Homework #5
Telegram vs WhatsApp Security

CNS Course Sapienza

Riccardo Prinzivalle, 1904064

November 30, 2020

1 Homework Goal

This homework contains a comparison of Telegram and WhatsApp security, with an in deep to protocols comparisons and past and some current threat an vulnerabilities.

2 Telegram Security basics

Telegram uses a security protocol called MTProto, developed by the telegram team. It is a symmetric encryption protocol based on 256-bit symmetric AES encryption, 2048-bit RSA encryption and Diffie–Hellman key exchange. The protocol is divided in 3 layers:

- **High-level** component which defines the method whereby API queries and responses are converted to binary messages.
- **Cryptographic/authorization** layer which defines the method used to encrypt messages prior to being transmitted through the transport protocol.
- **Transport** component, which defines the method for the client and the server to transmit messages over some other existing network protocol.

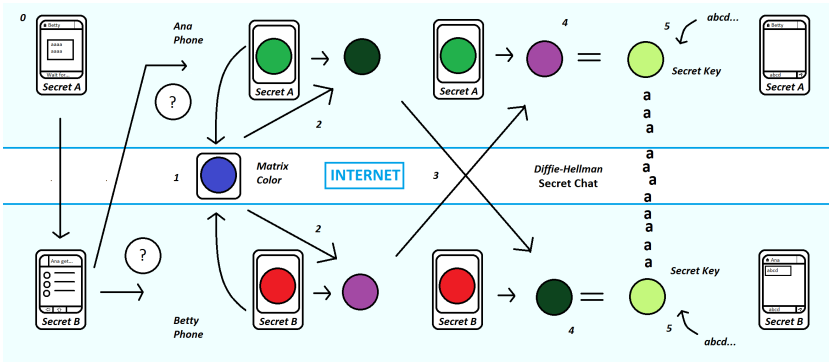

Figure 1: Telegram encryption scheme [1]

3 WhatsApp Security Basics

4 Protocols comparison

5 Past Evolution and Fixed Vulnerabilities

6 Current Vulnerabilities and Security Threats

7 Conclusion

After this brief introduction on elliptic curves, it is obvious why they have been widely adopted in many cases of asymmetric encryption: they use less bits for the same level of security, so are more efficient to compute and their base concepts are easier to visualize. As suggested on section , EC can be easily used in hybrid encryption scheme, in the key exchange phase.

References

[1] D. Sanguinetti. `https://commons.wikimedia.org/w/index.php?curid=36531862`.