BabelCrypt: The Universal Encryption Layer for Mobile Messaging Applications

Middle East Technical University, Ankara

Sabanci University, Istanbul

Northeastern University, Boston

Ahmet Talha Ozcan, **Can Gemicioglu**, Kaan Onarlioglu, Michael Weissbacher, Collin Mulliner, William Robertson and Engin Kirda

Communication Today

Privacy Threats

- Intercepted communication between user and service provider
- Malicious communication service provider
- Compromised accounts
- Malicious third party code

Current Methods

- Standalone messaging applications
  - Silent Text
  - ChatSecure
  - Threema
  - TextSecure

- Another Similar System

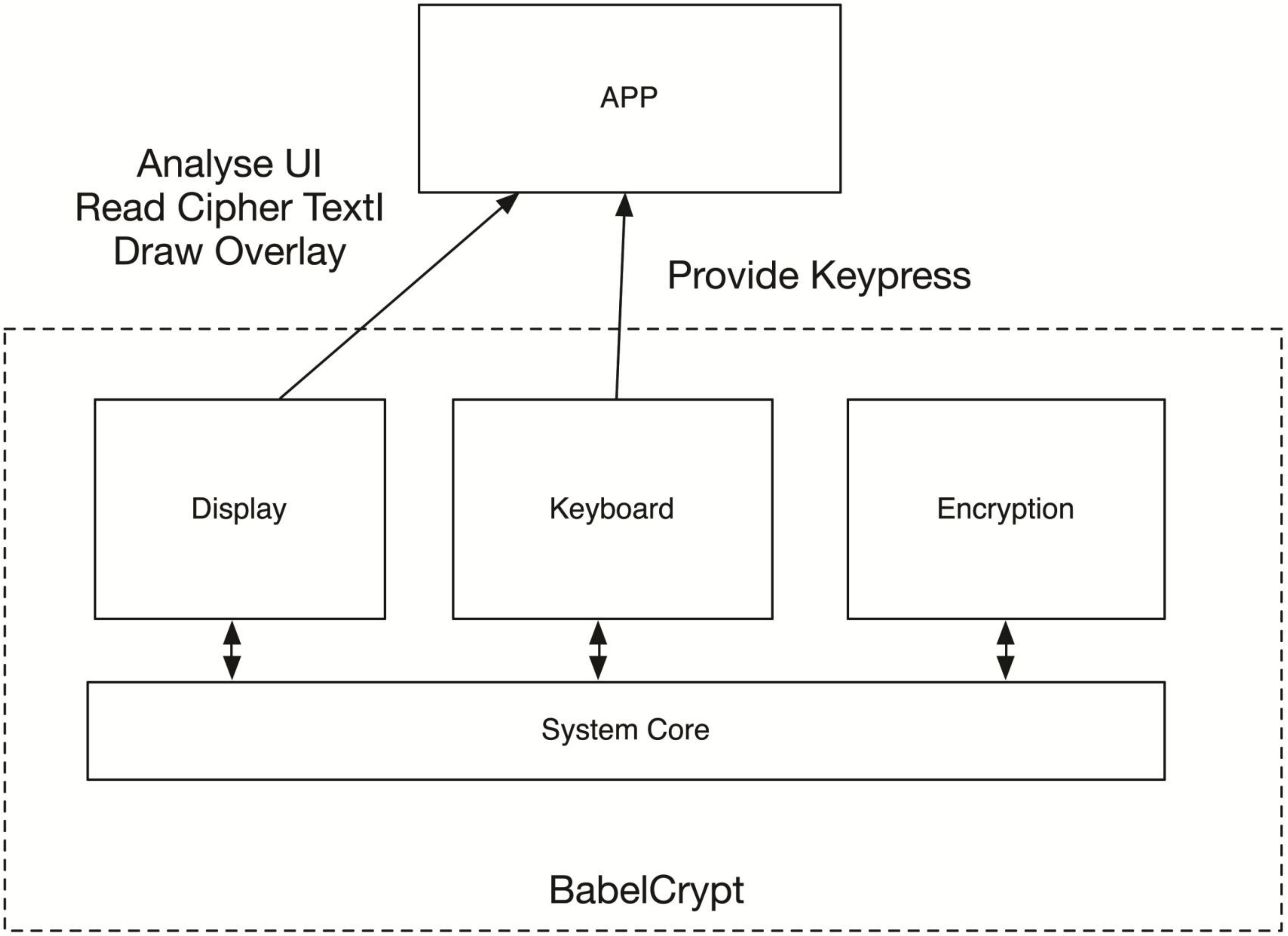
  Mimesis Aegis

BabelCrypt

BabelCrypt provides a solution to these threats with a generic and application transparent system that handles both the encryption and decryption on the users side.

