MULTI-CHANNEL MOBILE WIRELESS NETWORK ATTACKS ON SMS

Omego Obinna (k1633137@kingston.ac.uk)

Joint work with: E. Pfluegel, M. Tunnicliffe, C. Clarke, C. Politis

Kingston University

Talk at WWRF Meeting 39, Barcelona

Contents

- Introduction
- Security issues in 1G, 2G, 3G and 4G
- Covert Multi-channel Exploit with SMS
- Defence
- Conclusion

Goal

- SMS can be used for covert messaging with multi – channels on mobile networks.

Introduction

- Mobile Services
  - Text Messaging (SMS).
  - Cloud Computing
  - Video Streaming and conferencing
  - IP telephony
  - Mobile Banking
- Mobile Technologies
  - First Generation (1G) Analog Transmission
  - Second Generation (2G) GPRS and EDGE
  - Third Generation (3G) 3GPP and UMTS
  - Forth Generation (4G) LTE

The Future: 5th Generation (5G)

- To meet demands of future applications
  - To enable a fully mobile and connected society
- Provide new levels of performance:
  - High throughput
  - Low latency
  - High connectivity density
- Provide an efficient heterogeneous environment
  - Assured security

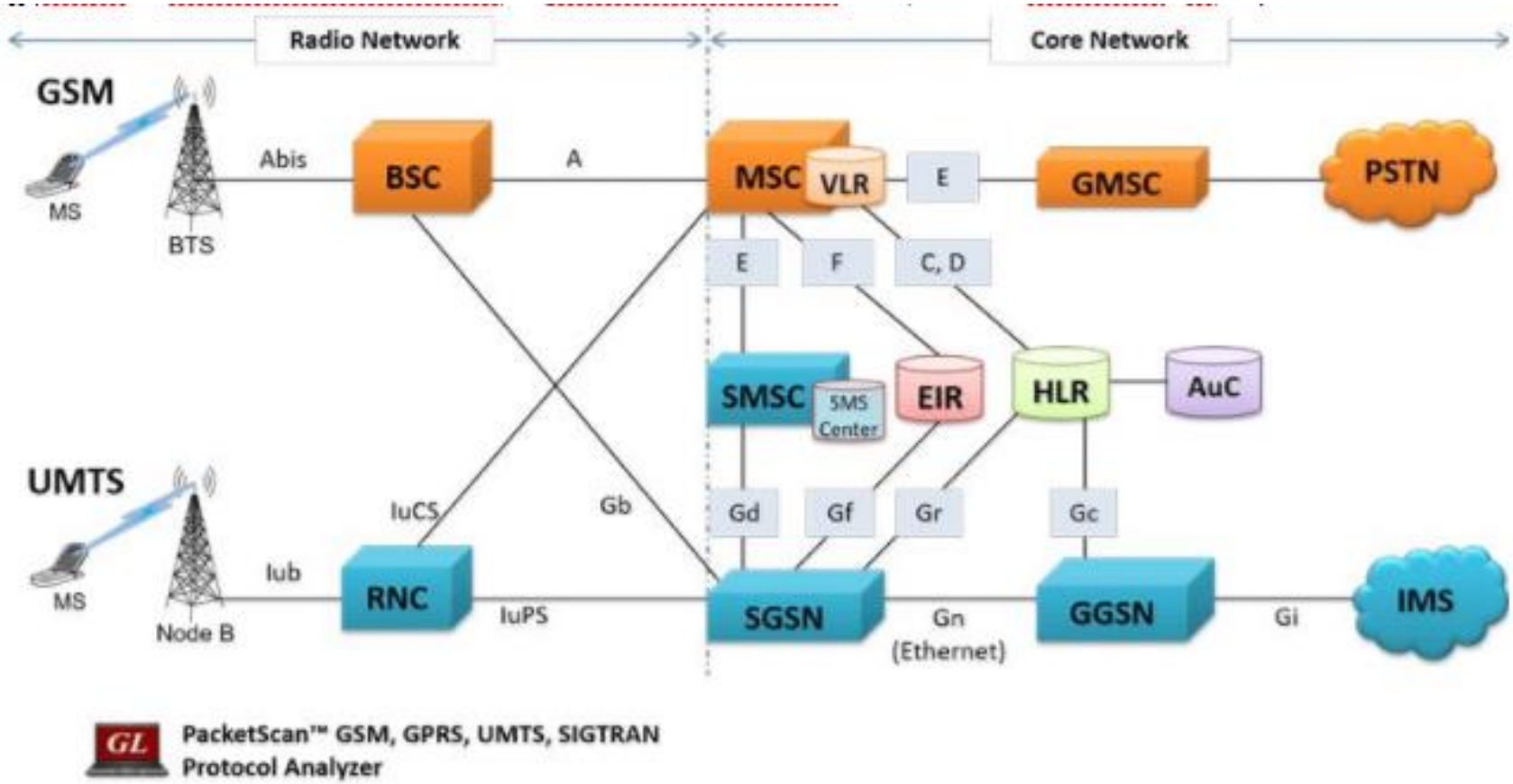
Security in 1G and 2G

- 1G
  - No authentication
  - No encryption
- 2G
  - GSM Phone Authentication
    - “A” Encryption algorithm based on 128-bit key
    - International Mobile Subscriber Identity (ISMI) transferred in plain-text
    - International Mobile Equipment Identity (IMEI) can be requested in plain-text and not authenticated
    - No mutual authentication
    - Encryption ends at the base station

Security in 3G

- 3GPP (3rd Generation Partnership Project) and UMTS (Universal Mobile Telecommunications Service)
  - Security Algorithms
    - 128 bit key -- SNOW 3G -- Stream cipher
    - 128 bit key -- Kasumi -- Block cipher
    - 128 bit key -- Milenage -- Block cipher
  - Security Issues
    - IMSI transferred in plaintext
    - IMEI can be requested in plain-text and not authenticated
    - Encryption ends at RNC (Radio Network Control) but still not end to end.
    - Privacy issue allows tracking of subscribers.

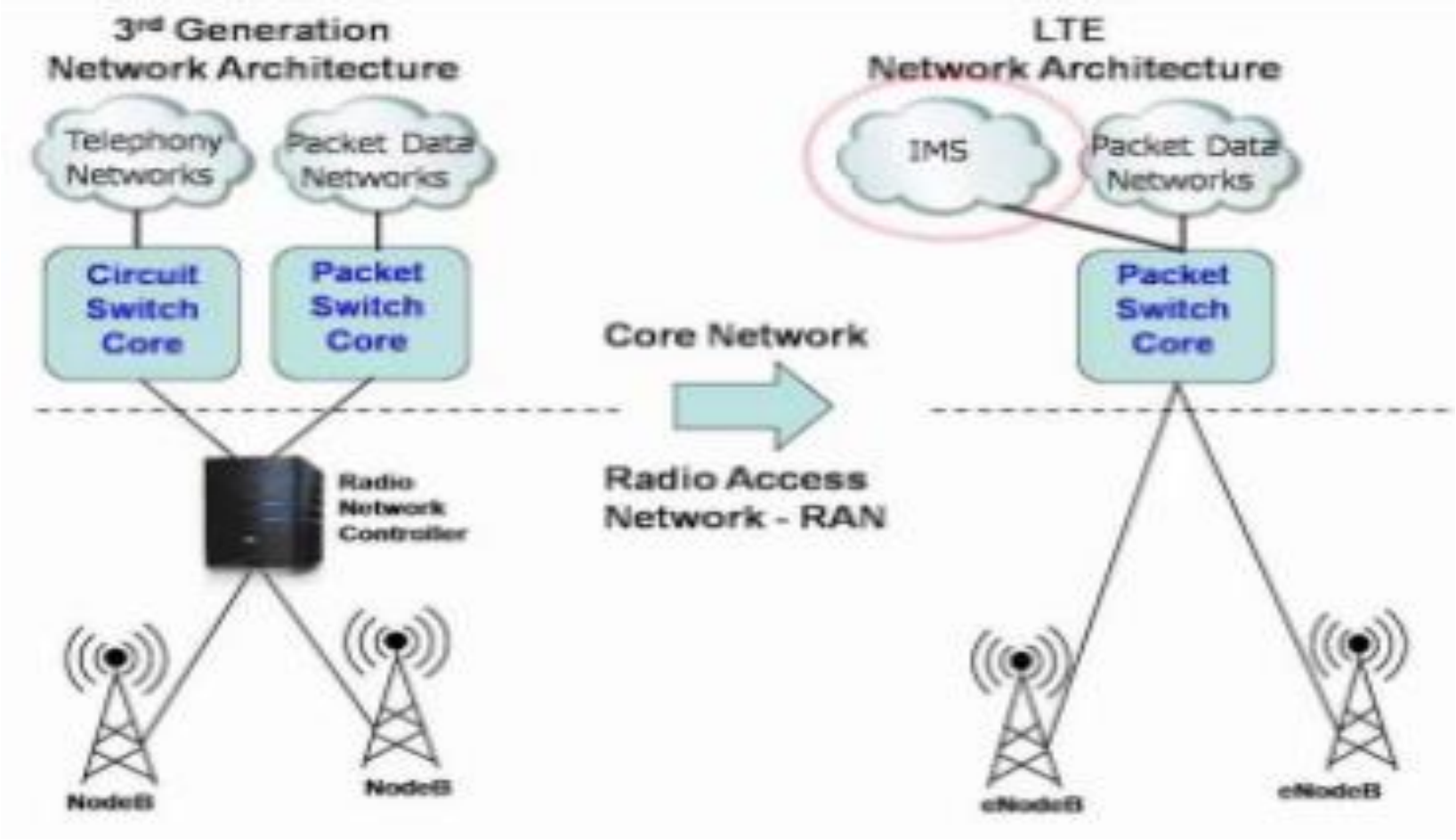
2G and 3G Network architecture: security



