CryptoSMS
Text message encryption for Android

David Brazdil

University of Cambridge

September 15, 2011

Powerful enemies

- Can read and manipulate everything you send
- Can send a message from arbitrary phone number
- Can gain physical access to your handset
- Can install a malicious application on your phone

Strong protection

- Messages encrypted with AES/CBC/HMAC
- Key negotiation with Elliptic Curve Diffie-Hellman
- Authentication provided by external application
- Forward secrecy
- All data stored in an encrypted file

With thanks to Richard Clayton and Joseph Bonneau

Data SMS standard

- sent to a specific port
- not stored by the OS
- 133 bytes instead of 140
- long messages divided into multiple parts
  - 82 bytes in first part
  - 130 bytes in other parts
- text compression with DEFLATE

Text compresses very well

French

Salut Pierre, ça va ? Je suis désolé, mais je ne serai pas là à cinq heures, parce que je suis malade. Je suis libre ce lundi et toi ? Quand tu as quelques problèmes, appelles-moi. J'espère que tout sera ok.

UTF-16	UTF-16 + DEFLATE	UTF-8	UTF-8 + DEFLATE
412 B	210 B	212 B	164 B

Text compresses very well

Hebrew

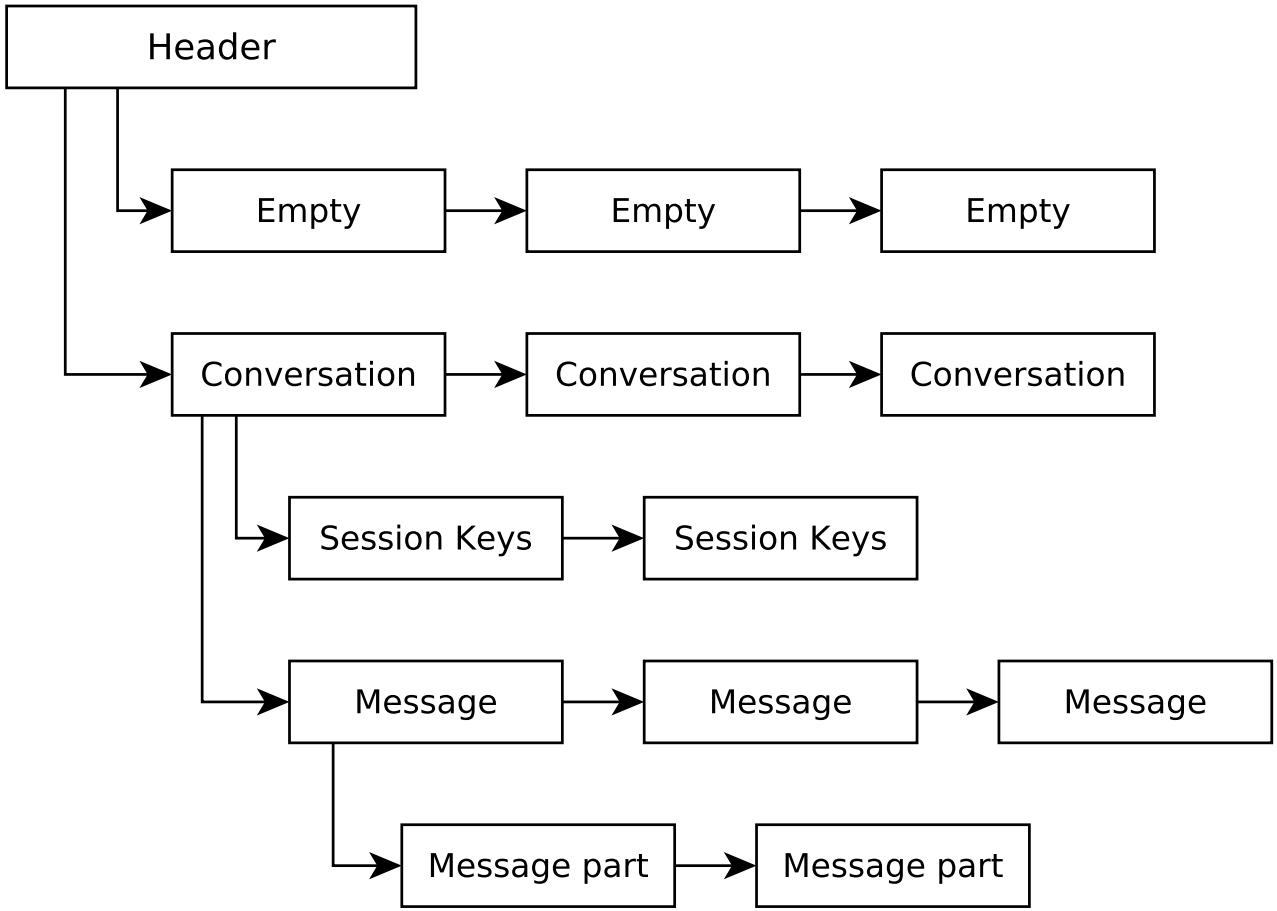
דוד אחי היקר! איפה היית אתמול בלילה? לא עם הבחורה ההיא מ ישו אני מקווה? נכנסתי למועדון עם דן ודניאל. שניהם באמת יודעים לשתות! חבל שלא היית שם כדי לעזור לי להוציא אותם משם. אני מקווה שזה לא יקרה שוב ...

UTF-16	UTF-16 + DEFLATE	UTF-8	UTF-8 + DEFLATE
404 B	201 B	353 B	189 B

Storage file

- all messages and session keys are reencrypted under a new key
- not necessary to decrypt the whole file
- does not reveal its internal structure
- speed optimized for the most common tasks

Storage file structure



Reveals nothing to the outside

IV	MAC	Encrypted header
IV	MAC	Encrypted entry 1
IV	MAC	Encrypted entry 2
IV	MAC	Encrypted entry 3
IV	MAC	Encrypted entry 4
IV	MAC	Encrypted entry 5
IV	MAC	Encrypted entry 6
IV	MAC	Encrypted entry 7

⋮

Cooperation with the Key Ring

- Signs data and verifies signatures
- Shared login session
- Application locks itself after logging out
- Storage file key stored in the Key Ring

Achievements and issues

- ✗ Uninstalling the Key Ring deletes the storage key
- ✓ Messages encrypted and authenticated
- ✓ Data protected in a safe storage file