dell'Applicazione Protocollo Signal

Applicazioni 4 Signal

Difetti di

Signal VS WhatsApp

applicazione Chrome), per poi rilasciarlo anche per Windows, Mac e Linux nel 2017.

A seguito del nuovo rilascio delle applicazioni nel 2011 i due servizi assumono la propria natura **open-source** che ancora oggi caratterizza l'applicazione Signal. Nel 2013 Marlinspike fonda il progetto open-source Open Whisper Systems, grazie a cui rilascia la prima versione di Signal nel 2015 (anche per PC come

SIGNAL

Storia dell'Applicazione Applicazione Signal Nel 2013 Marlinspike abbandona Twitter e fonda la OWS.

Applicazione Signal

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

Applicazione Signal Storia dell'Apolicazione

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





2 Applicazione

dell'Applicazione

L'Applicazione e il Protocollo Signal 3 Crittografia

Applicazioni

4 Signal

Difetti di Signal VS WhatsApp

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. [1]

SIGNAL

Applicazione Signal

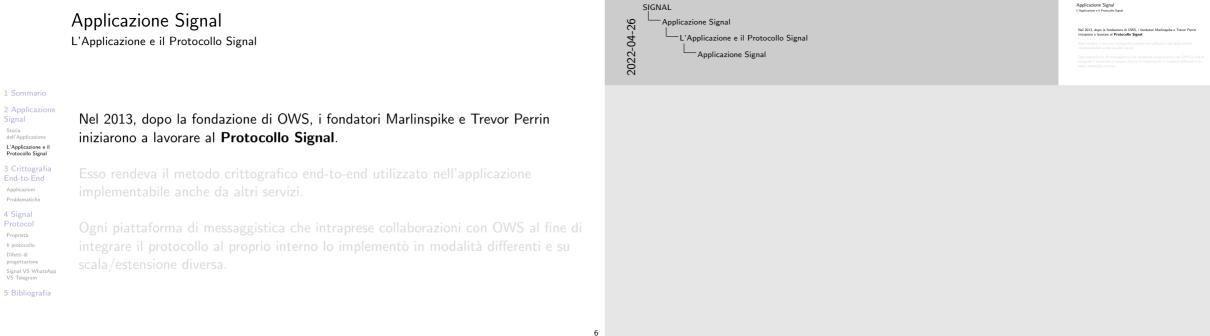
Storia dell'Applicazione



Applicazione Signal

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

Storia dell'Apolicazione





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

Applicazioni

Difetti di Signal VS WhatsApp L'Applicazione e il Protocollo Signal

2 Applicazione 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

implementabile anche da altri servizi.

4 Signal Protocol

SIGNAL

Applicazione Signal

iniziarono a lavorare al Protocollo Signal L'Applicazione e il Protocollo Signal Esso rendeva il metodo crittografico end-to-end utilizzato nell'applicazione Applicazione Signal

Applicazione Signal

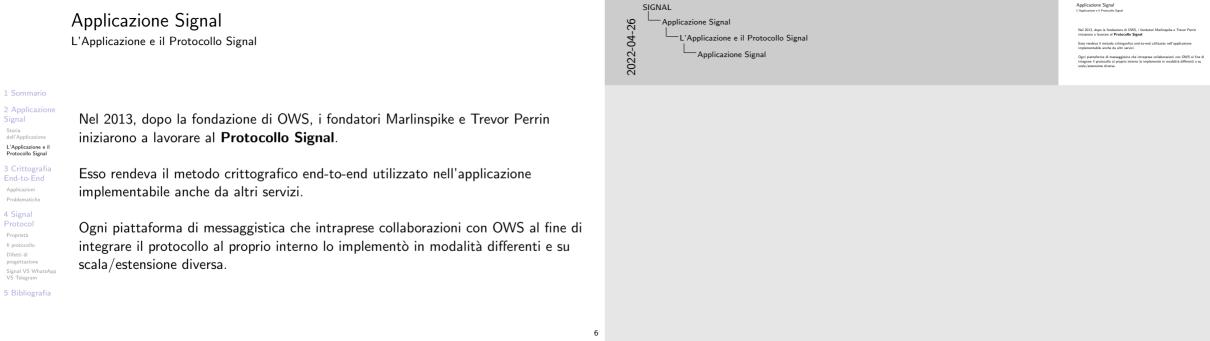
Nel 2013, dono la fondazione di CWS, i fondatori Marlinsnike e Treuve Perrin











L'Applicazione e il Protocollo Signal

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

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

- Tra le più note implementazioni (parziali) del protocollo troviamo:
 - ► Facebook: introdusse la feature Secret Conversations per gli utenti di

Applicazione Signal Facebook: usa Signal solo nelle Secret Conversations

SIGNAL

L'Applicazione e il Protocollo Signal Applicazione Signal

Applicazione Signal

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

L'Applicazione e il Protocollo Signal

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

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

- Tra le più note implementazioni (parziali) del protocollo troviamo:
 - ► Facebook: introdusse la feature Secret Conversations per gli utenti di Facebook Messenger nel luglio 2016
 - Allo: rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in

SIGNAL

Applicazione Signal

- Facebook: introdusse la feature Secret Conversations per eli utenti di Facebook Messenger nel luglio 2016 L'Applicazione e il Protocollo Signal - Applicazione Signal Facebook: usa Signal solo nelle Secret Conversations

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

Applicazione Signal

Tra le niù note implementazioni (narziali) del protocollo troviamo

L'Applicazione e il Protocollo Signal

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

4 Signal

Difetti di Signal VS WhatsApp

5 Bibliografia

Tra le più note implementazioni (parziali) del protocollo troviamo:

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

Applicazione Signal

SIGNAL

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

► Allo: rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata i

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

L'Applicazione e il Protocollo Signal

Applicazione Signal

• 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 Signal VS WhatsApp

5 Bibliografia

Tra le più note implementazioni (parziali) del protocollo troviamo:

- ► Facebook: introdusse la feature Secret Conversations per gli utenti di Facebook Messenger nel luglio 2016
- Allo: rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata in modalità incognito
- **Duo**: protezione delle videochat
- **Skype**: conversazioni private dal 2018

SIGNAL Applicazione Signal Tra le niù note implementazioni (parziali) del protocollo troviamo Facebook Messenger nel luglio 2016 L'Applicazione e il Protocollo Signal ► Allo: rilasciata nel settembre 2016, sfruttava il protocollo se utilizzata i Applicazione Signal Facebook: usa Signal solo nelle Secret Conversations

Applicazione Signal

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

L'Applicazione e il Protocollo Signal

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

4 Signal

Difetti di

Signal VS WhatsApp

- Tra le più note implementazioni (parziali) del protocollo troviamo:
 - ▶ Facebook: introdusse la feature Secret Conversations per gli utenti di Facebook Messenger nel luglio 2016
 - Allo: rilasciata nel settembre 2016, sfruttava il protocollo 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

SIGNAL

Tra le niù note implementazioni (parziali) del protocollo troviamo Facebook Messenger nel luglio 2016 ► Allo: rilasciata nel settembre 2016. sfruttava il protocollo 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

L'Applicazione e il Protocollo Signal

Applicazione Signal

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

Difetti di

Signal VS WhatsApp

4 Signal

[2], [1]

Tra le più note implementazioni (parziali) del protocollo troviamo:

- ▶ Facebook: introdusse la feature Secret Conversations per gli utenti di Facebook Messenger nel luglio 2016
- Allo: rilasciata nel settembre 2016, sfruttava il protocollo 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)

L'Applicazione e il Protocollo Signal Applicazione Signal

SIGNAL

Applicazione Signal

Tra le niù note implementazioni (parziali) del protocollo troviamo ► Facebook: introdusse la feature Secret Conversations per eli utenti di Facebook Messenger nel luglio 2016 ► Allo: rilasciata nel settembre 2016. sfruttava il protocollo 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

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 il Protocollo Signal

3 Crittografia

Applicazioni

Signal VS WhatsApp

4 Signal

contenuto che viene scambiato

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

Ciascuna di queste features richiede che le conversazioni intraprese siano dichiarate

Applicazione Signal L'Applicazione e il Protocollo Signal Applicazione Signal

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

Applicazione Signal

La dichiarazione delle conversazioni come "private" avviene in genere per selezione esplicita da parte dell'utente e non di default. WhatsApp implementa automaticamente la crittografia end-to-end sia per le chat private che per quelle di gruppo, tuttavia se si vuole verificare che le

conversazioni siano private è necessario che entrambe le persone che partecipano alla conversazione selezionino la chat di interesse, clicchino sul nome del contatto, selezionino l'opzione "Crittografia" e scannerizzino il codice QR che viene presentato sul dispositivo dell'altro utente oppure confrontino i numeri a 60 cifre presentati.

L'Applicazione e il Protocollo Signal

2 Applicazione

dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia

Applicazioni

4 Signal

Difetti di

Signal VS WhatsApp

Inoltre, conversazioni già avvenute non possono essere protette applicando il

"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

protocollo ex post.

