Cellphone Data Stealing

Thomas Lux

November 25th 2013

Introduction

In our modern day network of cell phones and towers, we get to enjoy seamlessly rolling from one cell tower connection to the next without ever dropping a call. As impressive as this on-the-go hand off is, the need to search for cell towers can actually prompt your phone to send data to anonymous sources. Cell phones are programmed to automatically search for, find, and connect to towers. A 'ping' that is sent as frequently as every 7 seconds [1] often contains data that can be used to compromise personal information of the cell phone user. Knowing that cell phones must perform the task of searching for towers, there is a strong need for a secure way to about this search. In this paper we will explore the concept of making this search process more secure after first understanding how this came to be a problem. This includes knowing how towers connect to cell phones, and the impact users will face if the connection process is left insecure. If you would like a more in depth history of how cell phones have developed over the years, you can see [4].

Connecting to the World

Cell phones are an amazing technology. They have provided us with a new level of connectivity, and they have grown in popularity immensely over the past years. Now, it is to the point where upwards of 90% of adults in the United States own at least one cell phone [1]. Across the world, as many as 3.3 billion people use some sort of mobile (cell) phone [6]. As we begin to analyze how massive our cell networks must be, we find some

simple flaws and limitations of this technology that we've nearly become dependent on.

To start, we can look at how the cell tower network is designed. One cell tower has approximately a range of 10 square miles. Each tower also has around 832 different frequencies it can use to broadcast and receive. Each cell phone takes two signals, one for transmission and one for reception, leaving us with half the original number of frequencies per tower. If two cell phone transmissions are on similar frequencies, the messages often get distorted. Given this, two adjacent cell towers are not able to use frequencies that are exceedingly similar. Now, after accounting for all the necessary circumstances we've limited the number of separate cell phone users to which one tower can connect to be about 56. [2] What we find is that there ends up being a very dense network of cell towers, and transfers between them must happen very frequently.

Devices that can trick your phone

Since cell phones spend so much time switching from tower to tower, they must constantly search for the next available frequency while on the move. This process of searching for towers in cell phones is a point of insecurity. When mobile phones find a tower, they immediately send information regarding their unique ID, and a variety of other private information. One of the devices that is capable of 'tricking' a cell phone is called the **Stingray**. This device emits a signal that cell phones mistake for a tower and then receives all of the cell phone's identification information. [5] This device is not the only of it's type. It and its siblings are frequently utilized by law enforcement agencies for the tracking of individuals. Most of the problems that are introduced by these pieces of equipment are regarding personal privacy. As to date, there are not known ways to manipulate the cell phone information that is received into direct confidential personal information. This information does however provide relatively precise location estimations, allowing the user to be tracked. The tracking information is capable of locating users within a range of 150 feet [1].

How the tech works

Stingray is a box-like device that is also dubbed an "IMSI Catcher". The device sends out signals that resemble those of cell towers in order to get cell phones to try and connect to it. In this process, the cell phone sends the Stingray device it's International Mobile Subscriber Number and it's Electronic Serial Number possibly along with hundreds of other unique digital identifiers [5].

How this effects everyone

This hasn't become a very large issue in the eye of the public to this day. Although many people are concerned with breach of privacy, this is still not a flaw that many cell providers are intent on fixing. The main impact of this tracking technology currently is that it provides not only our government, but other governments as well, the ability to track people without their express permission. This topic is one that has been approached in more legal terms [3], but has yet to pass through true legislation. The primary legal issues are now switching from the cell providers to the government. Mainly, with devices such as **Stingray** and **Triggerfish** [5], 'fake' cell tower signals can be produced, bypassing the need for private sector cooperation in such acts.

Impact and Solution

This technology has the potential to change the way that cell phones connect to cell towers. Over the next few years it is very likely that legislation will be passed prohibiting law enforcement agencies from abusing cellular device tracking information. Also likely in the coming years is some sort of verification system when a cell phone connects to a tower. Once cell service providers realize they can advertise it as added security, it is likely that a system of verifications will be added to the tower connection process. The chances of this significantly decreasing the performance of the phone is highly unlikely since the task would only have to be performed on initial tower linking. Mobile security

in general has been a field slow to catch on. Many mobile (aka cellular) devices are still insecure, and put millions at risk of losing personal information [6]. Over time, this will change, but many small flaws like the lack of tower verification still crowd the platforms.

References

[1] Ronald Bailey. Your cellphone ls spying on you. *reason*, 2013. This person is very .. skeptical. Much of this paper seems distorted and non-scientific, but regardless there are some valuable ideas that can be taken. Much of the information regarding the functionality of cell phones and some of the tech specs seem reliable.

[2] JON CHOATE. Cell phone geometry. *Geometer's Corner*, n/a. A lot about the process of how cell phones connect to networks and how the networks of towers function. Interesting stuff for the technical side of phones.

[3] William Curtiss. Triggering a closer review: Direct acquisition of cell site location tracking information and the argument for consistency across statutory regimes. *Colum. JL and Soc. Probs.*, 45:139, 2011. This paper seems to be more focused on the actual legal side of cell phone tracking. Not as relevant to this project, but has some interesting information about what a cellphone can do that could be useful.

[4] Tom Farley. Mobile telephone history. *Telektronikk*, 101(3/4):22, 2005. History of the cell phone, cited by choatecell, so I'm just using a referred reference.

[5] Ryan Gallagher. Meet the machines that steal your phone's data, 2013. Main article of inspiration, has information of various spy tools.

[6] Henry B Wolfe. The insecurity of mobile phones. *Proceedings of Informing Science and IT Education Conference*, 2010. Opens with a mention of how few articles there are on cell phone security, didn't realize that's such a sparse topic. There is one paper that's mentioned in the citations as being really well collected. They also say that the topics mentioned in that paper are only a subset of the topics in this one. We'll see.