Security in 4G

- LTE (Long Term Evolution)
  - Security Algorithms
    - 128 bit key -- Kasumi --- Block cipher
    - 128 bit key -- Milenage --- Block cipher
- Security Issues
  - HeNBs (Home eNodeB) mobile radio access component easily be affordable by adversaries
  - Optimized for micro-deployment areas
    - Indoor premises, public hotspots
  - Adversary can simultaneously create rouge version with functionalities of legitimate base station and user
  - De-synchronization attacks
    - Rouge “home” node can desynchronize handover process

3G and 4G Network Architecture Evolution: Security



Some attacks

- YAMAS (Yet Another Man in the Middle Attack Script)
  - This uses an sslstrip to strip ssl off the traffic so that the victims credentials are transmitted as clear text and are saved in Text File.
  - Almost no detection capabilities for the end-users.
- Key Reinstallation Attacks (KRACK) on wifi
  - By Mathy Vanhoef a postdoc security researcher in the computer science department of the Belgian university.
  - WPA2 flaw
    - Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys, and others
  - Victims are tricked into reinstalling an already-in-use key by manipulating and replaying cryptographic handshake messages.

Cost of Attacking Infrastructure

- Network setup cost
- Open source software/hardware such as
  - USRP (Universal Software Radio Peripheral)
  - Osmocom
  - OpenBTS
  - OpenLTE
  - QT Mobile Hotspot
- HeNB metro cell cost ($2000-$5000)
- HeNB medium cell cost ($10,000)