SIGNAL

Applicazione Signal

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

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

Applicazione Signal

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

Storia dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia

4 Signal

Difetti di

Signal VS WhatsApp

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

- ► Salvano solo le informazioni strettamente necessarie

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

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

Applicazione Signal L'Applicazione e il Protocollo Signal Applicazione Signal

SIGNAL

Applicazione Signal

L'Applicazione e il Protocollo Signal

- 2 Applicazione

dell'Applicazione L'Applicazione e i

Protocollo Signal 3 Crittografia

4 Signal

Difetti di

Signal VS WhatsApp

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

- ► Salvano solo le informazioni strettamente necessarie
- ▶ Rendono impossibile a terze parti accedere ai messaggi o ai file scambiati tra

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



SIGNAL

Applicazione Signal

L'Applicazione e il Protocollo Signal tutti i prodotti OWS sono incentrati sulla privacy deeli utenti. infatti Applicazione Signal

► 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 Signal VS WhatsAnn

VS Telegram

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

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

La crittografia End-to-End (E2EE) è un processo di comunicazione sicura ch

mpedisce 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.

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

gli Internet provider e utenti malevoli

2 Applicazione

ria 'Applicazione

dell'Applicazione L'Applicazione e

3 Crittografia

End-to-End
Applicazioni

Applicazioni Problematich

4 Signal

Protocol
Proprietà
Il protocollo
Difetti di

II protocollo Difetti di progettazione Signal VS WhatsApp

VS Telegram

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

Crittografia End-to-End

La critagrafia End to End (EXE) a an process of consortance does the imported a factor for a factor for a confidence of the imported a factor for a factor for a confidence of the imported a factor for a factor for

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.

End-to-End Encryption

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

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

2 Applicazione

dell'Applicazione

3 Crittografia

End-to-End

4 Signal

Difetti di progettazione

Signal VS WhatsAni VS Telegram

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. [4]

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

End-to-End Encryption

si tratta di dati presentati in un formato non leggibile Grazie alla E2EE è possibile proteggere i dati trasmessi da terze parti malintenzionate che possono includere i provider dei servizi di telecomunicazione

gli Internet provider e utenti malevoli

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

E2EE si basa sulla crittografia asimmetrica.

- 2 Applicazione Signal

Storia dell'Applicazione

3 Crittografia

End-to-End

4 Signal

Difetti di

progettazione VS Telegram

Signal VS WhatsApp

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

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

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

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

SIGNAL

End-to-End Encryption

Crittografia End-to-End

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

3 Crittografia

End-to-End

4 Signal

Difetti di

progettazione Signal VS WhatsAnn 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

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

SIGNAL

Crittografia End-to-End

dunque conservabili solo in ciphertext.

La crittografia asimmetrica, o a chiave pubblica, cifra e decifra i dati usando due ► La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario End-to-End Encryption I messaggi vengono crittografati dal mittente, pertanto, anche se intercettati da una terza persona, essi non le saranno visibili in plaintext e saranno

End-to-End Encryption

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

2 Applicazione Signal

Storia dell'Applicazione

3 Crittografia

End-to-End

4 Signal

Difetti di progettazione Signal VS WhatsAnn

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

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.

2 Applicazione Signal

dell'Applicazione

Protocollo Signal 3 Crittografia

End-to-End

4 Signal

Difetti di progettazione Signal VS WhatsAn 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

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

chiave privata.

SIGNAL

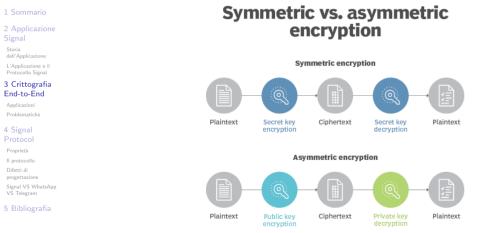
Crittografia End-to-End

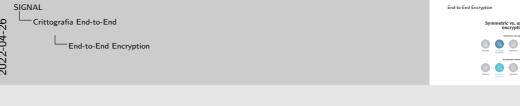
La crittografia asimmetrica, o a chiave pubblica, cifra e decifra i dati usando du ► La chiave pubblica è usata per cifrare un messaggio e inviarlo al proprietario --- End-to-End Encryption In seguito, il messaggio può essere decifrato solo utilizzando la corrispondent Al contrario, la crittografia simmetrica 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 dunque conservabili solo in ciphertext.

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





Applicazioni

dell'Applicazione

Protocollo Signal

Applicazioni

4 Signal

Signal VS WhatsApp

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

▶ **Gestione password**: a entrambi gli endpoint della comunicazione si trova lo

Data storage: nei servizi di storage in cloud può anche essere garantita E2EE

Alcuni sistemi, come ad esempio Lavabit e Hushmail, hanno in passato dichiarato di implementare la crittografia end-to-end nonostante ciò non fosse vero. [6] 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 compagnia aveva in precedenza dichiarato che il proprio livello di sicurezza era

tale che nemmeno gli amministratori avevano accesso al contenuto delle mail scambiate dai propri utenti. [7], [8]

SIGNAL

plaintext, [9]

Crittografia End-to-End

End-to-End Encryption

-Applicazion

Hushmail, altro email provider dichiarato sicuro, utilizzò le password dei propri utenti per decrittare le email e consegnarle al governo federale in

End-to-End Encryption

mantanam mirata la conversazioni deali utenti

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, oltre al fatto che utilizza il protocollo di crittografia

non standard MTProto. [10]

13

Applicazioni

dell'Applicazione Protocollo Signal

Applicazioni

4 Signal

progettazione

- ► Comunicazioni sicure: applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- ▶ Gestione password: a entrambi gli endpoint della comunicazione si trova lo stesso utente. l'unica persona munita di chiave:
- Data storage: nei servizi di storage in cloud può anche essere garantita E2EE

Alcuni sistemi, come ad esempio Lavabit e Hushmail, hanno in passato dichiarato di implementare la crittografia end-to-end nonostante ciò non fosse vero. [6] 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 compagnia aveva in precedenza dichiarato che il proprio livello di sicurezza era tale che nemmeno gli amministratori avevano accesso al contenuto delle mail scambiate dai propri utenti. [7], [8] Hushmail, altro email provider dichiarato sicuro, utilizzò le password dei propri utenti per decrittare le email e consegnarle al governo federale in plaintext, [9]

End-to-End Encryption

► Comunicazioni sicure: anniicazioni di messaggistica e nosta elettronica ne mantenere private le conversazioni degli utenti;

► Gestione password: a entrambi eli endocint della comunicazione si trova lo

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, oltre al fatto che utilizza il protocollo di crittografia non standard MTProto. [10]

13

SIGNAL

Crittografia End-to-End

End-to-End Encryption

-Applicazion

Applicazioni

dell'Applicazione Protocollo Signal

Applicazioni

4 Signal

Difetti di Signal VS WhatsApp



- ► Comunicazioni sicure: applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- ▶ Gestione password: a entrambi gli endpoint della comunicazione si trova lo stesso utente. 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.

Crittografia End-to-End ► Comunicazioni sicure: anniirazioni di messaggistica e nosta elettronica ne mantenere private le conversazioni degli utenti; -Applicazion ► Gestione nassword: a entrambi eli endocint della comunicazione si trova le ▶ Data storage: nei servizi di storage in cloud nuò anche essere garantita ESE End-to-End Encryption in transit, proteggendo i dati degli utenti anche dall'accesso da parte dei

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. [6]

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 compagnia aveva in precedenza dichiarato che il proprio livello di sicurezza era tale che nemmeno gli amministratori avevano accesso al contenuto delle mail scambiate dai propri utenti. [7], [8] Hushmail, altro email provider dichiarato sicuro, utilizzò le password dei propri utenti per decrittare le email e consegnarle al governo federale in

plaintext, [9] 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, oltre al fatto che utilizza il protocollo di crittografia non standard MTProto. [10]

13

Problematiche

2 Applicazione Signal

Storia dell'Applicazione

3 Crittografia

Applicazioni

Problematiche 4 Signal

Difetti di progettazione

Signal VS WhatsApp

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

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

SIGNAL

trasmessi potrebbero essere protetti in modo poco sicuro sui dispositivi endpoint

End-to-End Encryption

La EZEE non garantisco di nor sé né la sicusarza né la privacy in quanto i da

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

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

Problematiche

2 Applicazione Signal

dell'Applicazione

Applicazioni

Il protocollo

Difetti di

Problematiche 4 Signal

Signal VS WhatsApp

progettazione

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. [11], [5]

SIGNAL

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

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 dati misliore della sola crittografia "in transit" Per molti sistemi di messaggistica i messaggi passano attraverso un intermediario che E conserva finché non venzono recunerati dal destinatario. Anche se motetti d crittografia, essi lo sono solamente in transito, quindi nossono essere letti da

End-to-End Encryption

provider di servizi. [11], [5]

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

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

Problematiche

2 Applicazione Signal

dell'Applicazione

Protocollo Signal

Problematiche

4 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



- 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. 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)

End-to-End Encryption

• Backdoors: nonostante le backdoors non siano sempre implementate volutamente, esse possono essere introdotte grazie a cyber-attacks e poi essere utilizzate per la negoziazione delle chiavi o per oltrepassare la protezione crittografica.

