WhatsApp Backdoor (/Bug?)

Another reason for not trusting closed-source crypto
WhatsApp

• 1 billion monthly active users (February 2016)
  • 1/7 of world population
• end-to-end encryption “completely” implemented April 2016
• Implements the Signal protocol
The Backdoor

Alice

Bob

https://tobi.rocks/
The Backdoor

Alice

Bob

https://tobi.rocks/
The Backdoor

Alice

Bob

https://tobi.rocks/
The Backdoor

Alice and Bob meet in person and verify the fingerprint

Alice

Bob
The Backdoor

Alice

https://tobi.rocks/

Bob
The Backdoor

4  "Hi Bob"

Alice → Cloud → Bob

https://tobi.rocks/
The Backdoor

Alice

Bob

4 “Hi Bob”

5 Key

https://tobi.rocks/
The Backdoor

4 “Hi Bob”
5 🔒
6 “Hi Bob”

https://tobi.rocks/
The Backdoor

Bob’s security code has changed

Alice

4 “Hi Bob”

5

6 “Hi Bob”

Bob

https://tobi.rocks/
The Backdoor

Bob’s security code has changed

4 “Hi Bob”

5 Key

6 “Hi Bob”

8 “Hi Bob”

Alice

Bob

https://tobi.rocks/
Signal is doing it right

- The warning is displayed
- The message is never retransmitted
Disclosure Timeline
Disclosure Timeline

• Whitehat report on April 10
Disclosure Timeline

• Whitehat report on April 10
• Facebook, May 25: “This is expected behavior”
Disclosure Timeline

• Whitehat report on April 10
• Facebook, May 25: “This is expected behavior”
• Me: “This should not be expected behavior. “
Disclosure Timeline

• Whitehat report on April 10
• Facebook, May 25: “This is expected behavior”
• Me: “This should not be expected behavior. “
• Facebook, May 31: “We were previously aware of the issue [...] for now it's not something we're actively working on changing”
Disclosure Timeline

• Whitehat report on April 10
• Facebook, May 25: “This is expected behavior”
• Me: “This should not be expected behavior. “
• Facebook, May 31: “We were previously aware of the issue [...] for now it's not something we're actively working on changing”
• Status (December 28): Not fixed
More reasons to use Signal

• Signal is open source
• Signal has mostly reproducible builds
• WhatsApp may store Metadata (according to privacy policy)
  • time stamp information
  • success of message delivery
  • phone numbers of sender and recipient
  • contact lists
  • “other information”
• Signal stores less:
  • last day a user connected
  • contact lists are not stored on signal servers