Mobile Spy Communications

J. Ostrev, V. Galabov, V. Karlova – Sergieva, T. Pavlov, A. Marinchev

***Abstract*— Security in communications is always critical. It includes two or more sources of transmission - reception and transmission medium and affects a set of protocols and devices and data transfer systems. Usually, encryption and decryption do not solve all security issues. Interference in the communication process is possible and can often destroy security. There are complex hardware and software systems that can often successfully replace one or more parts of the communication process, the identification of which is almost impossible during the process, especially by users and cases of lack of control. Typically, government organizations (but not only) own and use such systems. At the same time, such systems can be used illegally - at any time, for anyone, and for any purpose of espionage. This makes the topic of spying on mobile communications extremely important and relevant.**

***Index Terms*— security in communications, communication process, spying on mobile communications, home location register (HLR)**

I. POSSIBLE WAYS OF SPYING

There is already a wide range of different options for spying on mobile communications:

- Screenshot screens control of employees, video recordings, and video feeds offering
- Direct monitoring (Messaging and Applications)
- Using of previous account information
- Third party invisible monitoring
- Applications with desktop control orientation
- Employees' mobile devices spying procedures
- GPS tracking
- GPS exchange data Applications
- Internet monitoring (IP addresses, cookies, etc.)
- Clipboard monitoring
- Spying data at VOIP calls
- Tracking communication logs
- Viewing and Remote control
- Using data about Access to calendar, notes, reminders, etc.
- Access to the user hardware (Surroundings)
- Laptop tracking, using some specific generated data to omit additional sensitive content and users data, usually for hacking or third party interest
- Mobile hacking
- Others Spying Applications sending sensitive documents data.

Summary information on mobile fraud is shown on Fig.1.
Fake base-stations.1

- Used for: IMSI/IMEI/location tracking, call &data interception
- Exploit weaknesses in 2G & 3G (partially)
- Knows as IMSI Catchers
- Difficult to detect on normal phones (Darshak, Cryptophone or Snoopsnitch)

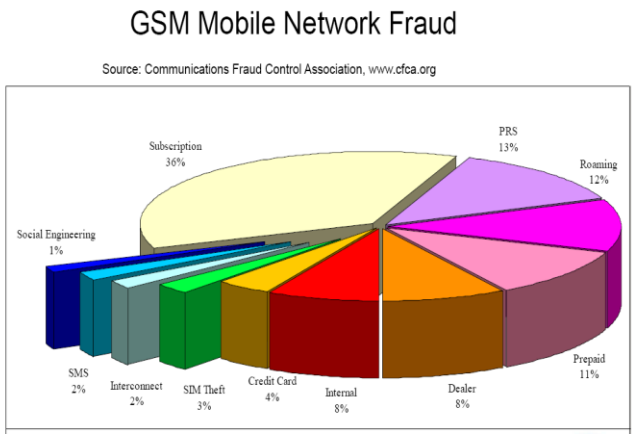

Fig. 1. Summary information on mobile fraud

At Fig. 2 the localization of a subscriber is shown.

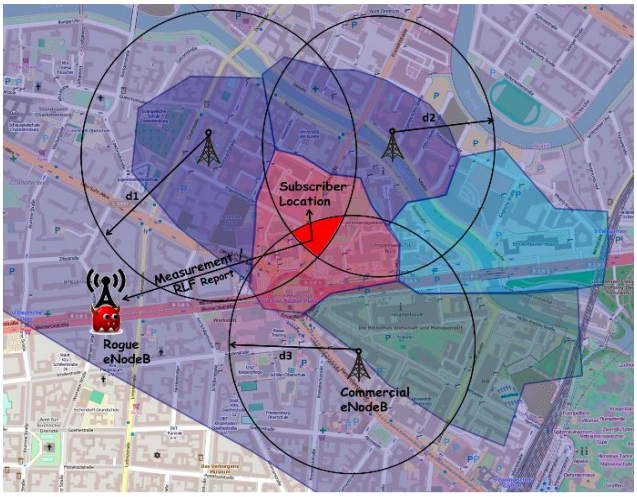

Fig. 2. Localization of a subscriber

Many algorithms already are implemented, but all they are submitted to target parameters IMEI and IMSI checking.

