Establishing a stingray proof connection for the exchange of medical files

Akhil Madamala [1] H.Parveen Sultana [1]
[1] VIT University, Vellore 632014, India

Akhilmadamala701@gmail.com , hparveensultana@vit.ac.in

abstract:

Last year, out of the blue, the medical field experienced more attacks than any other field. It is bound to repeat as per the ID Theft Center. While the medicinal services industry experienced identify fraud in availing health care services; it is still yet to deal with the threat of hackers. Since the technology came late to the medical industry, the threat of identity thieves doesn't seem to go away any time. the personal medical files are made use of by a wide range of criminals. these medical files bid for higher prices in the black market than the financial information. From the security view, these conditions make accessing medical files through mobile a difficult task.

This paper aims to provide a concept to mitigate one of the most popular and common attack known as IMSI attacks

Introduction:

The immediate need for attention:

Electronic health records are anticipated to develop over 7% a year, as per a February Accenture report. In the meantime, information exchanges for medical coverage through the Affordable Care Act trades this year numbered eight million. It is vital to protect your reports since That data incorporates all the sensitive information. Hackers of such information can sell it to fraudsters—not only the individuals who need to execute medicinal misrepresentation.

Thieves could, of course, use a credit card or Social Security number from a medical file to commit not only financial fraud but also to sell useful parts to the black-market parties interested, who can exploit them in a variety of ways.

For instance, Fragmentation of information within the industry. If you visit the emergency room, the hospital will have one health record, while the ER will have another. Since ERs aren't necessarily owned by hospitals, if you go to the hospital after that, it may also create a new file on you. As result, there is a possibility of getting wrong medication for treatments, which can be life threating. The sheer number of attacks last year makes this fact more obvious. Moreover, the security of health industry lags far behind. Though the Affordable Care Act is disputed by many; analysts believe that it can reduce this threat slowly but surely. In 2013 Ponemon Institute study on records data fraud, just 36% of such casualties acquired out-of-take costs, those that did paid out $19,000—much more than the $50 liability limit for

deceitful Mastercard charges. victims whose professions needs them to pass the medical tests can lose their employments.

Literature review:

The network has cells connected by a fixed-location radio transmitter and receiver, a Base Transceiver Station (BTS) to identify the base station, it has a unique Base Station Identity Code (BSIC) and frequency specified by Absolute Radio Frequency Channel numbers (ARFCN) and it gets updated when the cell is connected with a new cell with a different location area code. the BTS can ask for the MSs unique identifiers (IMSI, IMEI), by sending an Identity Request. since the GSM can only authenticate in one way, the mobile has to authenticate to the base tower and this weakness is taken as a advantage by the hackers.

The following are some of the technologies available in the market and brief description of their functioning

SGP Technologies' Blackphone
The Blackphone is a security-improved cell phone created by SGP Technologies, a collaboration between ween the Spanish cell phone organization, Geeks Phone, and the encoded interchanges firm, Silent Circle. The Blackphone keeps running on an Android-based restrictive Private OS and courses portable interchanges utilizing VoIP through a Virtual Private Network (VPN) for extra security, supporting 2G, 3G and 4G groups. It offers a packaged suite of Silent Circle security applications that permit different capacities, for example, voice or video calls or encoded content informing.

XCell Technologies:
XCell Technologies, situated in Geneva, essentially creates Stealth Phones with a wide range of security highlights. The essential telephone warns the client to adjacent interceptors (IMSI catchers) and call capture attempt while the most powerful telephones take into account dynamic IMEI changing to avoid tracking. Its telephones territory from €400 to €80

Snoopsnitch:

Snoopsnitch is imsi catcher app that is developed on the platform of android by Security Research Labs, a German firm founded by Karsten Nohl.it is available free on play store. its minimum requirements in a smartphone are have Qualcomm chipsets and root privileges available.

The app "collects and analyzes mobile radio data to make you aware of your mobile network security" and warns users when it suspects IMSI catcher activity and other mobile threats, but it is not able to restrict mobile from connecting to IMSI catchers. Snoop Snitch also allows users to draw on the data collected in the GSM security map and to contribute their own data to the map

CatcherCatcher was the Security Research Labs' olderversion to SnoopSnitch . even though can detect IMSI catchers, it was only available on mobile phones with the OsmocomBB software, which greatly limited the models of phones that it could be installed on (only a few versions of Motorola, Sony Ericsson, and some other models) .

Android IMSI-Catcher Detector (AIMSICD) is an free project by SecUpwN and started in 2012 . The app is still in development and has only implemented a handful of detection mechanisms, including the cross-checking of CIDs. It aims to expand its detection indicators to eventually

ZIPS (Zimperium Intrusion Prevention System), it detects and prevents man-in-the-middle attacks. Zimperium initially raised $8.0mm from Sierra Ventures in December 2013. In July 2014, this is the first company to offer enterprise-level security software for iOS devices.

