SMS E2E Encryption and Tunneling for Smart Mobile Devices

By Michael Kangethe
Bsc IT (JKUAT), Msc CS (UoN), CEH (Practical), PhD CS (UoN) (Ongoing)

Questions

1. Have you ever communicated with someone you know via SMS (sent or received) over the past 30 Days?
2. Have you ever had the feeling or suspicion that your SMS messages are not private?
3. Do you use Whatsapp or the Signal app for the privacy it provides?
4. Would you like the same level of privacy that Whatsapp or Signal provide for SMS communication?

If you answered **YES** to at least **TWO** of the Four Questions, this could be for you.

#whoami

- Researcher (Cryptography and AI) - Published
- Technical and Cyber Security Consultant
- Software Developer
- Lecturer
- PhD Candidate CS UoN - Randomized Cryptography
- Kenpo Practitioner - Shodan

SMS

SMS stands for **S**hort **M**essage **S**ervice and is commonly known as texting. It's a way to send text-only messages of up to 160 characters between phones.

The MOST Ubiquitous form of messaging:

- Device independent
- Provider independent (Doesn’t depend on the Service provider Airtel/Safaricom/Country)
- Doesn’t require internet connection - global reach

SMS Security

Dependent on the GSM Service providers encryption implementation A5/1, A5/2, A5/3 ,A5/4

Depending on the Country'S Agreement and export controls

Between mobile and base station controller (BSC, the network entity entity that manages the radio resources). The radio link transports a couple of higher level protocols, among them MAP which is used to transport SMS.

Encryption and security is not E-2-E, Just over the air from Device to BTS

Refer here : https://payatu.com/dissecting-gsm-encryption-location-update-process#:~:text=GSM%20makes%20use%20of%20a,a%20ciphering%20key%20(KC).

Note

Cellular service providers retain records of the parties to a text message and the date and time it was sent. They do not, however, retain the content of text messages for very long, if at all.

They can However turn retain and turn over your text if requested through a court order.

Laws only change as technology advances.

major cellular service providers. The memorandum contained information from the six largest cell phone carriers in the United States: Verizon, T-Mobile, AT&T/Cingular, Sprint, Nextel and Virgin Mobile. All of the providers retained records of the date and time of the text message and the parties to the message for time periods ranging from sixty days to seven years.

However, the majority of cellular service providers do not save the content of text messages at all. As of 2010, Verizon Wireless saved text message content for three to five days while Virgin Mobile retained text message content for ninety days but stated that it would only disclose that content if law enforcement had a search warrant containing a "text of text" request. As recently as November 25, 2015, T-Mobile's privacy policy indicated that it retained "calls and text messages you send and receive (but we do not retain the content of those calls or messages after delivery)." Nathan Freitas, a fellow at the Berkman Center for Internet and Society at Harvard University explained that the carrier may have "details of whom [was]texted and when" but "the actual text is what is really hard to get, if not impossible" from the carrier. The Boston

Source:https://news.law.fordham.edu/jcfl/2016/06/02/cell-phone-forensics-powerful-tools-wielded-by-federal-investigators/#:~:text=Cellular%20service%20providers%20retain%20records,very%20long%2C%20if%20at%20all.