GPS tracking is a reliable entry point to start spying. It uses NMEA protocol. Once when data about movement is collected and stored for a given time period is possible to allocate target most preferable places as coordinates.

Usually, they are the workplace, living place and others such as public transport itinerary, preferable pubs, fitness etc.

GSM networks use the IMEI (International Mobile Equipment Identity) number to identify valid devices and IMSI (stands for International Mobile Subscriber Identity) and is a unique number assigned to the SIM card used by the mobile device. Both they are currently used and, on the focus, spying given target.

IMEI as a unique parameter is associated with each device. In this way, the devices can be physically distinguished and

https://doi.org/10.47978/TUS.2021.71.02.009

identified. They are a string - usually 14 characters, there are those with 15 or 16 sometimes. These additional numbers in the string are used to store the checksum and software version. The standards for this parameter after 2004 brings additional clarity. An IMEI is a collection of numbers, usually grouped as follows: - two digits, six digits, six digits, one digit and another digit with values respectively for the device manufacturer, device model, batch number and checksum - to prevent incorrect IMEI parameter. The first two parts related to the manufacturer and model are known as the Type Allocation Code (TAC). What is important is that the IMEI parameter is uniquely associated with the device. Therefore, when replacing the device, a new mobile service card can be identified. This affects traceability, which is important in espionage. Typically, tracking systems are able to detect replacement at any time on the device. A guarantee that this is possible are well-calculated sampling times over time, as well as the implemented calculation algorithms. When this is not done, for example, if data is tracked for a longer period of time, a possible replacement of the device by the user would be possible.

IMSI is a parameter that is also a string, usually numbers and used for identification. It is connected to data about the network and the service provider. The two parameters IMEI and IMSI are important and sufficient for effective identification of a user. Replacing a device or mobile service provider is not enough to interrupt to avoid a potential tracking process (legal or unregulated). Spyware vendors know how important it is to have time for new user data to be collected. It is usually very small. Less time required to replace a device or SIM card by a skilled user. Otherwise, spyware does not meet the requirements of efficiency today.

II. TARGET LOCALIZATION

At the beginning Target must be accessible. Additional hardware is needed. It replaces portion of the wireless chain. Usually some working place, living place and some possible entertainments are enough. Then start process to seek about target conversations. Entry point can be given conversation or part only using given word or phrase. As important parameters are used IMEI, IMSI and NMEA protocol data. Multithreading procedures currently check them, inside selected conversations to find the target correlation.

III. TARGET PRESENTATION

Tracking GPS and use NMEA provides opportunities for receiving and permanently storing data from which the location of a mobile device can be reproduced. Part of the structure involved in communications is replaced (Fig. 4). For this purpose, additional hardware imported into the communication chain is used. A certain perimeter geographical area remains under its control and all mobile devices that fall within this perimeter can be visualized and remain potentially under control. An available database of unregulated devices can be enriched with additional information, while using other data; non-GPS data, such as call participants, SMS recipients, and more.

All parameters are stored in Data Base and can be reused later. Data collection uses NMEA protocol about given target are shown at Fig. 3.

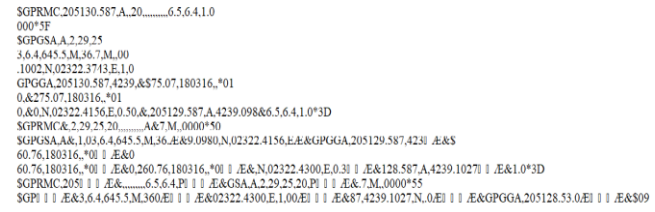

Fig. 3. Data collection uses NMEA protocol

This information is transmitted periodically; in this case the protocol used is GTGGA containing the coordinates for a given time. In this way, the movement of a subscriber can be reproduced late (Fig. 4). The Google Maps API can be used for this purpose. Thus stored, this information can be further processed to retrieve additional parameters. There are also methods for unauthorized access, which cannot be avoided except by excluding the scope of the selected subscriber.

