Cellular Infrastructure Monitoring

Sanil Sinai Borkar, Suresh Koppisetty
{*sanilborkar@ufl.edu, sureshk@ufl.edu*}

October 8, 2014

1 Related Work

Global System for Mobile Communication (GSM) is the default and widely used standard for mobile communication in the world today [1]. It is a standard to describe protocols for second generation (2G) digital cellular networks used by mobile phones. Unfortunately, as we have upgraded to higher generation of digital cellular networks, the security protocols for this widely used standard have not been upgraded thereby making cellular networks vulnerable to Distributed Denial of Service (DDoS) attacks and other security breaches [2], [3], [4].

This major loophole can encourage an attacker to take advantage of the flawed GSM security, and intercept voice and data information being transmitted to and/or from a GSM mobile device. IMSI-Catchers do exactly the same thing — they act as a "Man-In-The-Middle" (MITM), and eavesdrop on phones [5]. The IMSI-Catcher gets its name as it retrieves the International Mobile Subscriber Identity (IMSI), which identifies each subscriber uniquely, from the compromised mobile device. IMSI-Catchers have been around for nearly 2 decades now but some really interesting and significant work has been done in the recent years.

One of the first significant contributions was made by Chris Paget wherein he built an IMSI-Catcher using an USRP and free open source softwares such as GNU Radio, OpenBTS, and Asterisk. He presented and demonstrated it at DEFCON 2010 [6]. In this demonstration, nearly 24 of the attendees were connected to his "fake" base station. If they would make a call, they would hear an automated message notifying them of such a "fake" connection.

Taking a step further, Karsten Nohl explained and demonstrated how the GSM cipher suite viz. A5/1 can be broken [7], [8]. Later that year, he and Sylvain Munaut presented practical snooping attacks on A5/1 protocol by using special tools (like AirProbe [9], Kraken, Toast [10]) and custom firmware on a modified mobile phone [11]. However, this method can eavesdrop on a small number of freqeuncies at a given time, and is likely to lose the acquired phone once frequency hopping is used extensively during the calls. Although this explains the fundamentals of call interception in GSM, an attacker will resort to a much higher yielding IMSI-Catcher. For instance, some "intelligent" IMSI-Catchers can downgrade the mobile device to use A5/0 cipher (no encryption) thereby making it a target for eavesdropping [12].

Recently, a German company GSMK built a commercial IMSI-Catcher-Catcher (ICC) which is a device that detects an IMSI-Catcher. This ICC, called a "Cryptophone" [13], [14], is built on top of standard mobile devices like Samsung Galaxy S III and Samsung Galaxy S4. This customized "Crytophone" protects the data in your phone as well as the data that is being transmitted from your phone with the help of strong encryption methods viz. AES-256 and TwoFish [15]. This phone is a practical but expensive ICC amounting to nearly USD $3,500 per piece.

Working on the same lines as the "Cryptophone", this year, a team of researchers from Vienna built a low-cost ICC that could actually detect if your phone was trying to connect to a fake base station [5]. They built two types of ICCs — a stationary one that was installed on top of some buildings in Vienna, and a mobile one that was installed on a mobile device [16]. The mobile application could detect if the phone was trying to connect to a fake base station and warn the user accordingly with some notifications on the phone itself. Using this setup, they collected a dataset of nearly 40 million records but no concrete evidence of the presence of IMSI-Catchers was found.

Although the ICC built above does most of the work we are trying to do, it does not encompass all the requirements of our work. In addition to retrieving the cell and the cell tower information, we would want to store this data for further analysis. After a thorough analysis, we could come up with certain steps that could be taken to secure the data transmission from phones. Moreover, our mobile application would be available on the Android Play Store so that it can be downloaded by anyone and everyone for their own benefit. We can then take on these IMSI-Catchers on a global scale thereby defying their purpose.

References

[1] "Wikipedia," http://en.wikipedia.org/wiki/GSM, accessed: 2014-10-06.

[2] P. Traynor, P. McDaniel, and T. La Porta, "On Attack Causality in Internet-connected Cellular Networks," in *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, ser. SS'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 21:1–21:16. [Online]. Available: http://dl.acm.org/citation.cfm?id=1362903.1362924

[3] W. Enck, P. Traynor, P. McDaniel, and T. La Porta, "Exploiting Open Functionality in SMS-capable Cellular Networks," in *Proceedings of the 12th ACM Conference on Computer and Communications Security*, ser. CCS '05. New York, NY, USA: ACM, 2005, pp. 393–404. [Online]. Available: http://doi.acm.org/10.1145/1102120.1102171

[4] P. Traynor, W. Enck, P. McDaniel, and T. La Porta, "Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks," *IEEE/ACM Transactions on Networking, Vol. 17, No. 1*, Feb 2009.

[5] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," *Annual Computer Security Applications Conference (ACSAC) 2014*, December 8-12 2014.

[6] C. Paget, "Practical Cellphone Spying," Las Vegas, NV, 2010.

[7] K. Nohl, "Breaking GSM Phone Privacy," Las Vegas, NV, 2010.

[8] ——, "Attacking Phone Privacy," Las Vegas, NV, 2010.

[9] "Airprobe - How To," https://srlabs.de/airprobe-how-to/, accessed: 2014-10-04.

[10] "Decrypting GSM Phone Calls," https://srlabs.de/decrypting_gsm/, accessed: 2014-10-04.

[11] K. Nohl and S. Munaut, "Wideband GSM Sniffing," 2010.

[12] P. Traynor, P. McDaniel, and T. La Porta, "Security for Telecommunication Networks," Springer, 2008.

[13] A. Soltani and C. Timberg, "Tech Firm Tries to Pull Back Curtain on Surveillance Efforts in Washington," http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html, Sept 17, 2014, accessed: 2014-09-20.

[14] S. Khandelwal, "Fake Cell Phone Towers Could Be Intercepting Your Calls," http://thehackernews.com/2014/09/fake-cell-phone-towers-could-be_4.html, Sep 4, 2014, accessed: 2014-09-15.

[15] "Gesellschaft fr sichere Mobile Kommunikation mbH (GSMK) - Cryptophone," http://www.cryptophone.de/, accessed: 2014-09-20.

[16] A. Dabrowski, "Digital Self-Defense in Mobile Networks," Mar 18, 2014.