15

SIGNAL

Crittografia End-to-End

Problematiche

2 Applicazione

dell'Applicazione

Protocollo Signal 3 Crittografia

Problematiche

4 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



Crittografia End-to-End ► Endonint security: eli endonint sono vulnerabili se non protetti — Problematiche 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. 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)

End-to-End Encryption

• Backdoors: nonostante le backdoors non siano sempre implementate volutamente, esse possono essere introdotte grazie a cyber-attacks e poi essere utilizzate per la negoziazione delle chiavi o per oltrepassare la protezione crittografica.

Problematiche

2 Applicazione

dell'Applicazione

Protocollo Signal 3 Crittografia

Problematiche 4 Signal

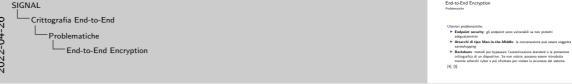
Difetti di

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

[4], [5]





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

Problematiche

- 2 Applicazione
- dell'Applicazione

Problematiche 4 Signal

Difetti di Signal VS WhatsApp

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

SIGNAL

Crittografia End-to-End

-- Problematiche End-to-End Encryption

definire accuratamente eli estremi della trasmissione

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

End-to-End Encryption

Problematiche

- dell'Applicazione
- Protocollo Signal

Problematiche

4 Signal

Difetti di

di decodificare e ricodificare i dati lungo il percorso, quindi è necessario definire accuratamente gli estremi della trasmissione

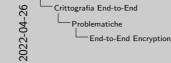
Privacy "eccessiva": enti governativi non hanno modo di verificare la natura dei contenuti trasmessi dagli utenti, pertanto non sono in grado di prendere misure adeguate in caso di illeciti

► Complessità nel definire gli endpoint: alcune implementazioni consentono

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

Signal VS WhatsApp







- ► 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

Problematiche

- dell'Applicazione
- Protocollo Signal

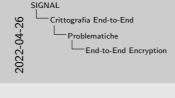
Problematiche

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

Signal VS WhatsApp





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

► Complessità nel definire «li endonint: alcune implementazioni consentone

misure adequate in caso di illeciti

Problematiche

- dell'Applicazione Protocollo Signal

Problematiche

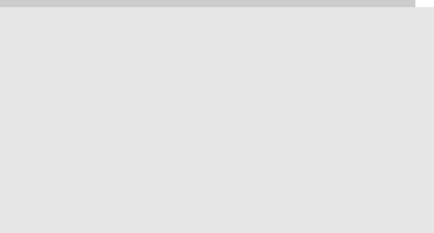
4 Signal

Difetti di progettazione

- ► 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

[12]

Signal VS WhatsApp



End-to-End Encryption

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

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

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

definire accuratamente eli estremi della trasmissione

misure adequate in caso di illeciti

SIGNAL

Crittografia End-to-End

End-to-End Encryption

— Problematiche

Proprietà

2 Applicazione

Storia dell'Applicazione

4 Signal

Protocol Proprietà

L'Applicazione e il Protocollo Signal 3 Crittografia

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in ambito crittografico:

- Confidenzialità
- Integrità

Autenticità

Signal VS WhatsApp

SIGNAL

Signal Protocol

digitali

Signal Protocol

• Integrità: dati trasmessi non danneggiati e/o dispersi

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

• 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

Signal Protocol

► Autenticità

Confidenzialiti

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in

Proprietà

- 2 Applicazione

Storia dell'Applicazione

L'Applicazione e i Protocollo Signal

3 Crittografia

4 Signal Protocol

Proprietà

Signal VS WhatsApp

Integrità

ambito crittografico:

Confidenzialità

Autenticità

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in

Le proprietà CIA spesso vengono accompagnate dalla non ripudiabilità

SIGNAL

Signal Protocol

Signal Protocol

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

• Integrità: dati trasmessi non danneggiati e/o dispersi

digitali

• 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

Signal Protocol

ambito crittografico: Confidenzialiti ► Integrità

► Autenticità

Tradizionalmente facciamo riferimento a tre proprietà come requisiti principali in

Le proprietà CIA spesso vengono accompagnate dalla non ripudiabilità

Proprietà

2 Applicazione

dell'Applicazione

3 Crittografia

4 Signal

Proprietà Difetti di progettazione

Signal VS WhatsApp

Ulteriori proprietà spesso richieste sono:

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



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

Signal Protocol

Illteriori proprietà spesso richieste sono

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.

Proprietà

2 Applicazione

dell'Applicazione

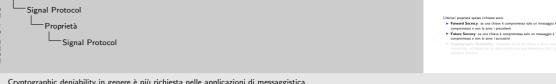
3 Crittografia

4 Signal Proprietà

Difetti di progettazione Signal VS WhatsApp

Ulteriori proprietà spesso richieste sono:

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



Signal Protocol

Cryptographic deniability in genere è più richiesta nelle applicazioni di messaggistica

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.

Proprietà

2 Applicazione

dell'Applicazione Protocollo Signal

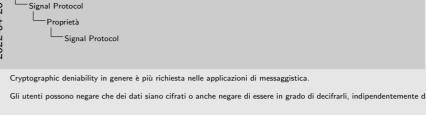
3 Crittografia

4 Signal

Proprietà Difetti di progettazione Signal VS WhatsApp

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.



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

Cryptographic Depiability: Essistenza di un file cifrato o di un messaggio

rinnegabile, nel senso che un altro utente non può dimostrare che i dati in

Signal Protocol

Gli utenti possono negare che dei dati siano cifrati o anche negare di essere in grado di decifrarli, indipendentemente dal fatto che ciò sia vero o meno

Signal Protocol

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

4 Signal

II protocollo

Applicazioni

dell'Applicazione

Il protocollo Signal fornisce crittografia end-to-end a sistemi di messaggistica

End-to-End istantanea e di chiamate vocali, combinando l'algoritmo "Double Ratchet", pre-chiavi e un triplo handshake Elliptic-curve Diffie-Hellman (3-DH).

Protocol

Difetti di





- progettazione Signal VS WhatsApp

Il protocollo

2 Applicazione

dell'Applicazione

3 Crittografia

4 Signal

II protocollo Difetti di Signal VS WhatsApp

Le specifiche di riferimento sono infatti: [13]

- **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

Signal Protocol

Il protocollo

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

Signal Protocol

Le specifiche di riferimento sono infatti: [13]

► ¥3DH: protocollo di negoziazione delle chiavi Extended Trinle Diffie.Hellman

Il protocollo

Il protocollo

dell'Applicazione

Protocollo Signal

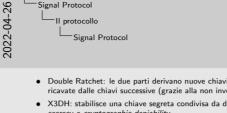
3 Crittografia

4 Signal

II protocollo Difetti di progettazione Signal VS WhatsApp

Le specifiche di riferimento sono infatti: [13]

- **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.



SIGNAL

Le specifiche di riferimento sono infatti: [13] > X3DH: protocollo di negoziazione della chiavi Extended Tripla Diffia Hallman ► Double Ratchet: alsoritmo utilizzato da due parti per lo scambio di messassi

Signal Protocol

Il protocollo

 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

Il protocollo

dell'Applicazione

Protocollo Signal

3 Crittografia

4 Signal

II protocollo Difetti di

Signal VS WhatsApp

Le specifiche di riferimento sono infatti: [13]

- **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 Protocol II protocollo ricavate dalle chiavi successive (grazie alla non invertibilità della funzione ratchet)

SIGNAL

Le specifiche di riferimento sono infatti: [13] > X3DH: protocollo di negoziazione della chiavi Extended Tripla Diffia Hallman Signal Protocol

► Double Ratchet: alsoritmo utilizzato da due parti per lo scambio di messaggi ► Sesame: eestisce le sessioni crittografate in ambiente asincrono e multi-device

Signal Protocol Il protocollo

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

• 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

Il protocollo: fasi di funzionamento [14]

- 2 Applicazione

Signal

dell'Applicazione

4 Signal

II protocollo Difetti di

Signal VS WhatsApp

► 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,

- ► DH ratchet phase

Symmetric ratchet phase

CONVERSATION: Alice e Bob possiedono la chiave segreta condivisa e

SIGNAL

Signal Protocol II protocollo Signal Protocol

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

Signal Protocol

Il materially, first all forest receives (14)

• 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.

Il protocollo: fasi di funzionamento [14]

- 2 Applicazione Signal
- dell'Applicazione Protocollo Signal

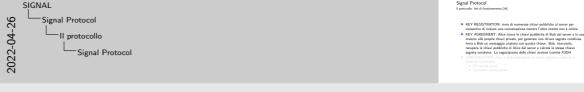
4 Signal

II protocollo

Difetti di progettazione Signal VS WhatsApp

- ► 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



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.