https://www.safaricom.co.ke/dataprivacystatement/

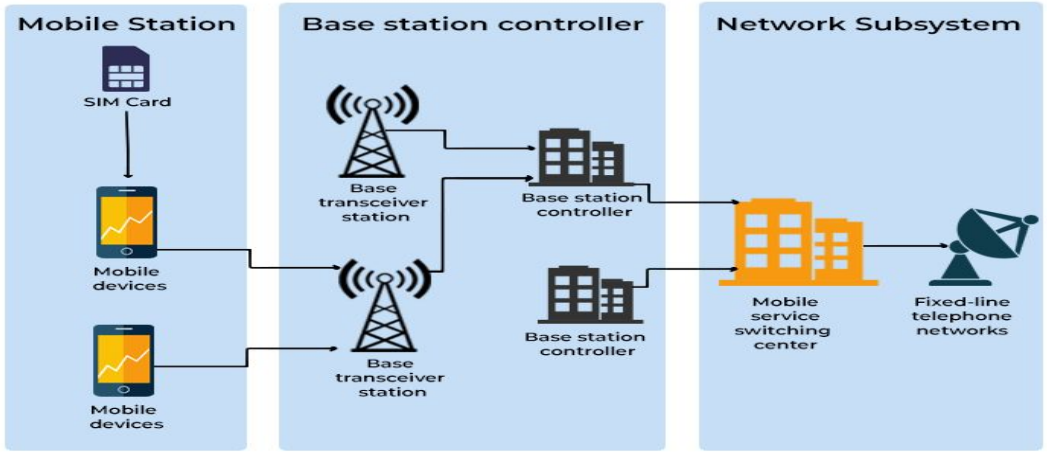
3.2.6 Your contact with us, such as when you: call us or interact with us through social media, our chatbot Zuri, 'snail mail', email (we may record your conversations, social media or other interactions with us), register your biometric information such as your voice, finger prints etc, visit a Safaricom Shop or other retail outlet.

3.2.7 Your account information, such as your handset type/model, tariff, top-ups; subscriptions (including third party subscriptions), billing statements, cloud hosting registration details, e-commerce registration and usage, M-PESA and mobile money transactions.

3.2.8 Your call data records: phone numbers that you call or send messages to (or receive calls and messages from), log of calls, messages or data sessions on the Safaricom network and your approximate location (save for customer service interactions as noted above we do not record or store message or call contents).

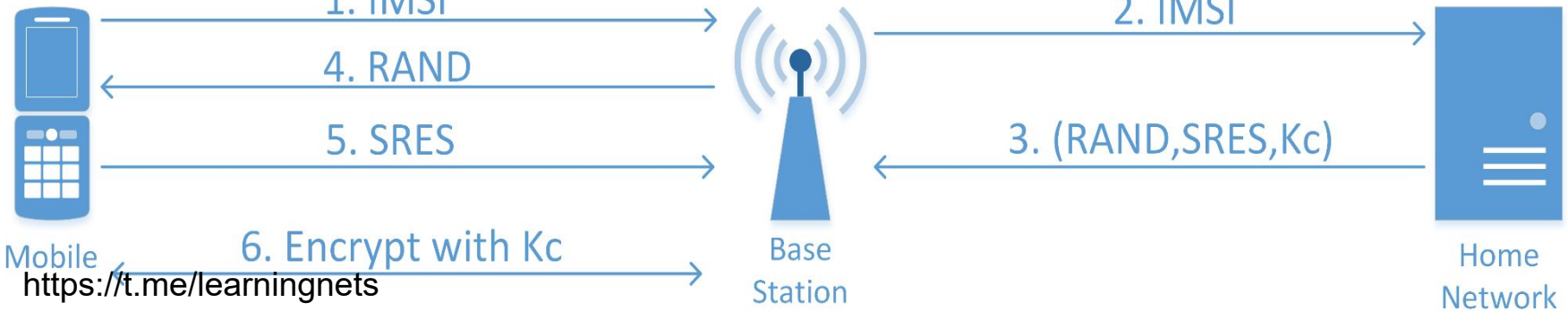
3.2.9 We use Closed Circuit Television (CCTV) surveillance recordings. CCTV Devices are installed at strategic locations to provide a safe and secure environment in all Safaricom premises as a part of our commitment to community safety, security and crime prevention.

