A Formal Security Analysis of the Signal Messaging Protocol

Luke Garratt
Computer Science
University of Oxford

Why what ☎ is doing is 👍

Luke Garratt
Computer Science
University of Oxford

Professors

Cas Cremers

Douglas Stebila

minions*

*PhD students

Katriel Cohn-Gordon

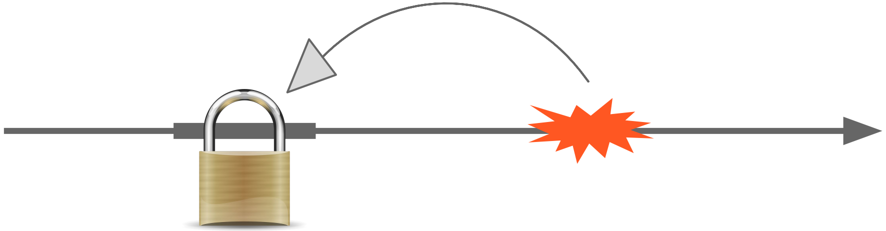
Luke Garratt

Ben Dowling

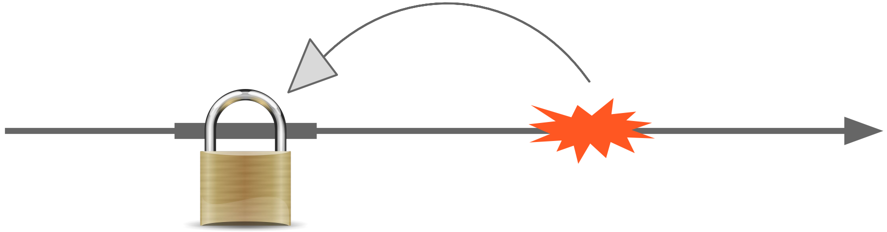
What *should* Signal achieve?

Does it?

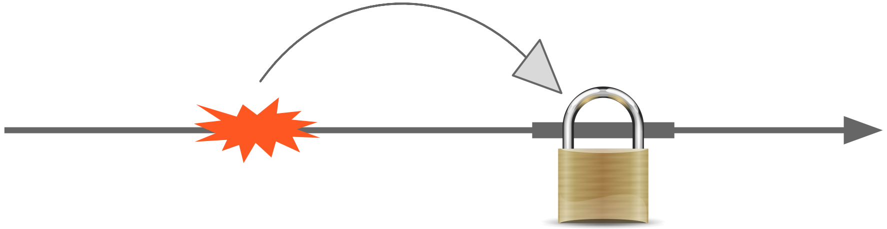
Forward secrecy:



Forward secrecy:



Post-compromise security:



Why is this useful?

Why is this useful?

Older protocols have ***no* forward secrecy.** (E.g. TLS-RSA)

- Adversary can store ciphertext traffic of target session, obtain long-term keys later and then decrypt.

Why is this useful?

Older protocols have _no_ forward secrecy. (E.g. TLS-RSA)

- Adversary can store ciphertext traffic of target session, obtain long-term keys later and then decrypt.

Newer protocols have forward secrecy. (E.g. TLS-DHE)

- Adversary must now obtain long-term keys first, wait for interesting target session and then launch a man-in-the-middle attack.

Why is this useful?

Older protocols have *no* forward secrecy. (E.g. TLS-RSA)

- Adversary can store ciphertext traffic of target session, obtain long-term keys later and then decrypt.

Newer protocols have forward secrecy. (E.g. TLS-DHE)

- Adversary must now obtain long-term keys first, wait for interesting target session and then launch a man-in-the-middle attack.

Fancy protocols have post-compromise security. (Signal?)

- Adversary must now obtain long-term keys and **immediately attack and keep on attacking** if it wants to compromise future targeted sessions.

[PCS, CSF '16]:
"Security guarantees even *after* your peer's key is compromised."

Our Signal security model

Adapted Bellare-Rogaway-style, multi-stage key exchange model.

