

Protocollo Signal

Elena Tonini, Matr.727382

Università degli Studi di Brescia

A.A. 2021/2022

2022-04-21

SIGNAL

Protocollo Signal

Elena Tonini, Matr.727382

Università degli Studi di Brescia

A.A. 2021/2022

Sommario I

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

5 Bibliografia

1. Sommario

2. Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

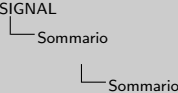
3. Crittografia End-to-End

Applicazioni
Problematiche

4. Signal Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal

2022-04-21



Sommario I
1. Sommario
2. Applicazione Signal
Storia dell'Applicazione
L'Applicazione e il Protocollo Signal
3. Crittografia End-to-End
Applicazioni
Problematiche
4. Signal Protocol
Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal

Sommario II

WhatsApp VS Signal VS Telegram

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

5 Bibliografia

5. Bibliografia

2022-04-21

SIGNAL

Sommario

Sommario

Sommario II

WhatsApp VS Signal VS Telegram

5. Bibliografia

Applicazione Signal

- 1 Sommario
- 2 Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3 Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4 Signal Protocol
 - Storia
 - Vulnerabilità
 - Attacchi possibili
 - Considerazioni
 - WhatsApp VS Signal
 - Telegram VS Signal
 - WhatsApp VS Signal VS Telegram
- 5 Bibliografia

Storia dell'Applicazione

L'applicazione Signal ha origine dall'unione dei due servizi di messaggistica **TextSecure** e **RedPhone**, sviluppati da **Moxie Marlinspike** e **Stuart Anderson**, che insieme fondarono la start-up **Whisper Systems** nel 2010.

Entrambe le applicazioni implementavano la crittografia end-to-end.



Applicazione Signal

Storia dell'Applicazione

L'applicazione Signal ha origine dall'unione dei due servizi di messaggistica **TextSecure** e **RedPhone**, sviluppati da **Moxie Marlinspike** e **Stuart Anderson**, che insieme fondarono la start-up **Whisper Systems** nel 2010.

Entrambe le applicazioni implementavano la crittografia end-to-end.

Applicazione Signal

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni

Problematiche

4 Signal Protocol

Storia

Vulnerabilità

Attacchi possibili

Considerazioni

WhatsApp VS Signal

Telegram VS Signal

WhatsApp VS Signal
VS Telegram

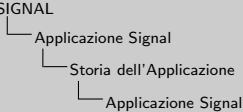
5 Bibliografia

Storia dell'Applicazione

L'applicazione Signal ha origine dall'unione dei due servizi di messaggistica **TextSecure** e **RedPhone**, sviluppati da **Moxie Marlinspike** e **Stuart Anderson**, che insieme fondarono la start-up **Whisper Systems** nel 2010.

Entrambe le applicazioni implementavano la crittografia end-to-end.

2022-04-21



Applicazione Signal

Storia dell'Applicazione

L'applicazione Signal ha origine dall'unione dei due servizi di messaggistica **TextSecure** e **RedPhone**, sviluppati da **Moxie Marlinspike** e **Stuart Anderson**, che insieme fondarono la start-up **Whisper Systems** nel 2010.

Entrambe le applicazioni implementavano la crittografia end-to-end.

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione

L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni

Problematiche

4 Signal Protocol

Storia

Vulnerabilità

Attacchi possibili

Considerazioni

WhatsApp VS Signal

Telegram VS Signal

WhatsApp VS Signal

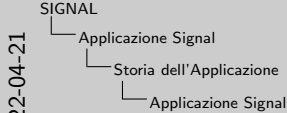
VS Telegram

5 Bibliografia

Applicazione Signal

A seguito del nuovo rilascio delle applicazioni nel 2011 i due servizi assumono la propria natura **open-source** che ancora oggi caratterizza l'applicazione Signal.