Il protocollo: fasi di funzionamento [14]

- 2 Applicazione Signal
- dell'Applicazione
- Protocollo Signal

4 Signal

II protocollo Difetti di progettazione Signal VS WhatsApp

possono conversare.

Symmetric ratchet phase

► 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

SIGNAL Signal Protoco II protocollo Signal Protocol Signal Protocol

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 us segreta condivisa. La negoziazione delle chiavi avviene tramite X3DH

► DH ratchet share 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.

Il protocollo: fasi di funzionamento

- 2 Applicazione

Storia dell'Applicazione

3 Crittografia

Applicazioni

4 Signal Protocol

Difetti di

II protocollo Signal VS WhatsApp





- Symmetric ratchet phase

 - Derivazione di una nuova chiave dalla chiave segreta condivisa.

- Signal Protocol Il protocollo Signal Protocol

SIGNAL

- - Symmetric ratchet phase Derivazione di una nuova chiave dalla chiave serreta condivisa.

Signal Protocol









Il protocollo: fasi di funzionamento

2 Applicazione

dell'Applicazione Protocollo Signal

3 Crittografia

Applicazioni

4 Signal Protocol



Difetti di

Signal VS WhatsApp

II protocollo

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 Signal Protocol II protocollo Signal Protocol Signal Protocol

Symmetric ratchet phase Derivazione di una nuova chiave dalla chiave segreta condivisa Se Aline invia nii) messaggi a Roh senza ringuere risnosta ngni messaggin sarb

criptato con una nuova chiave calcolata in funzione della precedente.

Il protocollo: fasi di funzionamento

2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

Applicazioni

4 Signal Protocol

II protocollo Difetti di

Signal VS WhatsApp

Symmetric ratchet phase

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

SIGNAL Signal Protocol II protocollo Signal Protocol

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 Protocol

Diffie-Hellman ratchet phase

Il protocollo: fasi di funzionamento

2 Applicazione

dell'Applicazione

3 Crittografia

Applicazioni

4 Signal Protocol

Proprietà

Signal VS WhatsApp





II protocollo Difetti di







Generazione di una nuova chiave segreta condivisa.

SIGNAL

Signal Protocol II protocollo Signal Protocol

Signal Protocol







Il protocollo: fasi di funzionamento

dell'Applicazione

Applicazioni

Signal VS WhatsApp

4 Signal Protocol

3 Crittografia

II protocollo Difetti di







Generazione di una nuova chiave segreta condivisa.

Se Bob invia un nuovo messaggio ad Alice genera una nuova coppia di chiavi effimere. Bob usa queste chiavi 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

Signal Protocol

effimere. Boh usa mueste chiavi ner calcolame una nuova condivisa, inviando noi l propria chiave effimera ad Alice per farle calcolare la chiave condivisa.

Il protocollo: fasi di funzionamento

2 Applicazione

dell'Applicazione

Applicazioni

4 Signal

Protocol

II protocollo Difetti di

Signal VS WhatsApp

3 Crittografia

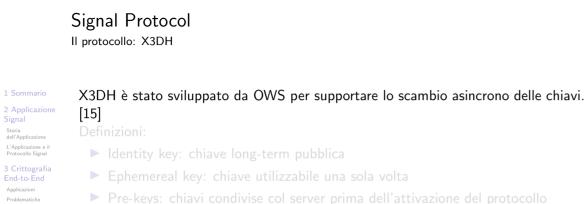
Diffie-Hellman ratchet phase

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 queste chiavi 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 Signal Protocol II protocollo Signal Protocol Signal Protocol

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



4 Signal

II protocollo

Signal VS WhatsApp

- ► Identity key: chiave long-term 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 condivise col server prima

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

SIGNAL

Signal Protocol

private (secret keys) sk.

II protocollo Signal Protocol

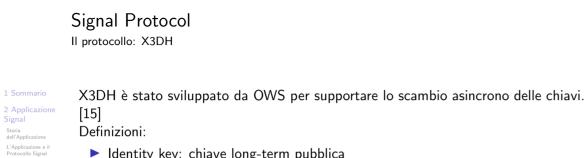
- Dopodiché scambiano le chiavi pubbliche attraverso un canale e da esse possono derivare una chiave segreta condivisa ssk. Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

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 svilunnato da OWS per supportare lo scambio asincrono delle chia

II sestember Valle



4 Signal

II protocollo

Signal VS WhatsApp

- ▶ Identity key: chiave long-term 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 condivise col server prima

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

SIGNAL

Signal Protocol

private (secret keys) sk.

II protocollo Signal Protocol

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 e da esse possono derivare una chiave segreta condivisa ssk. Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

Signal Protocol

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

II sestember Valle

► Identity key: chiave long-term 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 condivise col server prima

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

II protocollo: X3DH

Definizioni:

- 2 Applicazione Signal

Storia dell'Applicazione

3 Crittografia

4 Signal

II protocollo

Signal VS WhatsApp

SIGNAL

Signal Protocol

private (secret keys) sk.

II protocollo Signal Protocol Signal Protocol

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

II sestember Valle

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 e da esse possono derivare una chiave segreta condivisa ssk.

Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

II protocollo: X3DH

- 2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

- 4 Signal
- II protocollo Difetti di

- Signal VS WhatsApp

Definizioni:

- ▶ Identity key: chiave long-term 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 condivise col server prima

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

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



SIGNAL

Signal Protocol

II protocollo

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

Signal Protocol

Identity key: chiave long-term pubblica

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

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

II sestember Valle

Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

Il protocollo: X3DH

2 Applicazione

dell'Applicazione

Protocollo Signal 3 Crittografia

4 Signal

II protocollo Difetti di

Signal VS WhatsApp

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

stanno per finire

Definizioni:

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

▶ Identity key: chiave long-term 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

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

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

private (secret keys) sk.

SIGNAL

Signal Protoco —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 e da esse possono derivare una chiave segreta condivisa ssk.

Signal Protocol

Identity key: chiave long-term pubblica

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

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

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

II sestember Valle

Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

Il protocollo: X3DH

2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

4 Signal

II protocollo Difetti di

▶ One-time pre-keys: insiemi di pre-keys condivise 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 quando Signal VS WhatsApp

stanno per finire

Definizioni:

▶ Identity key: chiave long-term pubblica

► Ephemereal key: chiave utilizzabile una sola volta

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

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

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

24

SIGNAL

Signal Protoco

private (secret keys) sk.

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 e da esse possono derivare una chiave segreta condivisa ssk.

Possono esserci problemi di sicurezza se il canale attraverso cui avviene lo scambio di chiavi non è sicuro. [16], [17]

Signal Protocol

Identity key: chiave long-term pubblica

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

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

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

II protocollo: X3DH

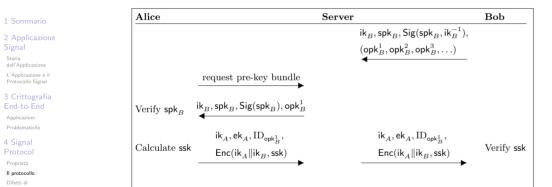


Figure: Funzionamento di X3DH semplificato

SIGNAL

Signal Protocol

Signal Protocol

III protocollo

Signal Protocol

Figure Fundamenta & XXIXI supplicates

Figure Fundamenta & XXIXI supplicates

[14]

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 $(opk^1, opk^2, opk^3, ...)$.

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_B^x . Una volta finite le opk_B ad Alice verranno inviate solo le altre chiavi senza opk_B .

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 Kev Derivation

ricevote le chiavi Ance vernica la liffia di sprig e se va a buoli li

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

[18].

[sof.

Alice invia un messaggio iniziale a Bob contenente ik_A , ek_A , $ID_{opk_B^X}$ (per fargli sapere quale opk_B^X 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. [14]

[14]

25

II protocollo: Double Ratchet

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

19] [14

[19], [1

A different

dell'Applicazione L'Applicazione e il

Protocollo Signal

2 Applicazione

End-to-End

Applicazioni

Problematiche

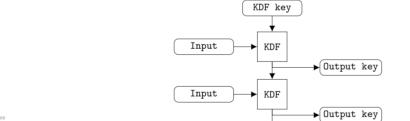
4 Signal

Proprietà

Il protocollo
Difetti di
progettazione

progettazione
Signal VS WhatsApp
VS Telegram

VS Telegram



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 j. Per garantire ciò è necessario usare un DH ratchet

Signal Protocol

Il protocollo: Double Ratchet

Algoritmo utilizzato per il proseguimento della conversazione, dopo averla

KDF key

SIGNAL

Signal Protocol

KDF key

KDF key

Figure: Catena KDF

Output key

► Output key

Input

Input

Il protocollo: Double Ratchet

Algoritmo utilizzato per il proseguimento della conversazione, dopo averla

dell'Applicazione

4 Signal

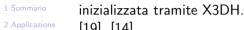
Difetti di

II protocollo

Signal VS WhatsApp







[19], [14]

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













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

Resilienza: l'output appare randomico

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

inizializzata tramite X3DH

Algoritmo utilizzato per il proseguimento della conversazione, dopo averla

[19], [14] A differenza di X3DH usa una catena KDE, come mostrato in fusura 2

Isput - HEF

Figure: Cateria KDF

Il protocollo: Double Ratchet

Signal Protocol

2 Applicazione

dell'Applicazione

L'Applicazione e i Protocollo Signal

3 Crittografia

Applicazioni

4 Signal

II protocollo

Difetti di

Signal VS WhatsApp

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

SIGNAL

Signal Protocol

Il protocollo

Signal Protocol

Signal Protocol

ratchet che garantisce sia forward secrety che future secrety

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

ratchet che garantisce sia forward secrecy che future secrecy.