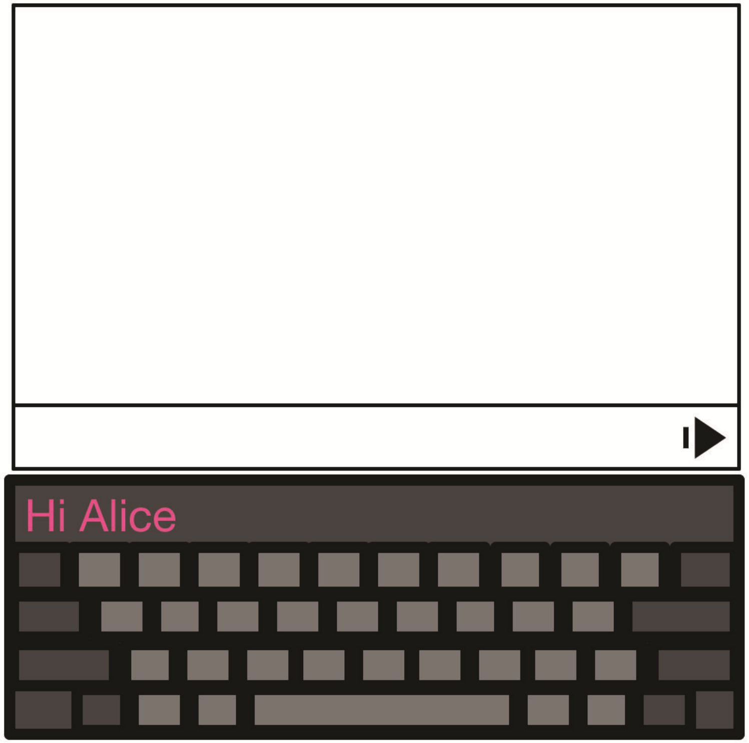
Goals

- Ensure that the user experience is not changed drastically.
- Underlying chat application should remain oblivious to the presence of the encryption layer.
- Be independent of the specifics of the underlying application, or the service provider.


APP
Analyse UI
Read Cipher TextI
Draw Overlay
Provide Keypress
Display
Keyboard
Encryption
System Core
BabelCrypt