SMS Security



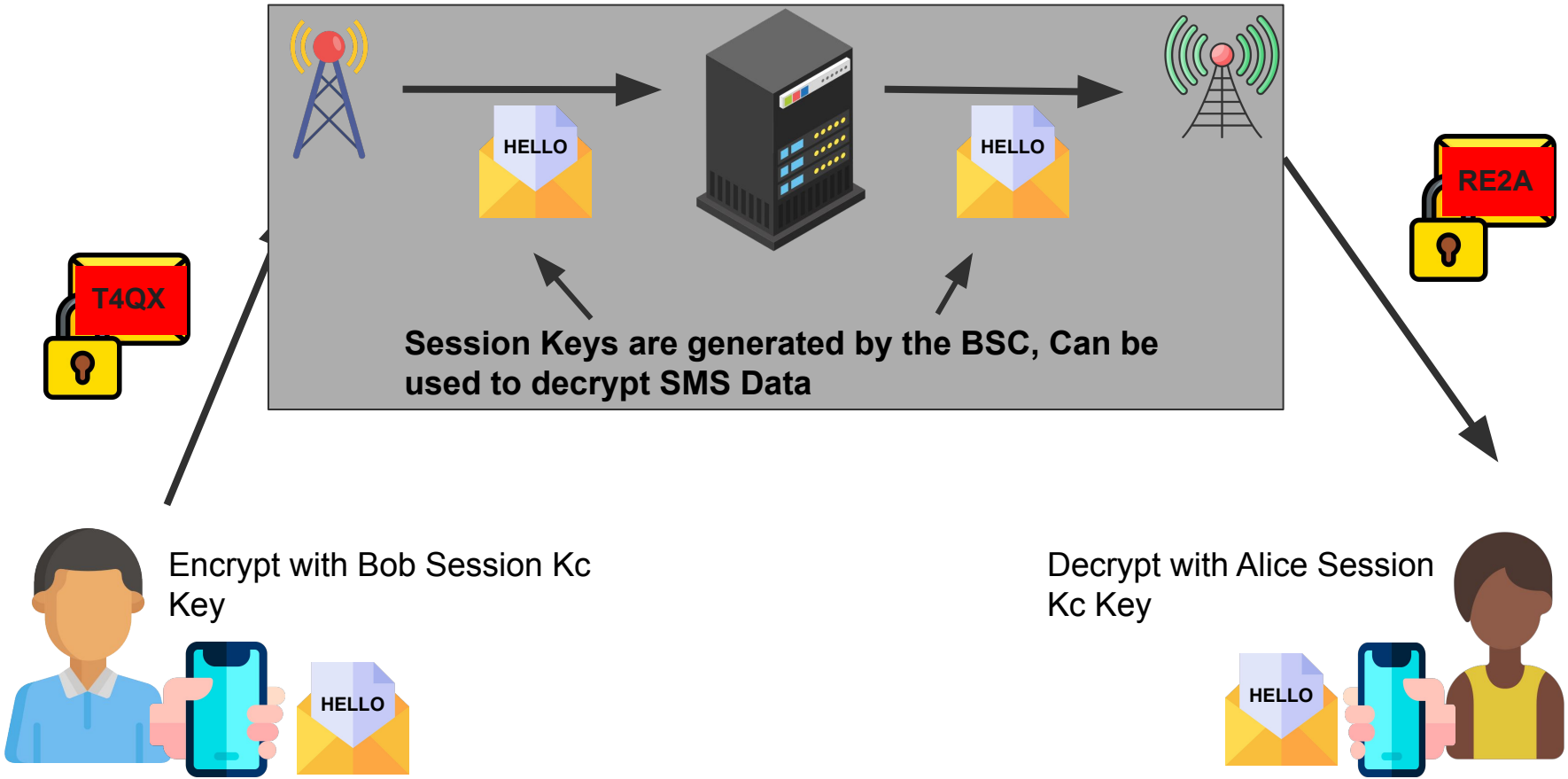
Sim Card

A3,A8
IMSI
Ki



Side Note

Any communication service provider who generates the shared key, or a portion of it, FROM their CENTRAL SERVICE/ SERVER can decrypt your encrypted communication. It is NOT encrypted with E-2-E.



Current SMS Communication and Security

SMS Privacy Issues

Since SMSes are not E-2-E Encrypted, s dependent on the Service Provider Only Encrypted from the device to the BTS the below issues arise:

GSM Sniffing: Voice Decryption 101 - Software Defined Radio Series Source -https://youtu.be/krJJKjYdwgc

Interception from in plaintext format From the service provider SS7 .