[1] Bellare and Rogaway, “Entity Authentication and Key Distribution”.

[2] Fischlin and Günther, “Multi-Stage Key Exchange…”.

Our Signal security model

Our model captures:

- Adversary has full network control.

Our Signal security model

Our model captures:

- Adversary has full network control.
- Perfect forward secrecy.

Our Signal security model

Our model captures:

- Adversary has full network control.
- Perfect forward secrecy.
- Key compromise impersonation attacks.

Our Signal security model

Our model captures:

- Adversary has full network control.
- Perfect forward secrecy.
- Key compromise impersonation attacks.
- Some (but not all) random numbers can be compromised.

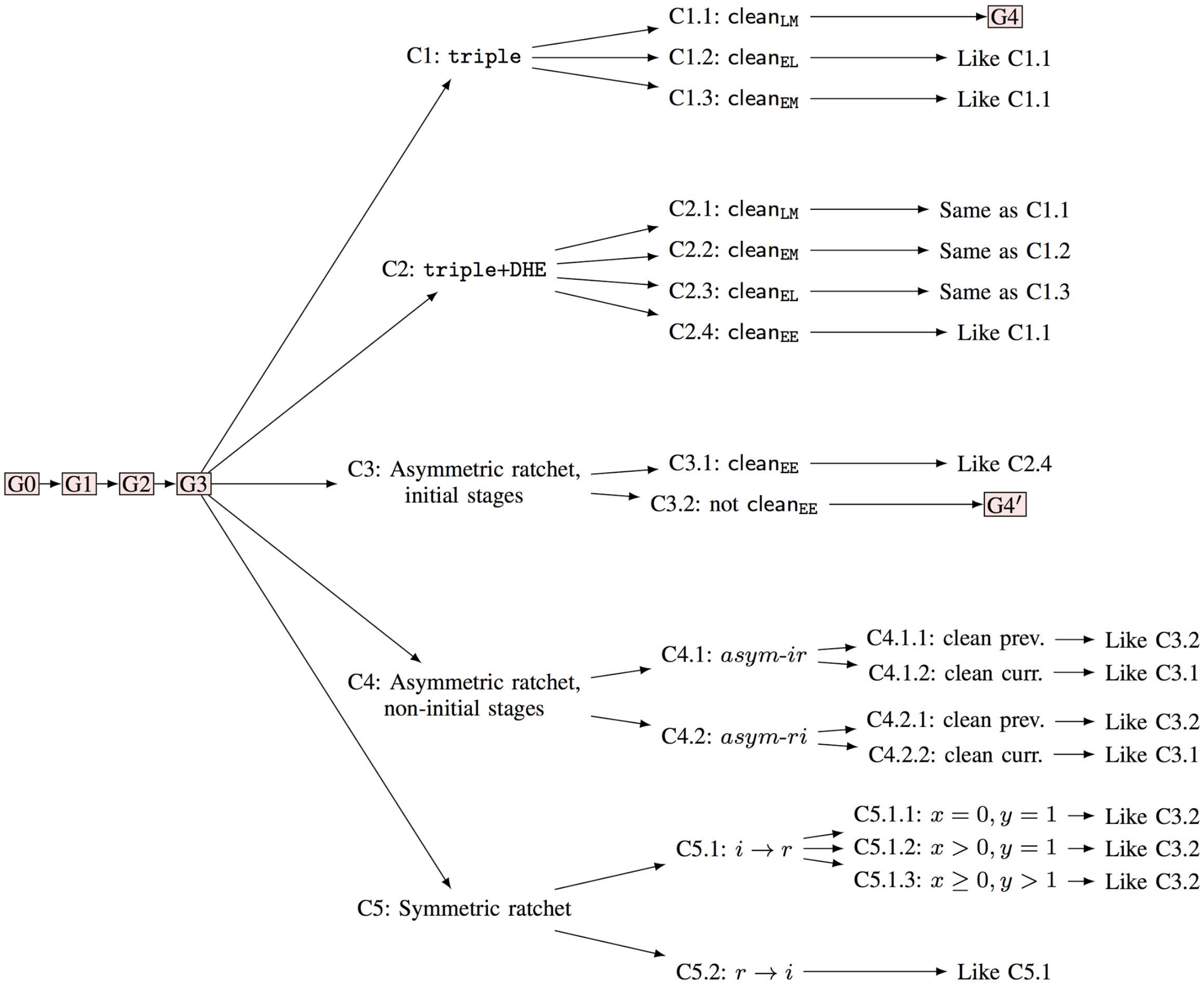
Our Signal security model

Our model captures:

- Adversary has full network control.
- Perfect forward secrecy.
- Key compromise impersonation attacks.
- Some (but not all) random numbers can be compromised.
- Post-compromise security.

Main result

Theorem. The Signal protocol is a secure multi-stage key exchange protocol in our model, under the GDH assumption and assuming all KDFs are random oracles.



G0 → G1 → G2 → G3

C1: triple

C1.1: $\mathsf{clean}_{\mathrm{LM}}$ → G4

C1.2: $\mathsf{clean}_{\mathrm{EL}}$ → Like C1.1

C1.3: $\mathsf{clean}_{\mathrm{EM}}$ → Like C1.1

C2: triple+DHE

C2.1: $\mathsf{clean}_{\mathrm{LM}}$ → Same as C1.1

C2.2: $\mathsf{clean}_{\mathrm{EM}}$ → Same as C1.2

C2.3: $\mathsf{clean}_{\mathrm{EL}}$ → Same as C1.3

C2.4: $\mathsf{clean}_{\mathrm{EE}}$ → Like C1.1

C3: Asymmetric ratchet, initial stages

C3.1: $\mathsf{clean}_{\mathrm{EE}}$ → Like C2.4

C3.2: not $\mathsf{clean}_{\mathrm{EE}}$ → G4′

C4: Asymmetric ratchet, non-initial stages

C4.1: $asym\text{-}ir$