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



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

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

Applicazione Signal

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

Applicazione Signal

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

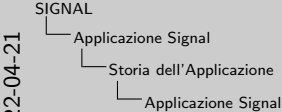
4 Signal Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

5 Bibliografia

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



2022-04-21

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

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

Applicazione Signal

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

Applicazione Signal

1 Sommario

2 Applicazione Signal

3 Crittografia End-to-End

4 Signal Protocol

5 Bibliografia

Storia dell'Applicazione

L'Applicazione e il Protocollo Signal

Applicazioni

Problematiche

Storia

Vulnerabilità

Attacchi possibili

Considerazioni

WhatsApp VS Signal

Telegram VS Signal

WhatsApp VS Signal VS Telegram

Nel febbraio 2018 Marlinspike e il co-fondatore di WhatsApp Brian Acton fondarono la **Signal Foundation**, il cui obiettivo è il supporto e l'accelerazione della diffusione della comunicazione privata e sicura. [Lumer]



Applicazione Signal

Nel febbraio 2018 Marlinspike e il co-fondatore di WhatsApp Brian Acton fondarono la **Signal Foundation**, il cui obiettivo è il supporto e l'accelerazione della diffusione della comunicazione privata e sicura. [Lumer]

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

5 Bibliografia

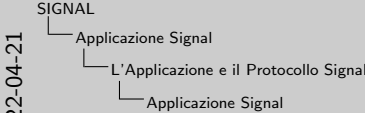
Applicazione Signal

L'Applicazione e il Protocollo Signal

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

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

Ogni piattaforma di messaggistica che intraprese collaborazioni con OWS al fine di integrare il protocollo Signal al proprio interno lo implementò in modalità differenti e su scala/estensione diversa.



2022-04-21

Applicazione Signal

L'Applicazione e il Protocollo Signal

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

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

Ogni piattaforma di messaggistica che intraprese collaborazioni con OWS al fine di integrare il protocollo Signal al proprio interno lo implementò in modalità differenti e su scala/estensione diversa.

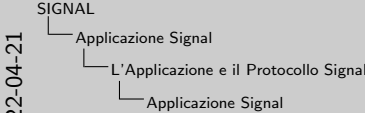
Applicazione Signal

L'Applicazione e il Protocollo Signal

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

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

Ogni piattaforma di messaggistica che intraprese collaborazioni con OWS al fine di integrare il protocollo Signal al proprio interno lo implementò in modalità differenti e su scala/estensione diversa.



2022-04-21

L'Applicazione e il Protocollo Signal

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

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

Ogni piattaforma di messaggistica che intraprese collaborazioni con OWS al fine di integrare il protocollo Signal al proprio interno lo implementò in modalità differenti e su scala/estensione diversa.

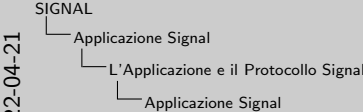
Applicazione Signal

L'Applicazione e il Protocollo Signal

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

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

Ogni piattaforma di messaggistica che intraprese collaborazioni con OWS al fine di integrare il protocollo Signal al proprio interno lo implementò in modalità differenti e su scala/estensione diversa.



2022-04-21

L'Applicazione e il Protocollo Signal

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

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

Ogni piattaforma di messaggistica che intraprese collaborazioni con OWS al fine di integrare il protocollo Signal al proprio interno lo implementò in modalità differenti e su scala/estensione diversa.

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

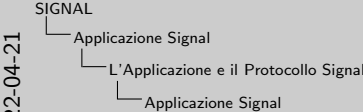
5 Bibliografia

Applicazione Signal

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

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

[Gre29], [Lumer]



- 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 più note implementazioni (parziali) del Protocollo Signal troviamo:

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

[Gre29], [Lumer]

1 Sommario

2 Applicazione Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

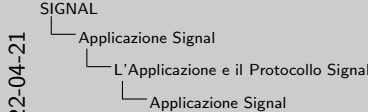
5 Bibliografia

Applicazione Signal

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

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

[Gre29], [Lumer]



- 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 più note implementazioni (parziali) del Protocollo Signal troviamo:

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

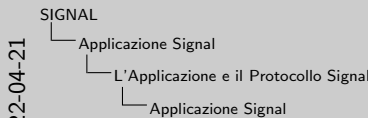
[Gre29], [Lumer]

Applicazione Signal

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

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

[Gre29], [Lumer]



- 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 più note implementazioni (parziali) del Protocollo Signal troviamo:

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

[Gre29], [Lumer]

1	Sommario
2	Applicazione Signal
3	Crittografia End-to-End
4	Signal Protocol
5	Bibliografia

Storia dell'Applicazione

L'Applicazione e il Protocollo Signal

Applicazioni

Problematiche

Storia

Vulnerabilità

Attacchi possibili

Considerazioni

WhatsApp VS Signal

Telegram VS Signal

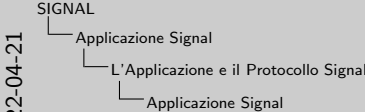
WhatsApp VS Signal VS Telegram

Applicazione Signal

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

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

[Gre29], [Lumer]



- 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 più note implementazioni (parziali) del Protocollo Signal troviamo:

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

WhatsApp: tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[Gre29], [Lumer]

Applicazione Signal



Applicazione Signal

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

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

► *WhatsApp*: tra le maggiori applicazioni che implementano Signal è l'unica che garantisce di default la crittografia end-to-end delle conversazioni (da aprile 2016)

[Gre29] [Lumer]

- 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

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

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

[Gre29], [Lumer]

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal VS Telegram

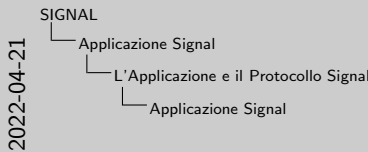
5 Bibliografia

Applicazione Signal

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

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

[Gre29], [Lumer]



- 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 più note implementazioni (parziali) del Protocollo Signal troviamo:

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

[Gre29], [Lumer]

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

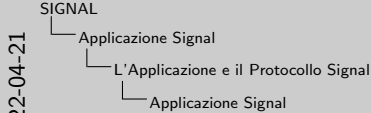
Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

5 Bibliografia

Applicazione Signal

Ciascuna di queste *features* richiede che le conversazioni intraprese siano dichiarate “private” affinché sia possibile applicare la crittografia end-to-end su tutto il contenuto che viene scambiato

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



2022-04-21

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

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

Applicazione Signal

Ciascuna di queste *features* richiede che le conversazioni intraprese siano dichiarate “private” affinché sia possibile applicare la crittografia end-to-end su tutto il contenuto che viene scambiato

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

Applicazione Signal

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

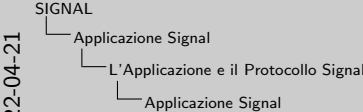
4 Signal Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

5 Bibliografia

Ciascuna di queste *features* richiede che le conversazioni intraprese siano dichiarate “private” affinché sia possibile applicare la crittografia end-to-end su tutto il contenuto che viene scambiato

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



2022-04-21

Applicazione Signal

Ciascuna di queste *features* richiede che le conversazioni intraprese siano dichiarate “private” affinché sia possibile applicare la crittografia end-to-end su tutto il contenuto che viene scambiato

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

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

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

Applicazione Signal

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal VS Telegram

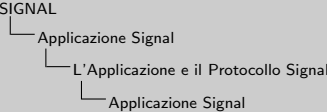
5 Bibliografia

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

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

[Lumer]

2022-04-21



Applicazione Signal

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

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

[Lumer]

Applicazione Signal

1 Sommario

2 Applicazione Signal

Storia dell'Applicazione
L'Applicazione e il Protocollo Signal

3 Crittografia End-to-End

Applicazioni
Problematiche

4 Signal Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

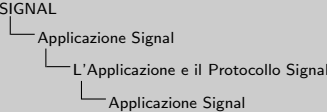
5 Bibliografia

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

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

[Lumer]

2022-04-21



Applicazione Signal

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

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

[Lumer]

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

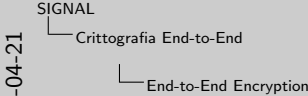
5 Bibliografia

End-to-End Encryption

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. [Gre29]



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

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

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

End-to-End Encryption

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. [Gre29]

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

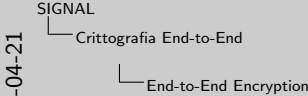
5 Bibliografia

End-to-End Encryption

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. [Gre29]



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

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

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

End-to-End Encryption

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. [Gre29]

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

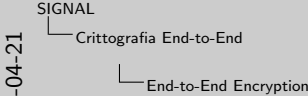
5 Bibliografia

End-to-End Encryption

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. [Gre29]



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

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

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

End-to-End Encryption

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. [Gre29]

2022-04-21

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

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

[int20]

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

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

[int20]

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.