Il protocollo: Double Ratchet

2 Applicazione

dell'Applicazione L'Applicazione e i Protocollo Signal

4 Signal

Difetti di

Signal VS WhatsApp

II protocollo

3 Crittografia

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 compromessa, si sia in grado di ristabilire la segretezza dall'applicazione successiva di una KDF.

SIGNAL

Signal Protocol

Combinando una catena KDF con un DH ratchet otteniamo un algoritmo Double II protocollo ratchet che garantisce sia forward secrety che future secrety DH ratchet infatti modifica eli input delle KDF in modo tale che, se anche una Signal Protocol

chiave venisse compromessa, si sia in grado di ristabilire la segretezza

Signal Protocol

Il protocollo: Double Ratchet

Il protocollo: Double Ratchet

2 Applicazione

dell'Applicazione

3 Crittografia

4 Signal

Proprietà

II protocollo Difetti di

Signal VS WhatsApp

Protocol

Sending ratchet

DH ratchet

► Receiving ratchet

Sia Alice che Bob hanno tre catene KDF da utilizzare:

II protocollo Signal Protocol

Signal Protocol

SIGNAL

Signal Protocol

► DH ratchet ► Sanding ratchet Receiving ratchet

Il protocollo: Double Ratchet

Sia Alice che Bob hanno tre catene KDF da utilizzare:







Il protocollo: Double Ratchet

2 Applicazione

dell'Applicazione

4 Signal

Signal VS WhatsApp

II protocollo Difetti di

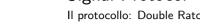
Protocol

3 Crittografia

progettazione





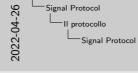




Sia Alice che Bob hanno tre catene KDF da utilizzare:

- 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

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

Signal Protocol

Il protocollo: Double Ratchet

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

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

SIGNAL

Signal Protocol

Il protocollo

Signal Protocol

2 Applicazione

dell'Applicazione L'Applicazione e il Protocollo Signal

3 Crittografia

Applicazioni

4 Signal

Signal VS WhatsApp

II protocollo Difetti di



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

In queste condizioni tuttavia non è ancora garantita la future secrecy

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

L'Applicazione e il Protocollo Signal

Applicazioni

Signal VS WhatsApp

Difetti di

II protocollo

4 Signal

3 Crittografia

Il protocollo: Double Ratchet

dell'Applicazione L'Applicazione e il Protocollo Signal

Applicazioni

4 Signal Protocol

II protocollo Difetti di

Signal VS WhatsApp

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 Signal Protocol

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

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.

N.B. Le chiavi vengono eliminate non appena utilizzate per decifrare un messaggio, se delle chiavi non vengono utilizzate vengono conservate finché non arriverà il messaggio corrispondente.

Il protocollo: Double Ratchet

1 Sommar

2 Applicazio

dell'Applicazione L'Applicazione e

3 Crittogra

Applicazioni

4 Signal

Protoco Proprietà

Proprietà

Il protocollo

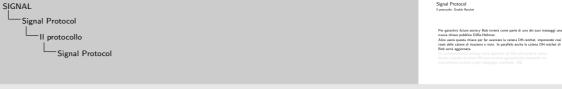
Difetti di progettazione Signal VS WhatsApp

E Bibliograf

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. [20]



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 sequenza 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.

N.B. Le chiavi vengono eliminate non appena utilizzate per decifrare un messaggio, se delle chiavi non vengono utilizzate vengono conservate finché non arriverà il messaggio corrispondente.

Il protocollo: Double Ratchet

1 Sommar

2 Applicazio

dell'Applicazione L'Applicazione e

3 Crittogra

Applicazioni

4 Signal

Protoco Proprietà

II protocollo Difetti di

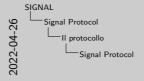
Difetti di progettazione Signal VS WhatsA VS Telegram

. Ribliografi 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



Per garantire future secrety. Bob invierà come parte di uno dei suoi messaggi una nuova chive pubblica Dillis-Hellman.

Alice userà questa chive per fer avanzare la catera DH-ratchet, imponendo codi il resett delle catere di ricezione e invio. In parallelo anche la catera DH-ratchet di Bob verrà aggiornata.

Un comportamento analoso verrià applicato da Bob selle ercorie catera.

Questo scambio di chiavi DH può av

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 sequenza 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.

N.B. Le chiavi vengono eliminate non appena utilizzate per decifrare un messaggio, se delle chiavi non vengono utilizzate vengono conservate finché non arriverà il messaggio corrispondente.

Il protocollo: Double Ratchet

1 Sommar

2 Applicazio Signal

dell'Applicazione
L'Applicazione e
Protocollo Signal

3 Crittogra End-to-End

Applicazioni

4 Signal Protocol

Il protocollo Difetti di

Difetti di progettazione Signal VS Whats VS Telegram

5 Bibliograf

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. [20]



or Paraceters.

Per grantire firture secrety Bob invitar come parte di uno dei suam messaggi una nouse chiave publica Diffie-Hillman. Alice userà questa chiave per fer avanzare la catena DH-ratchet, imponendo così il reset delle catena di riccainne e invic. In parallelo anche la catena DH-ratchet di Bob verrà aggiornata. Un comportamento analogo verrà applicato da Bob sufle proprie catena.

Un comportamento analogo verrà applicato da Bob ssille proprie catene.

Questo scambio di chiavi DH poò avvenire ogniqua/solta necessario ma
normalmente avviene a ogni messaggio scambiato. [20]

Signal Protocol

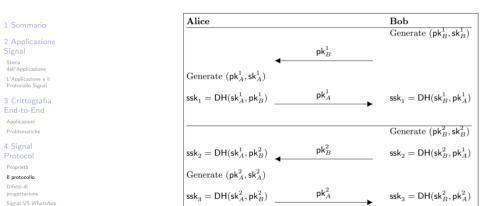
Questo sistema di catene garantisce dunque:

- 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 sequenza 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.

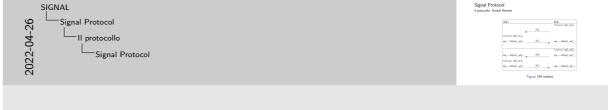
N.B. Le chiavi vengono eliminate non appena utilizzate per decifrare un messaggio, se delle chiavi non vengono utilizzate vengono conservate finché non arriverà il messaggio corrispondente.

Il protocollo: Double Ratchet

VS Telegram



Bibliografia Figure: DH ratchet



31

Il protocollo: Sesame

2 Applicazione

Signal dell'Applicazione L'Applicazione e il Protocollo Signal

Applicazioni

4 Signal Protocol

II protocollo Difetti di

progettazione Signal VS WhatsApp

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

Signal Protocol II protocollo Signal Protocol

SIGNAL

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

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.
- Alice e Bob possono aggiungere o rimuovere dispositivi, iniziando o terminando delle sessioni. • Alice e Bob possono iniziare una nuova sessione allo stesso tempo. Per il funzionamento 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, richiedendo a Bob di concordare nuovamente sulla sessione da utilizzare.

Il protocollo: Sesame

1. C

2 Applicazio

Storia dell'Applicazione L'Applicazione e Protocollo Signal

3 Crittogra

End-to-En

Applicazioni Problematich

4 Signal Protocol

Protoco

Il protocollo
Difetti di
progettazione
Signal VS WhatsApp

Dibliance

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



Signal Protocol
II protocolic: Swame

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.

diventa attiva.
In questo modo ogni dispositivo utilizza una sola sessione per ogni altro dispos remoto con cui comunica. [21]

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.
- Alice e Bob possono aggiungere o rimuovere dispositivi, iniziando o terminando delle sessioni
- Alice e Bob possono iniziare una nuova sessione allo stesso tempo. Per il funzionamento 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, 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 progettazione Signal VS WhatsApp

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. [21]



Ozni disnositivo degli utenti deve tenere tranzia di una sessione attiva ner ner

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.
- Alice e Bob possono aggiungere o rimuovere dispositivi, iniziando o terminando delle sessioni
- Alice e Bob possono iniziare una nuova sessione allo stesso tempo. Per il funzionamento 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, richiedendo a Bob di concordare nuovamente sulla sessione da utilizzare.

Il protocollo: Sesame

2 Applicazione Signal

dell'Applicazione

3 Crittografia

4 Signal

II protocollo Difetti di

Signal VS WhatsApp

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-keys, signed pre-key e identity public key.