Pwnie Express' Detector

Recently it was put forward on April 20, 2015, at the cryptography RSA Conference in San Francisco, it can detect a wide range of network threat from cell jammers to imsi catchers.
Pwnie Express is still in the process of refining the heuristics it uses to detect rogue and malicious cell towers and reducing the occurrence of false positives.
Since the prototype was only announced recently, little is known about the extent or effectiveness of its detecting capabilities.

SBA Research's IMSI Catcher Catcher

SBA Research, a joint academic research center based in Vienna, announced a prototype stationary IMSI catcher catcher in August 2012 . The device is designed using a Telit modem without a SIM card and a Raspberry Pi Linux computer, costing about €100 in parts. It was capable of detecting between 270 to 400 base stations in the center of Vienna, and approximately 20 to 30 such devices can cover an area of 20 km. The laboratory results of the use of the device is still pending.

Open-source Portable-IMSI-Catcher-Detector

An open-source project to create a portable, ARM-based detector, Portable-IMSI-Catcher-Detector, also exists. However, the project is still in its "very early stages of development" and is incomplete.

There are three modes of encryption for a GSM network: A5/0 – which is no encryption – A5/1 and A5/2. Both of them failed as early as 1999 and A5/2 was formally abandoned in 2007 due to its weakness.

Proposed methodology:

Smart phones today are already equipped with a fingerprint scanner, which can be improved by incorporating the pattern of vein behind the skin, and some devices even include iris scanner which makes the dream of privacy achievable more than ever. Even though users cannot access their medical records now directly through their smartphones the following frame work forms a iron clad defense and aims to change this and tries take the initiative in achieving this.

In First step, the user might be prompted to authenticate using finger print, which can be verified with the existing one in the database. Next, it can also include security questions and a photo capture option for the second human review for accessing more sensitive information than usual. In the next step, the problem is to establish a channel which is safe from IMSI attack

Every mobile usually is in sync with six strongest base stations and a calculation is done based on the loss parameter and selection parameter with is done every 5sec and base station switch is done, when value of selection parameter is more than the respective value of the current base station.

Stingray, the common term used for IMSI attacks, operates in two mode the active and the passive mode. In the passive mode, it is able to receive and analyze signals being transmitted by mobile devices and wireless carrier cell stations and in active mode will force each cellular device in the threat area, where the duplicate base tower is, to disconnect from its usual service provide base station and establishes a new connection with the attacker. then, it broadcasts signal that is stronger than the signals sent by legitimate cell sites operating in the area.so in order to curb this and keeping in the view of other usual behaviors, our idea is designed.

Our algorithm for establishing a secure channel involves cross-checking of CIDs collected by the phone against public base station databases which can be done by getNeighboringCell() and a table is maintained in the mobile and is updated in the cloud.it also checks for “changing LACs”.in the background, it monitors the receipt of silent SMS and displays information about the status of network connections

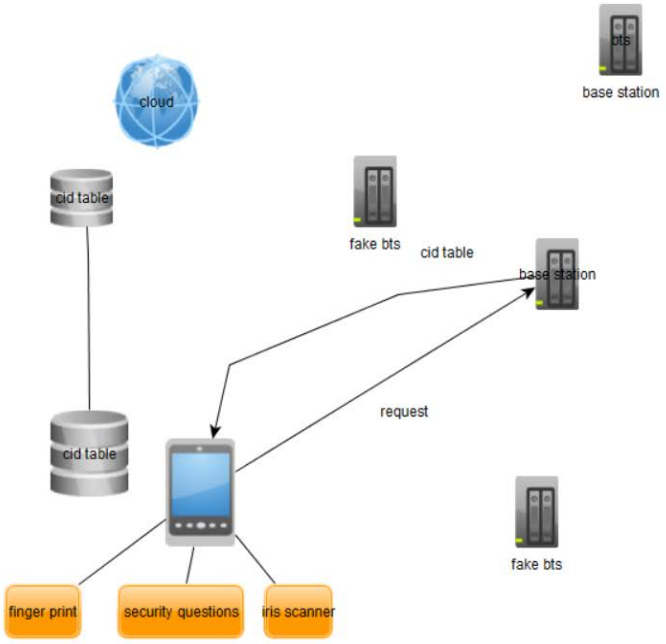

Figure 1.1 shows communication between mobile and bts Authentication at the mobile station is done by either of the two methods and Mobile station requests the base station for cids using getneighboringcell() command.

