Wardrive - "Are You Being Intercepted?"

Suresh Koppisetty, Sanil Sinai Borkar
CISE Department, University of Florida

Abstract

GSM standards mandate every cellphone to be 2G backward compatible, thereby making it the "weakest" target in the GSM security model. Many rogue base stations exploit this vulnerability by downgrading the user's cell network to 2G without their knowledge. We seek to wardrive the GSM networks by identifying the illicit cellular base stations. Our Android application provides a tool to identify the presence of a rogue base station, if any of the users were connected to it.

Introduction

- The security protocols for GSM have not been upgraded thereby making cellular networks vulnerable to security breaches.
- This major loophole can encourage an attacker to intercept voice and data information being transmitted to and/or from a GSM mobile device. International Mobile Subscriber Identity (IMSI)-Catchers (IC) do exactly the same thing. They act as a "Man-In-The-Middle" and eavesdrop on phones.
- Some "intelligent" IMSI-Catchers can downgrade the mobile device to use A5/0 cipher (no encryption) thereby making it a target for eavesdropping.
- A German company GSMK built a commercial IMSI-Catcher-Catcher (ICC) - "Cryptophone" - amounting to nearly USD $3,500 per piece.
- Our Android application will soon be available on Google Play Store, and could be downloaded by anyone to verify if they are connected to an IC.

Assumptions & Limitations

- Lists provided by [1] and [2] are exhaustive
- Currently, the application is available only for Android

System Architecture

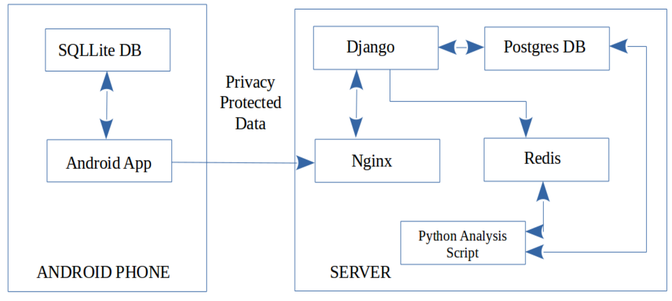

Figure 1: System Architecture

- The Android application is installed on phones to collect cellular network information
- All the data collected is stored locally on the phone, and then sent to the server after privacy protecting the PII data using HMAC-SHA1 (on every Cell ID change)
- This data can be displayed on the phone as logs (as per the user's request)
- Data is pushed to the server periodically or when an Internet connection is available
- A web-page lists out all the information of "unregistered" base stations from amongst the data collected

Experiments

- The application was installed on some Android phones in Gainesville
- Collected more than 20K data records within 15 days, more data being collected
- Analysed the data collected so far for any anomalies or abnormalities

Results

- In a typical scenario, a single cell phone collects cellular data at the rate of 30 data records per hour
- *Gainesville, FL*: One of the test phones subscribed to T-Mobile was found to connect to AT&T in nearly 5-6 separate scenarios, in places where T-Mobile had high network coverage.

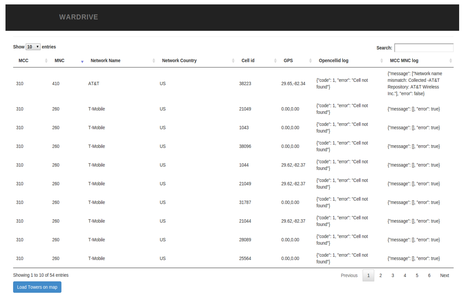

Figure 2: List of "gray" cell towers in Gainesville

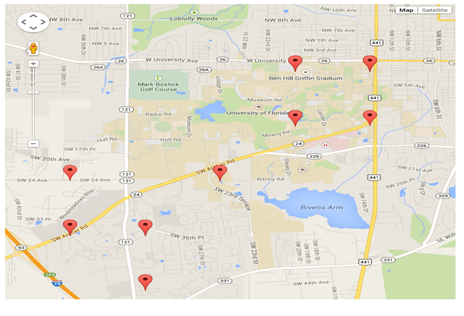

Figure 3: Wardrive of "gray" cell towers in Gainesville

Conclusion

- Although the T-Mobile phone was connected to AT&T, it does not indicate the presence of an IMSI-Catcher.
- Our assumption was wrong: Cell tower list in [1] is not exhaustive - there may be genuine cell towers that show up as "unregistered".
- We were not able to find any rogue base stations in Gainesville. However, once we try to gather more cellular data across state boundaries and geographies, we may get close to finding one.

Future Work

- Collecting low-level details regarding cellular network information for in-depth analyses
- Finding user-related trends in the data to draw conclusions

References

[1] Crowrd-sourced Cell ID Database.
`http://opencellid.org/`.

[2] Updated List of MCC and MNC Codes.
`http://www.mcc-mnc.com/`.

[3] Swati Khandelwal.
Fake Cell Phone Towers Could Be Intercepting Your Calls.
`http://thehackernews.com/`.

[4] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl.
IMSI-Catch Me If You Can: IMSI-Catcher-Catchers.
ACSAC 2014, December 8-12 2014.

[5] Patrick Traynor, Patrick McDaniel, and T. La Porta.
Security for Telecommunication Networks.
Springer, 2008.

Acknowledgements

- Professor Patrick Traynor
- Bradley Reaves, Georgia Institute of Technology
- CISE Department, University of Florida