Il protocollo: Sesame

1. C.....

2 Applicazione Signal

Storia dell'Applicazione L'Applicazione e il

3 Crittograf

End-to-End

Applicazioni

Problematich

4 Signal Protocol

Proprietà

Il protocollo

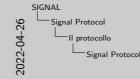
Difetti di

Difetti di progettazione Signal VS WhatsApp VS Telegram

v 5 Telegram

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 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 Protocol Il protocolo: 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 pre-time pre-tieve, signed pre-tie

- e identity public key.

 Il dispositivo mittente recupera dal server la identity public key del dispositivo
- Il dispositivo mittente recupera dal server la identity public key del dispositivo mittente recupera dal server la identity public key del dispositivo destinatario, signed pre-keys e una one-time pre-key se dispositife.
 - x son usa queste chiavi per creare sessione Double Ratchet sia un mi

Il protocollo: Sesame

1 C -----

2 Applicazione Signal

Storia dell'Applicazione L'Applicazione e il Protocollo Signal

3 Crittogra

Applicazioni

Applicazioni Problematiche

4 Signal

Protoco Proprietà

Proprietà
Il protocollo

Il protocollo

Difetti di
progettazione

Signal VS WhatsApp

V5 Telegram

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 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
Signal Protocol
II protocollo
Signal Protocol

Signal Protocol Il protocolo: Sesame

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

Il dispositivi comunicano al server le proprie one-time pre-levs. sirned pre-lev

- e identity public key.

 Il disposition mittente recupera dal server la identity public key de
- Il dispositivo mittente recupera dal server la identity public key del dispositivo destinatario, signed pre-keys e una one-time pre-key se disposibile.
- 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 messarerio iniziale X3DH.

Il protocollo: Sesame

► Il messaggio iniziale X3DH è aggiunto a ogni messaggio di apertura di

▶ I dispositivi comunicano solo con Double Ratchet.

- 2 Applicazione

dell'Applicazione

II protocollo Difetti di

progettazione

Signal VS WhatsApp





SIGNAL

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



34

Ratchet corrispondente.

► 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

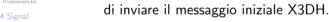
▶ Ricevuto il messaggio di conferma di apertura della sessione il mittente smette

Il protocollo: Sesame

- 2 Applicazione

dell'Applicazione

Signal VS WhatsApp



4 Signal

Protocol

II protocollo

Difetti di

progettazione

▶ I dispositivi comunicano solo con Double Ratchet.

3 Crittografia







34

SIGNAL

Il protocollo Signal Protocol

Signal Protocol

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 massaggio iniziale XRDH è aggiunto a neni messaggio di anertura di





Il protocollo: Sesame

- 2 Applicazione

dell'Applicazione

Protocollo Signal

4 Signal Protocol

II protocollo Difetti di

progettazione Signal VS WhatsApp

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

di inviare il messaggio iniziale X3DH.

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

► Il messaggio iniziale X3DH è aggiunto a ogni messaggio di apertura di

▶ I dispositivi comunicano solo con Double Ratchet. [21], [14]

SIGNAL

Signal Protocol

Signal Protocol Il protocollo

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

Signal Protocol

Il protocollo: Sesame

► Ricevuto il messaggio di conferma di apertura della sessione il mittente smette ► I dispositivi comunicano solo con Double Ratchet. [21], [14]

Difetti di progettazione

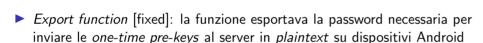
Frosch analysis [22]

dell'Applicazione

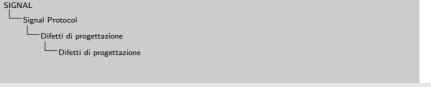
Protocollo Signal

4 Signal

Difetti di progettazione



► Vulnerabilità a UKS - Unknown kev-share attack



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

I difetti di progettazione 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 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.



SIGNAL

Signal Protocol

Difetti di progettazione

Difetti di progettazione

2 Applicazione

Difetti di Signal VS WhatsApp

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 4 Signal

Il paper [23] è il primo studio scientifico a riportare un'analisi formale dell'interazione tra X3DH e Double Ratchet.

Difetti di progettazione

Cohn-Gordon analysis [23]

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

36



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

dell'Applicazione oracoli che restituiscono un output simile a un output casuale. 3 Crittografia Applicazioni

Il paper [23] è il primo studio scientifico a riportare un'analisi formale dell'interazione tra X3DH e Double Ratchet.

SIGNAL

36

Signal Protocol

Difetti di progettazione

Difetti di progettazione

Difetti di progettazione

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

Cohn-Gordon analysis [23]

Definiamo questa condizione come random oracle model.

4 Signal

2 Applicazione

Protocol Difetti di

Signal VS WhatsApp

Difetti di progettazione Cohn-Gordon analysis [23]

Difetti di

2 Applicazione dell'Applicazione L'attacco UKS individuato in [22] non è valido in questo modello perché esso, come L'Applicazione e i Protocollo Signal

in effetti anche il protocollo Signal, non differenzia gli identificatori di sessione (i.e. 3 Crittografia l'ID della sessione Alice-Bob è lo stesso ID della sessione Alice-Charlie).

4 Signal

SIGNAL

Signal Protocol

Difetti di progettazione Difetti di progettazione

UKS è un attacco prevenibile a livello di applicazione (introducendo degli identificativi per gli utenti, e.g., il numero di telefono). N.B. Gli attacchi possono variare a seconda dell'implementazione fornita del protocollo, ma il protocollo in sé non presenta difetti rilevanti.

Difetti di progettazione

Cohn-Gordon analysis [23]

Difetti di progettazione Cohn-Gordon analysis [23]







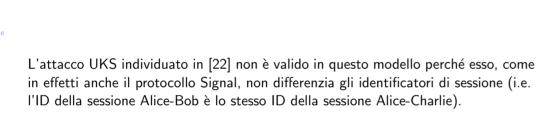
2 Applicazione

dell'Applicazione

L'Applicazione e i Protocollo Signal 3 Crittografia

4 Signal Difetti di

di debolezza nel protocollo.



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



SIGNAL

Signal Protocol

Difetti di progettazione Difetti di progettazione

UKS è un attacco prevenibile a livello di applicazione (introducendo degli identificativi per gli utenti, e.g., il numero di telefono). N.B. Gli attacchi possono variare a seconda dell'implementazione fornita del protocollo, ma il protocollo in sé non presenta difetti rilevanti.

Difetti di progettazione

Non sono stati individuati altri rilevanti difetti di progettazione che generino punt

Cohn-Gordon analysis [23]

2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

Applicazioni

4 Signal

II protocollo Difetti di

Signal VS WhatsApp VS Telegram

Pro

- ► Team indipendente no profit: non vende dati utente per scopi di marketing
- Open-source
- ► Interfaccia personalizzabile
- Crittografia end-to-end (anche sui metadati)
- ► Implementa il protocollo Signal

► Limite dimensioni file a 100MB



SIGNAL



Signal VS WhatsApp VS Telegram

2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

Applicazioni

4 Signal

Protocol

Difetti di

Signal VS WhatsApp

VS Telegram

Pro

- ► Team indipendente no profit: non vende dati utente per scopi di marketing
- Open-source
- ► Interfaccia personalizzabile
- Crittografia end-to-end (anche sui metadati)
- ► Implementa il protocollo Signal

Contro

► Limite dimensioni file a 100MB



Signal VS WhatsApp VS Telegram Signal VS WhatsApp VS Telegram Limite dimensioni file a 100MB Informazioni raccolte: numero di telefono

► Team indipendente no profit: non vende dati utente per scopi di marketine ► Onen-source ► Interfaccia personalizzabile ► Crittografia end.to.end (anche sui metadati) Implementa il protocollo Signal

Signal VS WhatsApp VS Telegram

SIGNAL

Signal Protocol

Sono in via di sviluppo nuove versioni dell'applicazione che non lo richiedano.

2 Applicazione Signal

dell'Applicazione

4 Signal

Difetti di progettazione Signal VS WhatsApp VS Telegram

L'applicazione Signal implementa il protocollo omonimo basandosi sulle librerie open-source: GitHub - Signal App

- Cryptographic functions laver
- Protocol library layer
- Service laver

Signal Protocol Signal VS WhatsApp VS Telegram Signal VS WhatsApp VS Telegram

onen-source: GitHub - Signal Ann

Signal VS WhatsApp VS Telegram

Dal livello più basso al più alto:

- Cryptographic functions layer: implementazione delle funzioni crittografiche
- Protocol library layer: usa le funzioni del livello crittografico per implementare il protocollo Service laver: combina le funzioni del livello protocollo per consentire di intraprendere effettivamente le conversazioni

SIGNAL

VERSIONE DESKTOP: All'installazione l'applicazione desktop genera una coppia di chiavi: la chiave pubblica viene presentata come QR code da scannerizzare con l'applicazione mobile. Lo smartphone crittografa l'identity key con la chiave pubblica del client desktop e la comunica al server Signal. Da questo momento l'applicazione desktop può essere usata anche se quella mobile non è in funzione.