Here for calls, a new key exchange is generated for every call. For SMS, the initial key exchange is stored securely on the phone and used through means of a hash-chain. Usually the Cell towers that do not have a distinguishing or a fake CID have the following indications

- Cell towers with a fluctuating signal quality
- When the phone's encryption is deactivated
- When the PDA unexpectedly changes from a 3G or 4G system to a 2G organize
- When I/O gadgets are enacted through baseband without guidelines from OS
- When telephone makes suspicious associations in spite of no client action or progressing updates
- When the phone tower does not give a table of "neighboring" cell tower

When the mobile experiences any of the cases stated above, a warning is given to the user stating that the channel is not secure and, it is automatically disconnected from the base tower

The system also monitors the receipt of silent SMS and displays information about the current status of the network and, sometimes warns if the usual base transceiver (BTS) towers are not used or connected and lets the user choose the option. The case is illustrated in the below case.

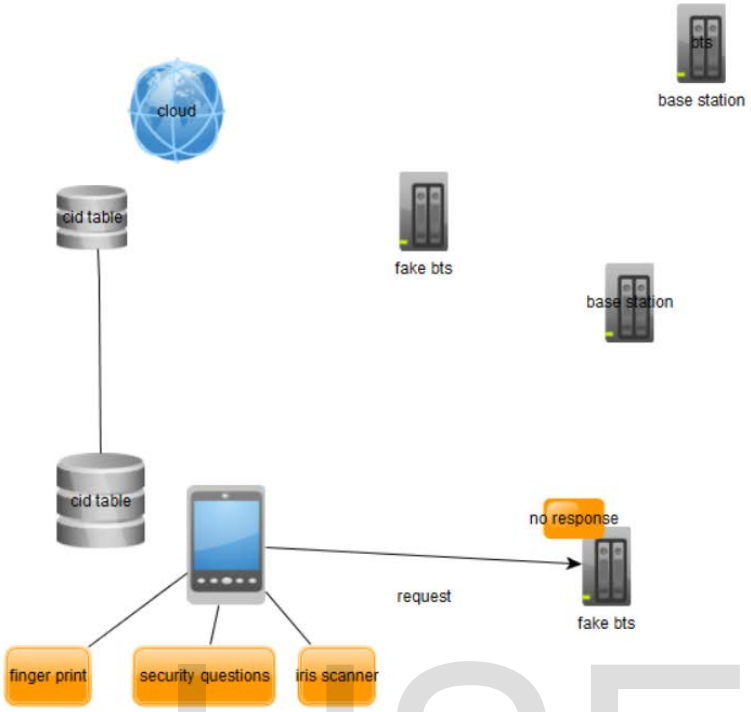

Figure 1.2 shows communication between a fake base tower and mobile.

In the above case illustrated by the diagram above , Mobile station requests to base station for CIDS using getneighboringcell() but, fake tower doesn't reply but, instead emits a strong signal subtly to direct a unprotection mobile station to establish the connection.

Conclusion:

The system relentlessly, with the frequency set by the user or the preinstalled profiles selection by the user like high security, moderate security or battery saver the frequency is decided and checks all the messages, calls and usual channels to make the connection as secure as possible. The proposed model has many heuristics that attackers commonly use and even if any one of the cases are satisfied. The model prevents the connection to the base tower even, when there is a strong signal. It also maintains a database in the mobile station as well as the cloud by only synchronizing when connected to the home base station in order to detect unusual activities that is to increase the probability of detection

Future work:

The proposed methodology can have other heuristics as long as they can keep the fault to genuine detection ratio to the minimal and cloud database as it gets bigger with the data from large number of users can have hashed values in the cloud for the effective management to facilitate security as well as easy management. In order to increase security we can use BLADE DATABASE data base for automation of data without human intervention i.e. we do not need to add staff to manage it.

References:

1.Andy lilly, armour communications on *IMSI catchers: hacking mobile communications.*

2. Mesud Hadžialić, *Member, IEEE*, Mirko Škrbić, Kemal Huseinović, *Member, IEEE*, Irvin Kočan,Jasmin Mušović, *Member, IEEE*, Alisa Hebibović and Lamija Kasumagić on an *Approach to Analyze Security of GSM Network.*

3. https://en.wikipedia.org/wiki/Stingray phone_tracker.

4. Ravishankar Borgaonkar, Andrew Martin Department of Computer Science University of Oxford Shinjo Park, Altaf Shaik, Jean-Pierre Seifert TU Berlin & Telekom Innovation Laboratories on *White-Stingray: Evaluating IMSI Catchers Detection Applications.*

5.https://www.wired.com/2017/03/medical-devices-next-security-nightmare/.

6.https://www.networkworld.com/article/3212991/internet-of-things/iot-security-for-healthcare-is-in-critical-condition.html

7. https://ytd2525.wordpress.com/category/mobile.