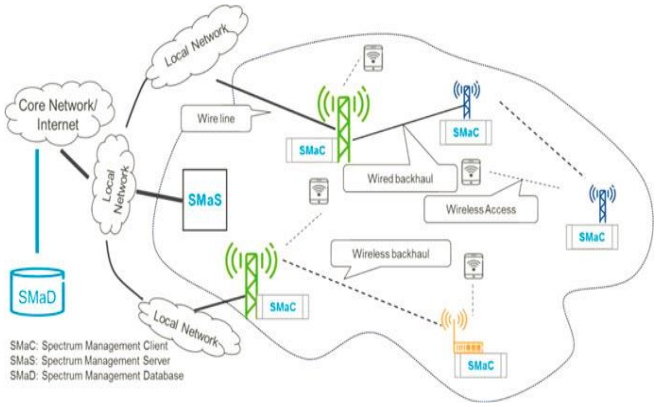

Fig. 4. Subsequently reproduction of the movement of a subscriber

Target location information using the NMEA protocol can be used to visualize it. The Google API is used for this purpose (Fig. 5).

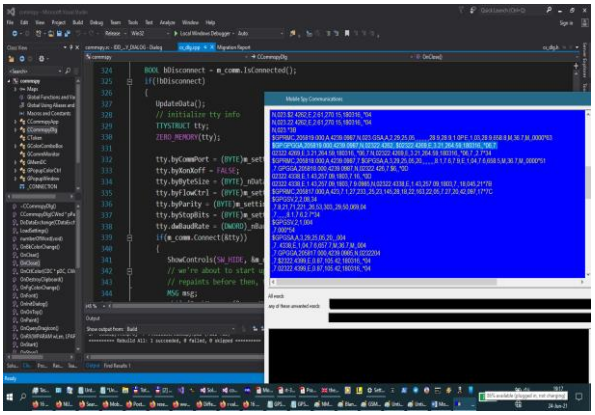

Fig. 5. The Google API

For this purpose, a dialog application of C ++ and Visual Studio 2019 was created and controls from Microsoft Foundation Class (MFC) were used. An Access database stores information about traceable subscribers. More important parameters are the coordinates and time, which are later used to illustrate the movement of a traceable object. Graphic files containing the illustrated movement are also stored in the database and can be used for additional research –

frequency or repeatability of movements, correlation with other traceable persons, etc. (Fig. 6).

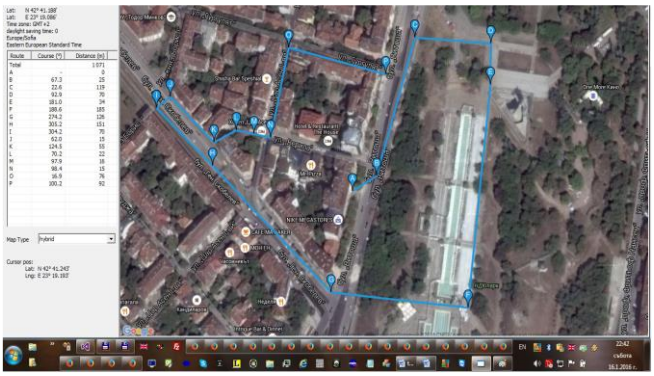

Fig. 6. Correlation with other traceable persons

Functions for tracking conversations of certain subscribers are also implemented - correlation using HLR [3, 7, 9]. Home Location Register (HLR) is a database that contains data regarding authorized subscribers using a global system for mobile communication (GSM) core network. The home location register stores information ranging from phone numbers to current location of the subscriber. Some data contained in the home location register include the mobile Station International.

More information about the details is published and discussed in [4, 5, 6, 8].

IV. Mobile Monitor

Usually almost all IM apps (such as Viber, Skype, AOL, WhatsApp and many more) are tractable. The SMS messages are also tractable. Also the app usage, the website history, and more are typical spying style. The user activity is another easy to track and use data (for example Tinder and Instagram (!), as a result - direct control to parameters, stored usually for given user means to be able to be observed remotely. Company policies for using certain applications can be entry points and future new action tracking data. There are many applications that can be used for unauthorized collection of user data. Such information can be very efficiently used to further process and easily use sensitive data for users. The information containing personal data is a commodity and it has been successfully sold. There is already a tendency for companies and consumers to ensure their security. The priority for security is as high as the cost of cyber security. The use of new technologies and protocols and not so new, but not so popular additionally brings security difficulties, because breakthrough opportunities are added. The need for new solutions to maintain security is constantly growing. Some features already implemented at the most used spy apps are shown below. They still are currently important. (Fig. 7).