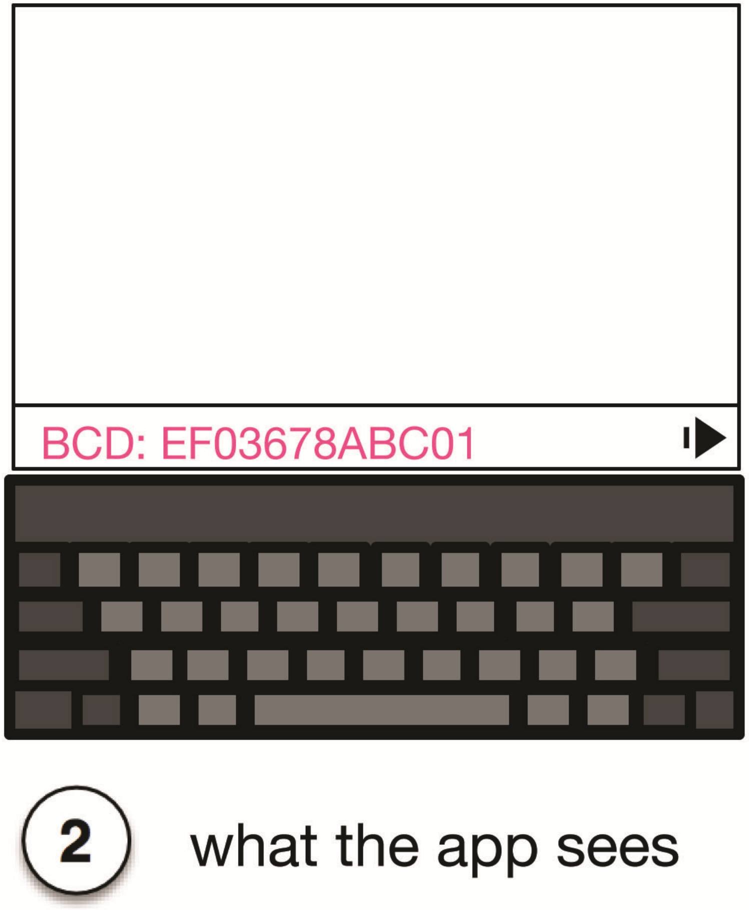
NEU SECLAB

System Design



1 the user types

System Design

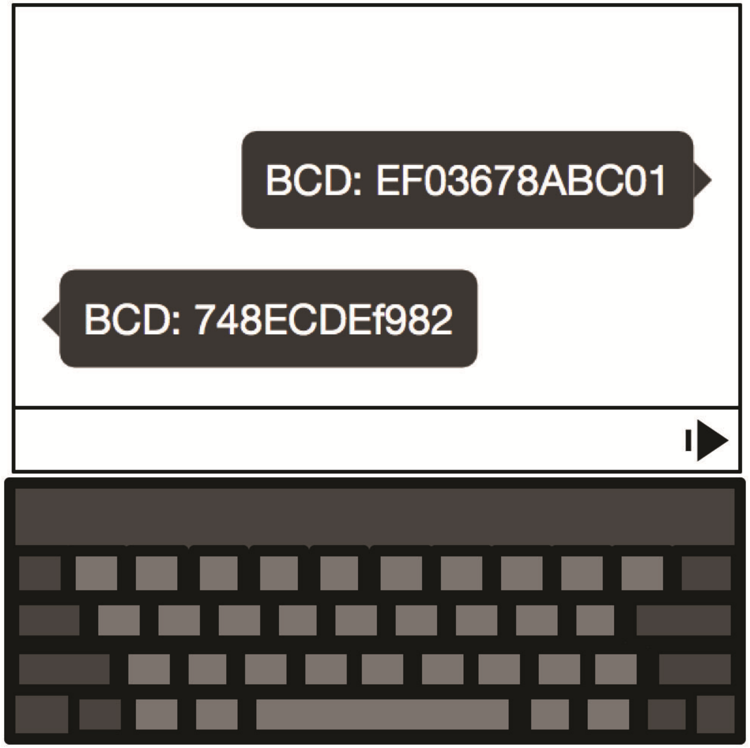


System Design

BCD: EF03678ABC01

3 what the app sends

System Design

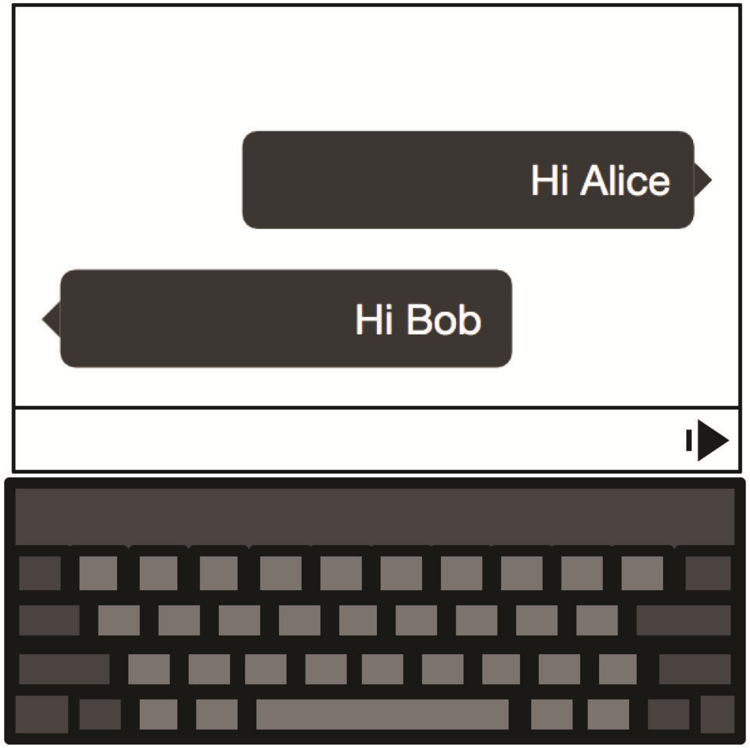