C4.1.1: clean prev. → Like C3.2

C4.1.2: clean curr. → Like C3.1

C4.2: $asym\text{-}ri$

C4.2.1: clean prev. → Like C3.2

C4.2.2: clean curr. → Like C3.1

C5: Symmetric ratchet

C5.1: $i \to r$

C5.1.1: $x = 0, y = 1$ → Like C3.2

C5.1.2: $x > 0, y = 1$ → Like C3.2

C5.1.3: $x \geq 0, y > 1$ → Like C3.2

C5.2: $r \to i$ → Like C5.1

Limitations

Limitations

- Theoretical analysis (not considering implementations).

Limitations

- Theoretical analysis (not considering implementations).
- Long-term identity key is used in initial handshake and to sign medium-term key. We just assume for simplicity that the medium term key is authentic.

Limitations

- Theoretical analysis (not considering implementations).
- Long-term identity key is used in initial handshake and to sign medium-term key. We just assume for simplicity that the medium term key is authentic.
- We assume honest key distribution.

Limitations

- Theoretical analysis (not considering implementations).
- Long-term identity key is used in initial handshake and to sign medium-term key. We just assume for simplicity that the medium term key is authentic.
- We assume honest key distribution.
- Multiple devices not considered yet.

[Signal, EuroS&P '17]: "Looks pretty good! (some caveats)"

Thanks for listening

1. There’s this cool new security property called “post-compromise security”.
2. Signal Protocol achieves it in addition to other security properties.
3. But there is more to investigate.

[PCS] *On Post-Compromise Security.*
Cohn-Gordon, Cremers and Garratt. CSF ‘16.
ePrint link: ia.cr/2016/221.

[Signal] *A Formal Security Analysis of the Signal Messaging Protocol.*
Cohn-Gordon, Cremers, Dowling, Garratt, and Stebila. Euro S&P ‘17.
ePrint link: ia.cr/2016/1013.