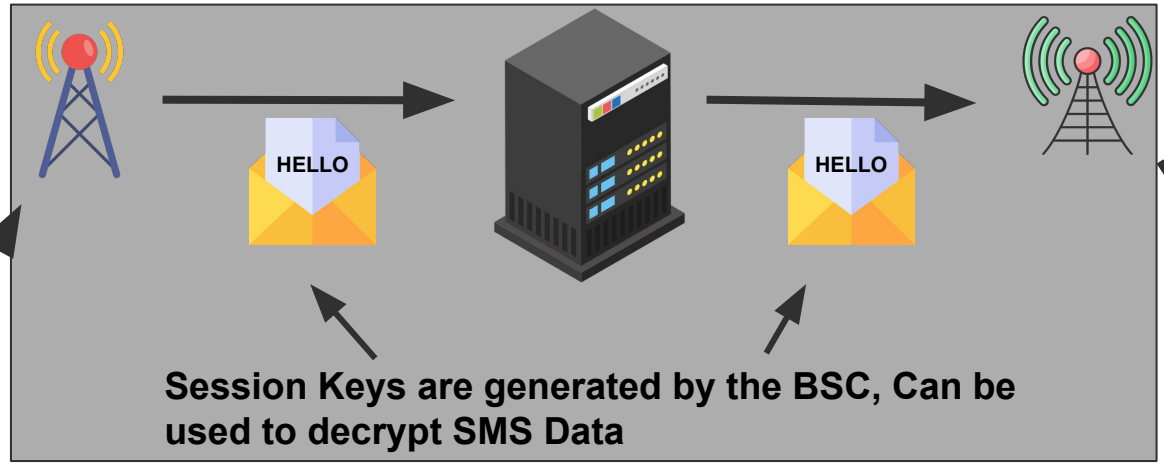
Communication network patterns analysis: Michael M Kangethe, Robert Oboko. Associations Rankings Model for Cellular Surveillance Analysis. Journal of Computer Sciences and Applications. Vol. 8, No. 2, 2020, pp 40-45. http://pubs.sciepub.com/jcsa/8/2/1

Encryption & Tunneling

Tunneling is a way to move packets from one network to another. Tunneling works via encapsulation: wrapping a packet inside another packet. Networking Basics. Network Layer.

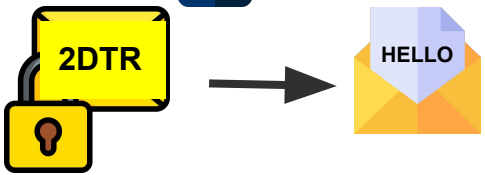
Encryption is the process of transforming information in such a way that an unauthorized third party cannot read it; a trusted person can decrypt data and access it in its original form though.

SMS E-2-E Leverages on GSM Technologies and Encryption Algorithms and solutions to enhance Security and Privacy in SMS Communications