BCD: EF03678ABC01

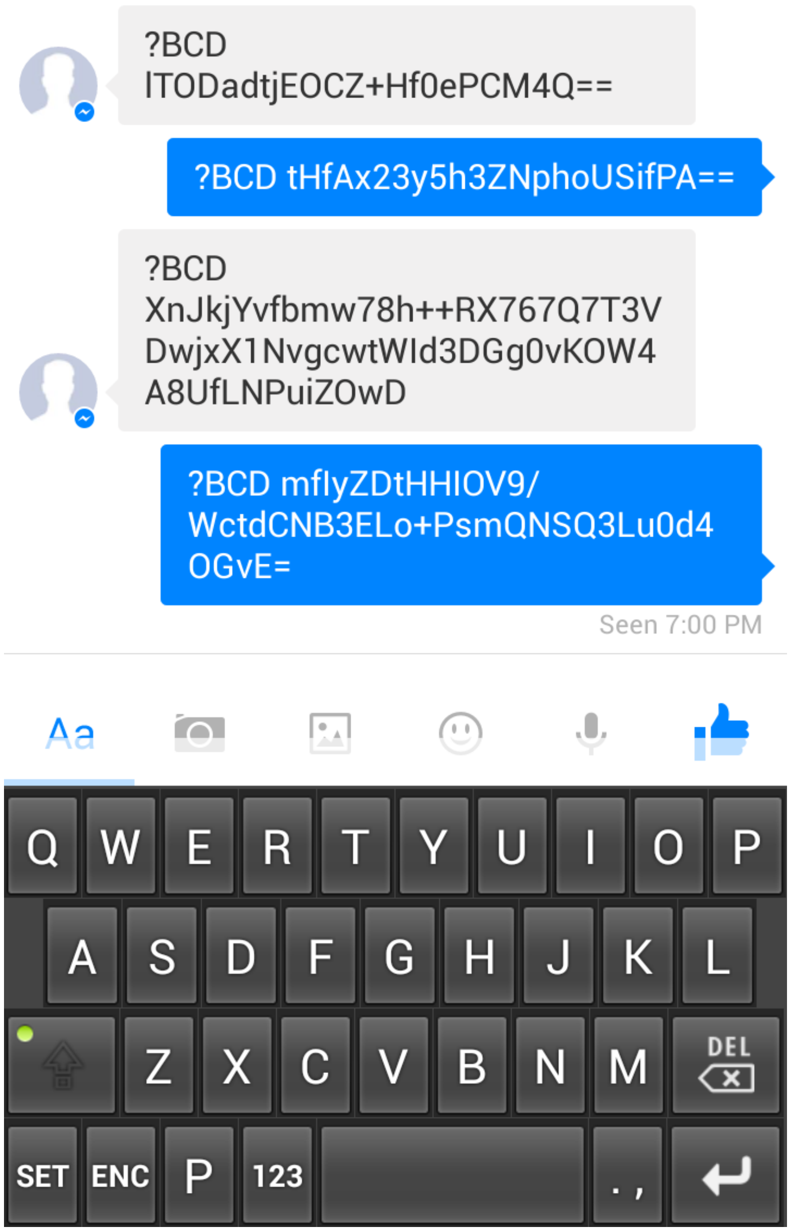
BCD: 748ECDEf982

4 what the app receives

System Design



5 what the user reads



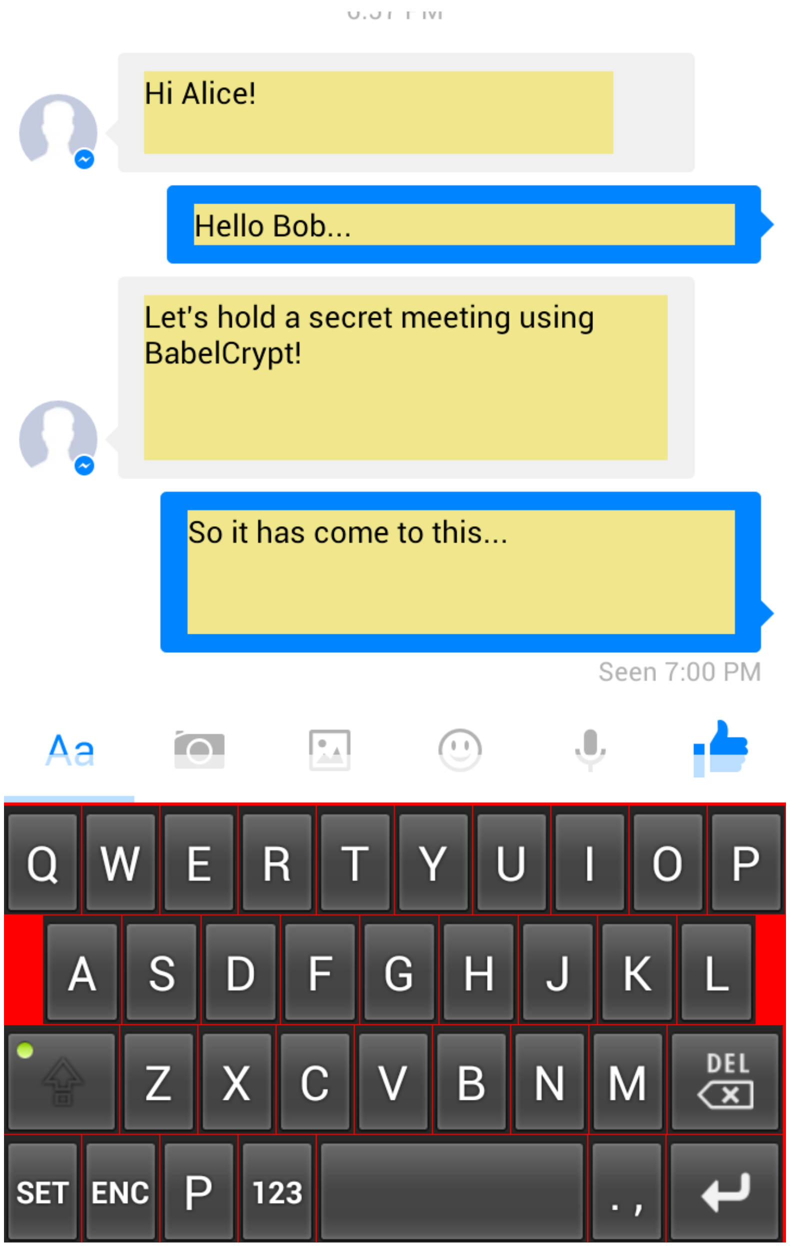
?BCD lTODadtjEOCZ+Hf0ePCM4Q==

?BCD tHfAx23y5h3ZNphoUSifPA==

?BCD XnJkjYvfbmw78h++RX767Q7T3VDwjxX1NvgcwtWId3DGg0vKOW4A8UfLNPuiZOwD

?BCD mflyZDtHHIOV9/WctdCNB3ELo+PsmQNSQ3Lu0d4OGvE=

Seen 7:00 PM



Hi Alice!

Hello Bob...

Let's hold a secret meeting using BabelCrypt!

So it has come to this...