[14]

2 Applicazione Signal

dell'Applicazione

3 Crittografia

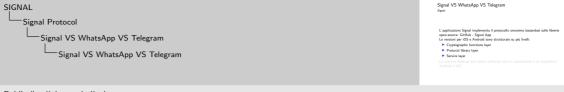
4 Signal

Difetti di progettazione Signal VS WhatsApp

VS Telegram

L'applicazione Signal implementa il protocollo omonimo basandosi sulle librerie open-source: GitHub - Signal App

- Le versioni per iOS e Android sono strutturate su più livelli:
- Cryptographic functions laver
- Protocol library layer
- Service laver



Dal livello più basso al più alto:

- Cryptographic functions layer: implementazione delle funzioni crittografiche
- Protocol library layer: usa le funzioni del livello crittografico per implementare il protocollo
- Service laver: combina le funzioni del livello protocollo per consentire di intraprendere effettivamente le conversazioni

VERSIONE DESKTOP: All'installazione l'applicazione desktop genera una coppia di chiavi: la chiave pubblica viene presentata come QR code da scannerizzare con l'applicazione mobile. Lo smartphone crittografa l'identity key con la chiave pubblica del client desktop e la comunica al server Signal. Da questo momento l'applicazione desktop può essere usata anche se quella mobile non è in funzione.

[14]

2 Applicazione Signal

dell'Applicazione

Protocollo Signal 3 Crittografia

4 Signal

Difetti di

Signal VS WhatsApp VS Telegram

L'applicazione Signal implementa il protocollo omonimo basandosi sulle librerie open-source: GitHub - Signal App

Le versioni per iOS e Android sono strutturate su più livelli:

- Cryptographic functions laver
- Protocol library layer
- Service laver

La versione desktop può essere utilizzata solo in associazione a un dispositivo Android o iOS.

SIGNAL Signal Protocol Signal VS WhatsApp VS Telegram Signal VS WhatsApp VS Telegram Dal livello più basso al più alto: • Cryptographic functions layer: implementazione delle funzioni crittografiche

L'applicazione Signal implementa il protocollo omonimo basandosi sulle libreri

onen-source: GitHub - Signal Ann Le versioni per iOS e Android sono strutturate su più livelli Cryptographic functions laver

Protocol library lawn

Signal VS WhatsApp VS Telegram

La versione desktop può essere utilizzata solo in associazione a un dispositivo Android o iOS.

- Protocol library layer: usa le funzioni del livello crittografico per implementare il protocollo
- Service laver: combina le funzioni del livello protocollo per consentire di intraprendere effettivamente le conversazioni

VERSIONE DESKTOP: All'installazione l'applicazione desktop genera una coppia di chiavi: la chiave pubblica viene presentata come QR code da scannerizzare con l'applicazione mobile. Lo smartphone crittografa l'identity key con la chiave pubblica del client desktop e la comunica al server Signal. Da questo momento l'applicazione desktop può essere usata anche se quella mobile non è in funzione.

[14]

Signal VS WhatsApp VS Telegram WhatsApp

2 Applicazione

dell'Applicazione

3 Crittografia

4 Signal

Difetti di Signal VS WhatsApp

VS Telegram

► Interfaccia parzialmente personalizzabile

2 miliardi di utenti attivi

Supporta autenticazione a due fattori

Pro

- Poche impostazioni sulla privacy

Raccolta dati utente per fini di marketing

▶ Backup basati su cloud non crittografati, metadati non crittografati

Crittografia end-to-end per chat, video, gruppi, chiamate, fotografie

► Implementa il protocollo Signal (l'implementazione in sé è closed-source)

Signal Protocol ► Crittografia end-to-end per chat, video, gruppi, chiamate, fotografie Signal VS WhatsApp VS Telegram ► 2 miliardi di utenti attivi Supporta autenticazione a due fattori Signal VS WhatsApp VS Telegram

Signal VS WhatsApp VS Telegram

Informazioni raccolte: numero di telefono, posizione, contatti, abitudini, cronologia di navigazione, cronologia acquisti, dati pubblicitari, ID utente e dispositivo, indirizzo e-mail, informazioni di pagamento, dati sulle prestazioni e altri contenuti utente

Recente (2019) problema di WhatsApp ha coinvolto numerose chat di gruppo i cui link erano disponibili tramite ricerca Google [bug eliminato a febbraio 2020]

SIGNAL

Signal VS WhatsApp VS Telegram WhatsApp

2 Applicazione

dell'Applicazione

Protocollo Signal

3 Crittografia

4 Signal

Difetti di Signal VS WhatsApp VS Telegram

5 Bibliografia

Pro

- Crittografia end-to-end per chat, video, gruppi, chiamate, fotografie
- ▶ Implementa il protocollo Signal (l'implementazione in sé è closed-source)
- ► Interfaccia parzialmente personalizzabile
- 2 miliardi di utenti attivi
- Supporta autenticazione a due fattori

Contro

- ► Poche impostazioni sulla privacy
- ► Raccolta dati utente per fini di marketing
- ▶ Backup basati su cloud non crittografati, metadati non crittografati

Signal Protocol ► Crittografia end-to-end per chat, video, gruppi, chiamate, fotografie Signal VS WhatsApp VS Telegram ► 2 miliardi di utenti attivi Signal VS WhatsApp VS Telegram Supporta autenticazione a due fattori Poche impostazioni sulla privacy Raccolta dati utente per fini di marketing ► Backun hasati su cloud non crittografati, metadati non crittografat Informazioni raccolte: numero di telefono, posizione, contatti, abitudini, cronologia di navigazione, cronologia acquisti, dati pubblicitari, ID utente e

Signal VS WhatsApp VS Telegram

dispositivo, indirizzo e-mail, informazioni di pagamento, dati sulle prestazioni e altri contenuti utente Recente (2019) problema di WhatsApp ha coinvolto numerose chat di gruppo i cui link erano disponibili tramite ricerca Google [bug eliminato a febbraio

SIGNAL

2020]

Signal VS WhatsApp VS Telegram WhatsApp

2 Applicazione

dell'Applicazione L'Applicazione e i Protocollo Signal

4 Signal

Difetti di progettazione Signal VS WhatsApp

VS Telegram

WhatsApp implementa il protocollo Signal basandosi sulle librerie open-source: GitHub - WhatsApp

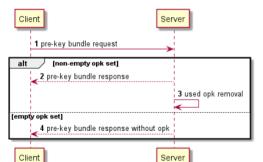


Figure Whats Annininializations assigns (singula dispositiva)

Signal Protocol WhatsApp implementa il protocollo Signal basandosi sulle librerie open-source Signal VS WhatsApp VS Telegram all / Journally sales Signal VS WhatsApp VS Telegram

Signal VS WhatsApp VS Telegram

SIGNAL

Signal VS WhatsApp VS Telegram WhatsApp

Client

2 Applicazione

dell'Applicazione L'Applicazione e i Protocollo Signal

4 Signal

Difetti di progettazione Signal VS WhatsApp

VS Telegram

WhatsApp implementa il protocollo Signal basandosi sulle librerie open-source: GitHub - WhatsApp

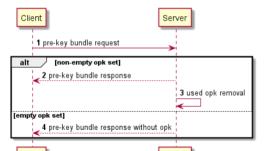


Figure: WhatsApp inizializzazione sessione (singolo dispositivo)

Server



Signal VS WhatsApp VS Telegram Telegram

Pro

2 Applicazione Signal

dell'Applicazione

Protocollo Signal

3 Crittografia

4 Signal

Difetti di

Signal VS WhatsApp VS Telegram

- Sicurezza: autenticazione a due fattori
- Supporta file di qualsiasi dimensione
- Eliminazione automatica dell'account se inutilizzato per troppo tempo
- ► Interfaccia personalizzabile

- Crittografia end-to-end solo per chat segrete, non per chat individuali e di
- ► Chat cloud che utilizzano la crittografia client-server: l'azienda ha accesso ai

► Usa GPS per trovare utenti nelle vicinanze



SIGNAL

 Eliminazione automatica dell'account se inutilizzato per troppo tempo Interfaccia personalizzabile

Signal VS WhatsApp VS Telegram

Messaggi crittografati sul dispositivo utente ma decrittati sui server, ri-crittografati e poi inviati al destinatario per essere decrittati in modo definitivo

Telegram possiede le chiavi lato server e può teoricamente accedere al contenuto dei messaggi.

Telegram garantisce di non aver condiviso ad oggi alcun dato con terze parti e/o enti governativi.