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

5 Bibliografia

1 Sommario

2 Applicazione
Signal

Storia
dell'Applicazione
L'Applicazione e il
Protocollo Signal

3 Crittografia
End-to-End

Applicazioni
Problematiche

4 Signal
Protocol

Storia
Vulnerabilità
Attacchi possibili
Considerazioni
WhatsApp VS Signal
Telegram VS Signal
WhatsApp VS Signal
VS Telegram

5 Bibliografia

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

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

[int20]

2022-04-21

SIGNAL
Crittografia End-to-End

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.

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

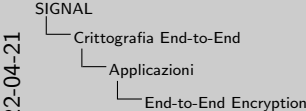
Per molti sistemi di messaggistica i messaggi passano attraverso un intermediario che li conserva finché non vengono recuperati dal destinatario. Anche se protetti da crittografia, essi lo sono solamente in transito, quindi possono essere letti dai provider di servizi.

[int20]

End-to-End Encryption

Applicazioni

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



La protezione dei dati tramite *encryption in transit* consiste nel cifrare i dati solo lungo il percorso su cui vengono trasmessi ma non alla sorgente. In queste condizioni, colui che invia i dati ha accesso al loro contenuto, cosa che si vuole spesso evitare.

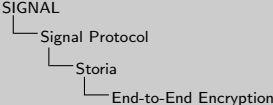
- **Comunicazioni sicure:** applicazioni di messaggistica e posta elettronica per mantenere private le conversazioni degli utenti;
- **Gestione password:** in questo caso a entrambi gli endpoint della comunicazione si trova lo stesso utente, che è l'unica persona munita di chiave;
- **Data storage:**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

End-to-End Encryption

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:** se non volute, possono essere introdotte tramite attacchi cyber e poi sfruttate per violare la sicurezza del sistema

2022-04-21




Contrariamente alle due politiche *Security by Design* e *Open security* la sicurezza tramite offuscazione è fortemente sconsigliata, in quanto affida la sicurezza del sistema al fatto che nessuno riesca a comprenderlo. Questa pratica rende quindi il sistema vulnerabile a qualsiasi attacco di tipo reverse engeneering, oltre che a possibili fughe di informazioni. L'utilizzo di ideologie “open” permette la validazione del sistema da parte di un maggior numero di enti e di membri di una comunità, permettendo così l'individuazione di falle in minor tempo.

Il metodo più efficiente, però, consiste sempre nell'utilizzo di sistemi già esistenti e ritenuti sicuri (p.e. tritium)


- ▶ **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:** se non volute, possono essere introdotte tramite attacchi cyber e poi sfruttate per violare la sicurezza del sistema

- 1 Sommario
- 2 Applicazione Signal
 - Storia dell'Applicazione
 - L'Applicazione e il Protocollo Signal
- 3 Crittografia End-to-End
 - Applicazioni
 - Problematiche
- 4 Signal Protocol
 - Storia
 - Vulnerabilità
 - Attacchi possibili
 - Considerazioni
 - WhatsApp VS Signal
 - Telegram VS Signal
 - WhatsApp VS Signal VS Telegram
- 5 Bibliografia


Bibliografia I




Andy Greenberg.
Hacker lexicon: What is the signal encryption protocol?
2020, November 29.



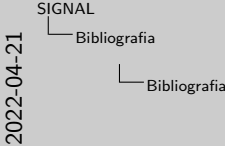
Cryptography concepts - fundamentals - e3kit — virgil security.
2020.



David J Lumb.
The story of signal.
Increment, (7), 2018, October.



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



Bibliografia I

**Andy Greenberg.**
Hacker lexicon: What is the signal encryption protocol?
2020, November 29.

**Cryptography concepts - fundamentals - e3kit — virgil security.**
2020.

**David J Lumb.**
The story of signal.
Increment, (7), 2018, October.

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