Seen 7:00 PM

Demo

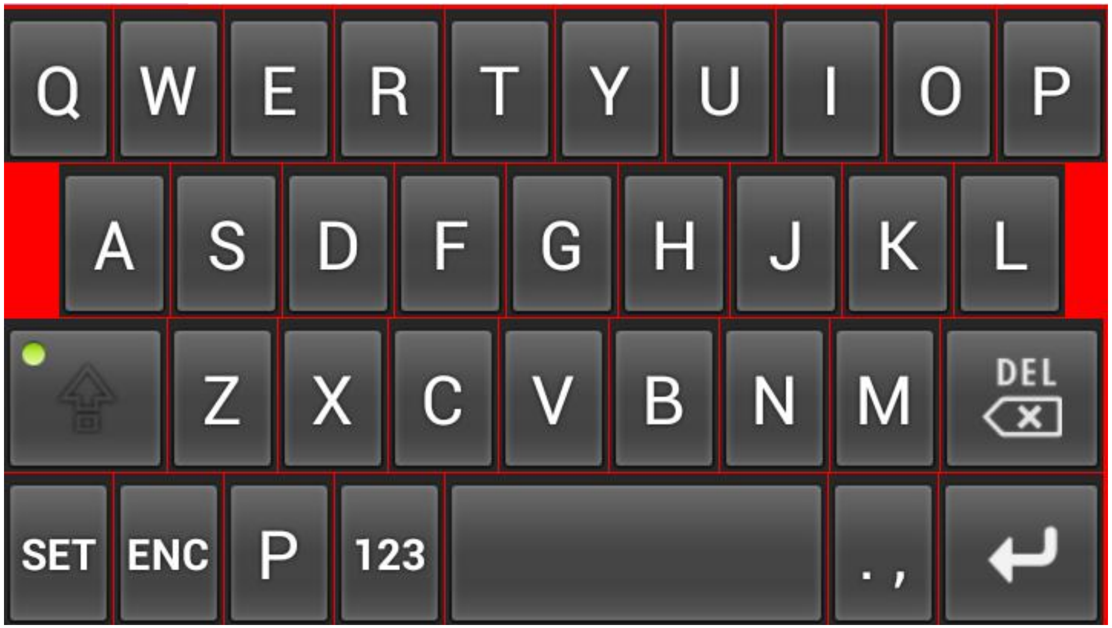
System Design

Multiple Encryption Modes:

- Shared Secrets: PBKDF2

System Design

- Secure Communication Protocol: Off-the-Record (OTR)



Usability

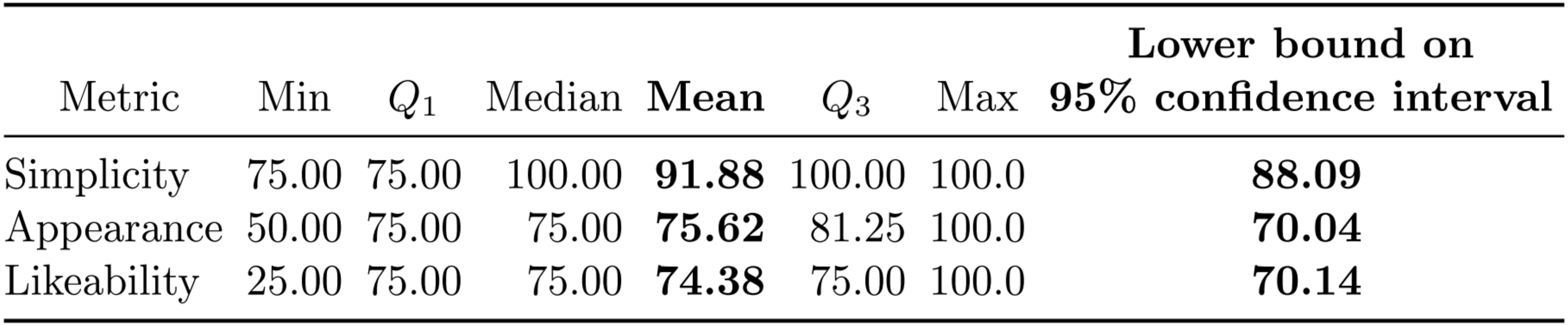
Tested system on:

- Facebook Messenger
- WhatsApp
- Skype
- Tango
- WeChat
- Viber

Usability

Performance overhead: 150.1ms average with 69.0 ms of standard deviation

Usability



Metric	Min	Q_1	Median	**Mean**	Q_3	Max	**Lower bound on 95% confidence interval**
Simplicity	75.00	75.00	100.00	**91.88**	100.00	100.0	**88.09**
Appearance	50.00	75.00	75.00	**75.62**	81.25	100.0	**70.04**
Likeability	25.00	75.00	75.00	**74.38**	75.00	100.0	**70.14**

User Study on Usability of BabelCrypt

Summary

- We have seen that the current options are not enough to defend against all threats.
- For most users, threats do not seem significant enough to change their habits.
- BabelCrypt is proposed as a system that will transparently protect the user.
- BabelCrypt can work with arbitrary security protocols without disturbing users.

Thank You!

Any questions?