What is Mobile Monitor

Mobile Monitor records a broad array of cell phone and tablet activity (see features below). Mobile Monitor never requires jailbreaking or rooting and installs in 5 minutes or less. All recorded data is sent to a secure web based location which allows you to review employee activity from any internet connected computer.

FEATURES

	iPhone/iPad	Android
	Add To Cart	Add To Cart
Tamper Proof	✓	✓
View Activity Remotely	✓	✓
Alert Word Notifications	✓	✓
24/7 Support	✓	✓
Website History	✓	✓
Viber	✓	✓
Skype	✓	
Kik - ***New!***	✓	✓
Tinder - ***New!***	✓	
Photos	✓	✓
SMS Text Messages	✓	✓
Call Log History	✓	✓
App Usage - ***New!***	✓	✓
Geolocation	✓	✓
Instagram		✓
WhatsApp - ***New!***	✓	✓

Fig. 7. List of applications or user parameters for spying

V. Conclusion

There are many applications that directly track the work of an employee's data. They are used for spying and gathering information. It can be further processed. Even with only the use of relatively simple algorithms, as a result, a large amount of additional information can be created with great reliability for a user using prediction and even though no real data is collected. Control in public networks is necessary and important, but the existence of data collection and processing capabilities in information technology that are available to users also introduces complications. An example of this is even a network protocol such as Simple Network Management Protocol (SNMP), which uses Management Information Base. The ability to use data about system software and hardware used may be a security breach or a potential entry point in the future to collect new data about a user or company.

In this study, we do not discuss the software we create, but we would like to draw attention to the possible consequences of such software when using relatively simple algorithms and affordable software.

As a result of policies on popular websites and applications, in particular, concerning social networks, e-commerce, as well as news portals, an increasing amount of consumer information is being processed.

Thus, the guarantee of whether and to what extent information from conversations can be separated from its context and how this can be used remains undefined.

There are many examples of this - the integration of applications such as WatsApp with Facebook, storage and processing of data from popular translation websites, increased cookie restriction and the use of more information, etc.

In recent years, there have been changes in scenarios for creating a separate account when registering.

They affect complementary new data and relationships with pre-existing ones, such as the mandatory addition of a telephone.

There is also a tendency for an increased minimum required amount of personal data.

In recent years, such trends have become increasingly relevant and also affect legal issues that await solutions in the European Union.

REFERENCES

[1] Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley "Network Security Bible" Wiley Publishing, Inc. Indianapolis, IN 46256 USA.

[2] Shahriar Binjani "Mobile communication security", Informatics School, Edinburgh University, 2012 UK

[3] Jochen H. Schiller "Mobile Communications" Second Edition 2003, London UK

[4] Published in the United States of America by IGI Global Information Science Reference (an imprint of IGI Global) Dark Web: Breakthroughs in Research and Practice Hershey PA, USA 17033

[5] Joseph Migga Kizza Guide to Computer Network Security Third Edition 2015, University of Tennessee, Chattanoo

[6] Alexander Kukushkin "Introduction toMobile Network Engineering" 2018 John Wiley & Sons Ltd

[7] Iosif I. Androulidakis "Mobile Phone Security and Forensics" A Practical Approach, Second Edition, Springer 2016, https://doi.org/10.1007/978-3-319-29742-2

[8] Tim Speed, Darla Nykamp, Mari Heiser, Joseph Anderson, Jaya Nampalli "Mobile Security: How to Secure, Privatize, and Recover Your Devices" Published by Packt Publishing Ltd. 2013, Birmingham B3 2PB, UK. ISBN 978-1-84969-360-8

[9] Hakima Chaouchi, Maryline Laurent-Maknavicius "Wireless and Mobile Network Security" John Wiley & Sons, Inc. Hoboken, NJ 07030 US