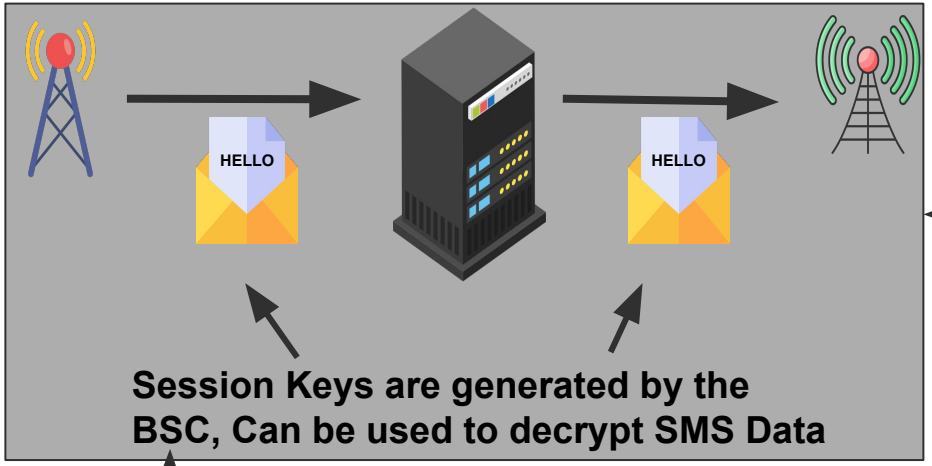


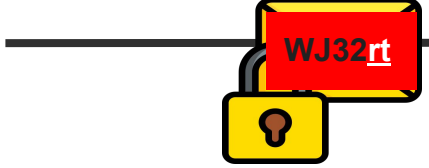
Encrypt with Bob Session Kc Key

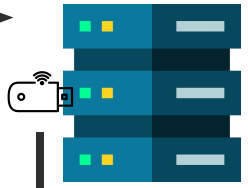
Decrypt with Alice Session Kc Key

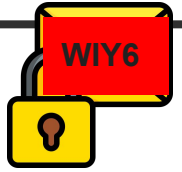


E-2-E SMS Communication and Security





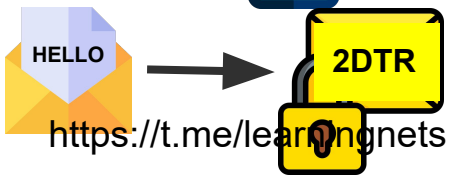


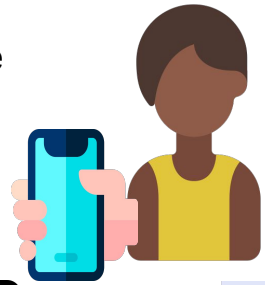


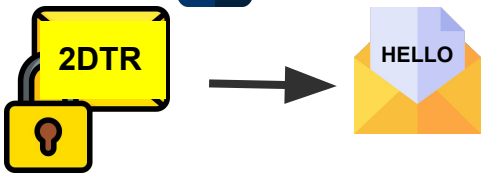
Decrypt
with SMS Gateway
Session Kc Key

Step 1: Encrypt with Bob
Session Kc Key and containing
Routing Info

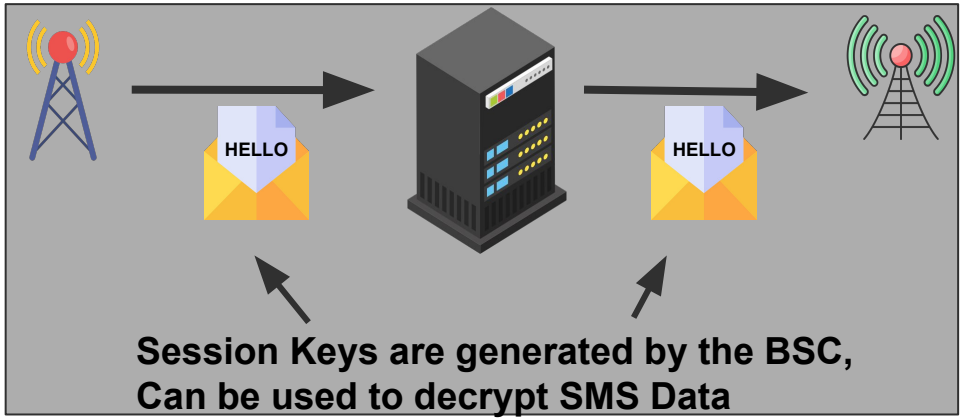
Decrypt with Alice
Session Kc Key



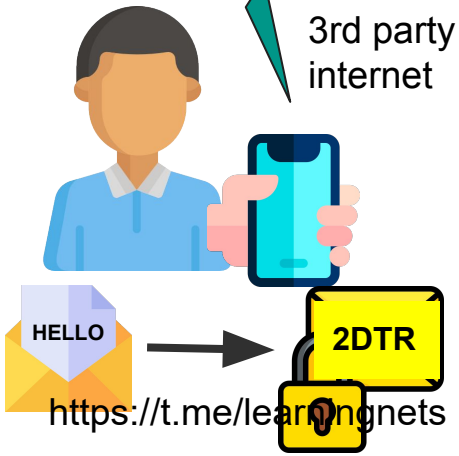




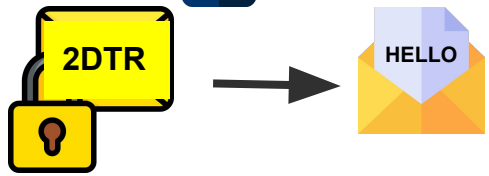
E-2-E SMS and Tunneling Communication and Security using SMS Gateway



Encrypt with Bob Session Ki Key and containing Routing Info to 3rd party SMS API over the internet



Decrypt with Alice Session Kc Key



E-2-E SMS and Tunneling Communication and Security using 3rd Party SMS API

Alice App Generates a **Shared Private key** and **IV** for **Alice&Bob** and appends the key to the

Encrypts The **Key Update** using Bob's Public Key

Decrypts SMS using own private key then compares hash received with hash of Shared Private Key and IV. if match Key Exchange successful

Alice Sends Bob Contact QR then Bob Scans Using APP

Bob Sends Alice Contact QR then Alice Scans Using APP

Here Bob and Alice can communicate using each others Public Key

Alice sends the **Encrypted Key Update** as an SMS to Bob

Bob sends **Hash** of **shared Key** and **IV** to Alice

If Exchange Successful Alice will send ACK
else send new Key and IV to Bob

Contact Key exchange Protocol

Bob Decrypts SMS Using own Private Key then Updates **Bob&Alice** Shared Private Key. Then generates a **hash** of the **Shared Private Key** and **IV**

If Message from Alice is ACK then Update key Exchange Confirmation else Do nothing and use Alice Public key for Communication

Privacy Options Security Matrix

	(Option 1) Encrypt and Send Directly	(Option 2) Encrypt and Send Using SMS Gateway	(Option 3) Encrypt and Send Online using SMS APIs