Signal VS WhatsApp VS Telegram Telegram

Pro

2 Applicazione Signal

dell'Applicazione

Protocollo Signal

3 Crittografia

4 Signal

Difetti di

progettazione Signal VS WhatsApp VS Telegram

- Sicurezza: autenticazione a due fattori
- Supporta file di qualsiasi dimensione
- Eliminazione automatica dell'account se inutilizzato per troppo tempo
- ► Interfaccia personalizzabile

- Contro
 - ► Crittografia end-to-end solo per chat segrete, non per chat individuali e di
 - gruppo ▶ Chat cloud che utilizzano la crittografia client-server: l'azienda ha accesso ai
 - messaggi

► Usa GPS per trovare utenti nelle vicinanze



SIGNAL

Signal Protocol

Signal VS WhatsApp VS Telegram ► Eliminazione automatica dell'account se inutilizzato per troppo tempo Interfaccia personalizzabile Signal VS WhatsApp VS Telegram ► Crittografia end-to-end solo per chat segrete, non per chat individuali e d ► Chat cloud che utilizzano la crittografia client-server: l'azienda ha accesso a ► Usa GPS ner trouare utenti nelle vicinanze Informazioni raccolte: indirizzo IP, dispositivi, cronologia dei nomi utente e contatti.

Signal VS WhatsApp VS Telegram

Messaggi crittografati sul dispositivo utente ma decrittati sui server, ri-crittografati e poi inviati al destinatario per essere decrittati in modo definitivo

Telegram possiede le chiavi lato server e può teoricamente accedere al contenuto dei messaggi.

Telegram garantisce di non aver condiviso ad oggi alcun dato con terze parti e/o enti governativi.

Telegram

Mentre Signal e WhatsApp utilizzano implementazioni del protocollo Signal,

Telegram utilizza il protocollo proprietario MTProto per la crittografia dei

Signal VS WhatsApp VS Telegram

Mentre Signal e WhatsApp utilizzano implementazioni del protocollo Signal

Telegram utilizza il protocollo proprietario MTProto per la crittografia dei

SIGNAL

43

Signal Protocol

da team più ampi e numerosi.

Signal VS WhatsApp VS Telegram

Signal VS WhatsApp VS Telegram

In ambito crittografico è considerata buona norma utilizzare protocolli e algoritmi verificati da un numero di ricercatori o esperti maggiore possibile. Ciò si contrappone alla logica di security through obscurity che invece vorrebbe che i protocolli siano tanto più sicuri quanto meno sono stati analizzati Per questo motivo protocolli open-source sono in genere preferibili, in quanto è più probabile che vengano rilevati eventuali bug in protocolli analizzati

dell'Applicazione

3 Crittografia

messaggi.

Difetti di

4 Signal







L'Applicazione e i Protocollo Signal

Signal VS WhatsApp VS Telegram Telegram

dell'Applicazione

L'Applicazione e i Protocollo Signal

4 Signal

VS Telegram

Difetti di Signal VS WhatsApp





Mentre Signal e WhatsApp utilizzano implementazioni del protocollo Signal,

messaggi. Essendo a implementazione closed-source non permette l'analisi completa da parte

dei ricercatori.

Telegram utilizza il protocollo proprietario MTProto per la crittografia dei

43

da team più ampi e numerosi.

SIGNAL

Signal Protoco Signal VS WhatsApp VS Telegram Signal VS WhatsApp VS Telegram

Mentre Signal e WhatsApp utilizzano implementazioni del protocollo Signal Telegram utilizza il protocollo proprietario MTProto per la crittografia dei In ambito crittografico è considerata buona norma utilizzare protocolli e algoritmi verificati da un numero di ricercatori o esperti maggiore possibile.

Signal VS WhatsApp VS Telegram

Ciò si contrappone alla logica di security through obscurity che invece vorrebbe che i protocolli siano tanto più sicuri quanto meno sono stati analizzati

Per questo motivo protocolli open-source sono in genere preferibili, in quanto è più probabile che vengano rilevati eventuali bug in protocolli analizzati





MTProto, part I

Telegram

dell'Applicazione

4 Signal

Difetti di

progettazione Signal VS WhatsApp

VS Telegram

NB: after decryption, msg, key must be equal to SHA-1 of data thus obtained

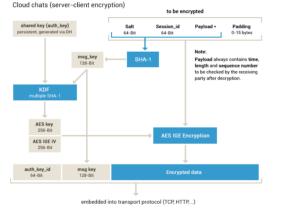


Figure: MTProto



Il salt, session_id e pavload del messaggio vengono crittografati con SHA-1 a creare una msg_kev . La msg_key viene usata insieme alla auth_key come input di una KDF che restituisce una chiave AES e un vettore di inizializzazione da utilizzare a

loro volta come input di una funzione AES IGE Encryption. Da quest'ultima funzione si ottengono i dati crittografati, ai quali vengono aggiunti auth_kev_id al fine di identificare l'utente e msg_kev.

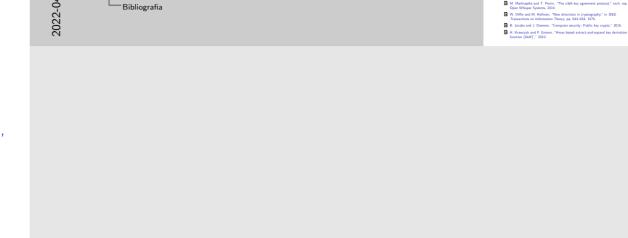
Al fine di autenticare il messaggio, una volta decodificato viene comparata la msg_kev ricevuta con quella computata localmente.[24]



Bibliografia I

SIGNAL Bibliografia II - Bibliografia K. Prodeen: "Snowden's email remoder loses anneal over encryption level Bibliografia II B. Gellman and J. Markon, "Edward snowden says motive behind leaks was t expose 'surveillance state'." The Washington Post, June 10, 2013 — Bibliografia R. Sinzel. "Encrypted e-mail company hushmail spills to feds." 2007 R C. M. East, N. A. Program, and C. T. Program, "Why telegram's securitflaws may not iran's inomalists at risk - committee to notest inormalists "Cryptography concepts - fundamentals - e3kit — virgil security," 2020. R. Lutkevich and M. Bacon, "end-to-end encountion (e2ee)." June 2021 K. Poulsen, "Snowden's email provider loses appeal over encryption keys," 2014, April 16. 2 Applicazione B. Gellman and J. Markon, "Edward snowden says motive behind leaks was to dell'Applicazione expose 'surveillance state'." The Washington Post, June 10, 2013. 3 Crittografia R. Singel, "Encrypted e-mail company hushmail spills to feds," 2007, Applicazioni November 7. 4 Signal C. M. East, N. A. Program, and C. T. Program, "Why telegram's security Protocol flaws may put iran's journalists at risk - committee to protect journalists." Difetti di 2016, May 1. Signal VS WhatsApp "Cryptography concepts - fundamentals - e3kit — virgil security," 2020. 5 Bibliografia B. Lutkevich and M. Bacon, "end-to-end encryption (e2ee)," June 2021.

Bibliografia III "Signal documentation," 2 Applicazione D. Van Dam, "Analysing the signal protocol - a manual and automated dell'Applicazione analysis of the signal protocol," Master's thesis, Radboud University, 2019. M. Marlinspike and T. Perrin, "The x3dh key agreement protocol," tech. rep., 3 Crittografia Open Whisper Systems, 2016. W. Diffie and M. Hellman, "New directions in cryptography," in IEEE 4 Signal Protocol Transactions on Information Theory, pp. 644–654, 1976. B. Jacobs and J. Daemen, "Computer security: Public key crypto," 2016. Difetti di progettazione Signal VS WhatsApp H. Krawczyk and P. Eronen, "Hmac-based extract-and-expand key derivation 5 Bibliografia function (hkdf)'," 2010.



Bibliografia III

"Signal documentation."

D. Van Dam, "Analysing the signal protocol - a manual and automated analysis of the signal protocol." Master's thesis. Radboud University. 2019.

47

SIGNAL

- Bibliografia

Bibliografia IV M. Marlinspike and T. Perrin, "The double ratchet algorithm," tech. rep., 2 Applicazione Open Whisper Systems, 2016. M. Pound, "Double ratchet messaging encryption - computerphile." Video. dell'Applicazione Protocollo Signal M. Marlinspike and T. Perrin, "The sesame algorithm: Session management for asynchronous message encryption." tech. rep., Open Whisper Systems, 2017. Г. Frosch, С. Mainka, С. Bader, F. Bergsma, J. Schwenk, and Т. Holz, "How secure is textsecure?." in 2016 IEEE European Symposium on Security and Privacy (EuroS P), pp. 457–472, 2016. K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, "A Signal VS WhatsApp 5 Bibliografia formal security analysis of the signal messaging protocol," in 2017 IEEE

Applicazioni

4 Signal

Difetti di

VS Telegram



Bibliografia IV

Onen Whisner Systems 2016

M. Marlinovike and T. Perrin. "The double ratchet algorithm." tech. rep.

M. Pound. "Double ratchet messaging encryption - computerphile." Video M. Marlinsnike and T. Perrin. "The sesame algorithm: Session management for

SIGNAL

- Bibliografia

Bibliografia V

2 Applicazione Signal Telegram.org, "Mtproto mobile protocol. core.,"



Applicazioni

4 Signal Protocol

Proprietà

Difetti di progettazione Signal VS WhatsApp VS Telegram 5 Bibliografia

SIGNAL

2022-04-26

-Bibliografia

Bibliografia





Bibliografia V

Telegram.org, "Mtproto mobile protocol. core.,"