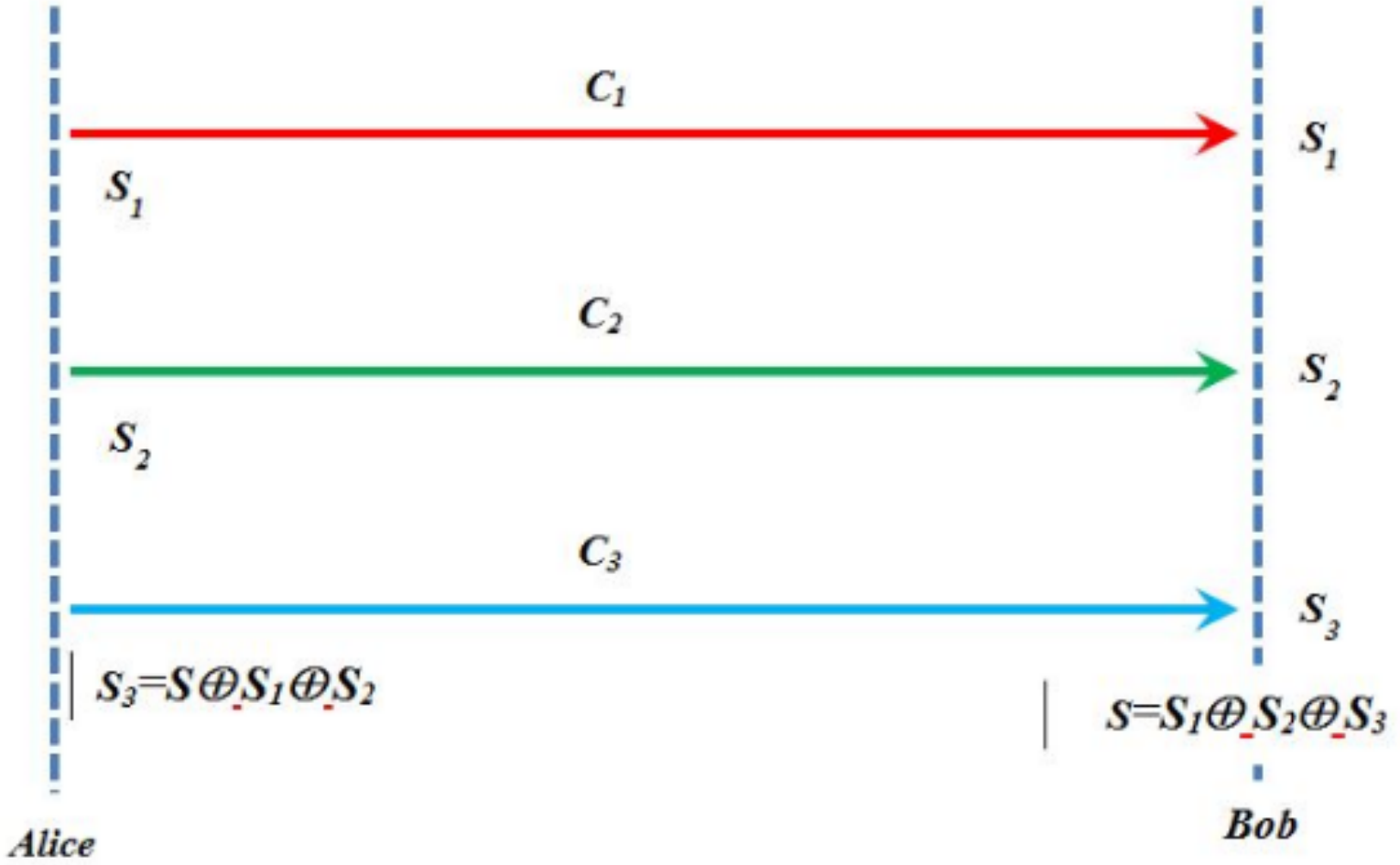
Related Work

- In our work, we adapt members of a protocol family that is initially devised for confidential communication through various social media channels:
  - Beato at el 2014
  - Clarke at el 2015
  - Pfluegel at el 2016
  - Pfluegel at el 2017
- We generalise and adopt these protocols in the context of Covert multi-channel messaging exploit.
- This is an emerging area of research and to our knowledge, the relevant literature base is still quite small.

Covert Multi-channel Exploit with SMS

- SMS
  - SMS used in many countries.
  - First commercially deployed in the 1990s (during 2G era)
  - Danger of illicit use
- Proposed Scenario
  - Alice and Bob are criminals
  - They want to exchange confidential message S via SMS
  - They create three independent SMS channels C_1, C_2 and C_3
  - Each channel belongs to a different provider
  - None of these providers exchange any information

Proposed SMS Exploit



Proposed Exploit

- Alice uses C_1 and C_2 to send fake messages S_1 and S_2 to Bob
- She then sends a third message $S_3 = S \oplus S_1 \oplus S_2$ on channel C_3
  - S_3 has the characteristics of random noise
  - Could not be mistaken for a true message
  - Could be embedded as a steganographic payload to prevent suspicion
- Bob easily recovers the original message $S = S_1 \oplus S_2 \oplus S_3$ while the channel providers remain unaware that any message has been sent

Possible Defence

- S_1 and S_2 could be detected algorithmically
  - Though Alice and Bob could also use genuine messages between them for the same purpose.
- Transmission/reception patterns between pairs of users could also reveal the presence of the attack
- Collaboration: message comparison between providers
  - Might be difficult since providers are typically competitors
  - Do not willingly share data
  - Could be achieved with compliance (e.g. law enforcement, government security services)

Cost of deployment

- Very cheap.
  - Burner mobiles or cheap dual sim mobile.
  - Pay-as-you-go SIMS.

Potential Threats

- Secret service operations.
- Terrorism operations.

Conclusion and Future Work

- We have proposed a Covert multi-channel messaging exploit.
- One of the key features of this protocol is its steganographic confidentiality property against the mobile network operators and external SMS interceptor which, to our knowledge, is a novel feature.
- Further research areas include the investigation of multi-provider messaging exploit variants and possible strategies for mitigating them.

Summary

- Various mobile wireless technologies and their services.
- Some security issues of present and previous mobile networks.
- A covert multichannel messaging exploit.
- We discuss potential ways of mitigating such malicious communication.
- The threats:
  - secret service operations
  - terrorisms operations

Thank You

- K1633137@kingston.ac.uk