SMS cannot be read by any party other than the sender and receiver	✅	✅	✅
Uses Public Key Encryption	✅	✅	✅
Uses Shared Private Key Encryption	✅	❌	❌
Sender and Receiver Partially Obscured	❌	✅	❌
Sender and Receiver Fully Obscured	❌	❌	✅

Privacy Options -Explained

- **(Option 1) - Encrypt and Send Directly**
  - SMS cannot be read by any party other than the sender and receiver
  - Sender and receiver is known
  - Uses Both Public and Shared Private Key Encryption
- **(Option 2) - Encrypt and Send Using SMS Gateway**
  - SMS cannot be read by any other party other than the sender and receiver
  - Sender and receiver can only be known by use of Advanced Querying and Data Mining techniques
  - Uses Both Public Key Encryption
- **(Option 3) - Encrypt and Send Online using SMS APIs**
  - SMS cannot be read by any other party other than the sender and receiver
  - Sender and receiver can Not be known even by use of Advanced Querying and Data Mining techniques
  - Uses Both Public Key Encryption

Target Users

Anyone who needs an extra layer of privacy in their SMS Communications

- Companies (With Sensitive Communications)
- Basically if you use whatsapp or Signal you are a target user

DEMO

Observed Issues for Further Research

Message Limitation and dependency on Key Size,

- This is only dependent on Public Key Communication and not a problem in Shared Private Key communication
- For Public Key Communication it uses Multiple messages due to the 256 bit Key size

Latency due to Tunneling and Proxying SMS.

- The time it takes for an SMS to arrive at the clients device is purely dependent to the SMS Gateway/API speed and Uptime.
- However negligible for Most Services

Available Devices

The Current POC has been tested to work on ALL Android Devices from Version 5 and above

Going Forward

Development for IOS Devices has started with a focus on the Kotlin Version Collaborations Welcome

Q&A

Thank you!

@MichK_01

github.com/mich01

linkedin.com/in/mkangethe

Demo APK Source Code: https://github.com/mich01/SpiderSMS