How a SIM card vulnerability can become a nightmare

Michael Guidry
Unified Defense Technologies, Inc.
12/13/16

Subscriber Identity Module (SIM) cards are ubiquitous. It is the invisible computer within all of our mobile devices, iPads, and even various products. It is used within government identification cards for computer consoles, and also some satellite connections. The smart card is also the technology behind recent credit card advancements in security as well. Smart Cards (aka SIM) are everywhere.

Underneath the surface of the SIM card there is a hidden vault holding keys relating to cryptography, and your subscriber identification aka phone number. It protects the data by using it in specific operations such as cryptography while protecting the real key information from leaking. I won’t go too far into the technical details of the SIM cards specifically but the vulnerability here would also apply to other security products, and possibly smart card uses.

Mobile phones are the cornerstone of the main technology required to do business in todays global economy. Companies like Uber, Facebook, Apple, and others rely almost solely on the mobile phone. If you consider recent statistics of user agents from various major companies then you will notice the graph increase of mobile vs desktop. This is also paired with the imaginary, or memory of people walking down a busy street recently. Everyone has mobile phones. In one form or another it has become one of the biggest tools for business in our modern age.

SIM cards for the majority of subscribers in first world, and other regions are usually manufactured by a small set of companies. This is important because the key information that is held relates to the subscribers account and it has ability for fraud if not handled properly. Gemalto handles a lot of manufacturing for many of the top telecoms. You can review information about the NSA stealing these keys which allows decryption of mobile phone session keys and allowing spying of conversations. It is important that the information is only held by the telecom, and the subscriber.

Ki keys are not available for reading from the SIM because that would allow someone to clone a SIM. In the past whenever phones didn’t carry a SIM card they would use their ESN (Electronic Serial Number) to authenticate to a telecom’s tower. This meant the data could be read out of the air using a tool called a GSM ‘snarfer.’ This allowed massive fraud, or spying on communications. It was also a lot harder to change numbers, and perform other activities.

In today’s world its very simple to swap a SIM card and then you are using a different providers network plus a different phone number, or account.   The ESN became the current IMEI (International Mobile Station Equipment Identity) and helps with forensics, and accounting in some ways. It was also widely used whenever Apple wouldn’t sell unlocked phones. The SIM is the important part that coordinates with the telecom to generate session encryption keys for placing calls, and data transmissions.

If you wanted to clone a SIM it wouldn't be as simple as putting it into a device, and then copying it to another SIM. This is because the SIM doesn't give you the internal key information but rather performs mathematical operations on a value that you give it. The tower will send a particular variable to the mobile phone, and it then communicates it into the SIM card, and uses the results. In the past people found cryptographically plausible methods to brute force the actual secret key (Ki) value. It would perform hundreds of thousands of cryptographic calculations on particular values that the application chose, and use them within analysis to break the code if you wish. This allowed writing the Ki to a new SIM card which would ultimately clone the original SIM.

The cryptographic algorithm had some weaknesses as well although a simple mitigation was put into place. The SIM card manufactures decided to limit the amount of these operations at around 65,535. This meant that if you attempted to use this brute force method that it would reach above this count, and destroy the SIM card. The newer cryptographic algorithms used may, or may not be stronger than the ones in place whenever the limitation was implemented although even the older one required hundreds of thousands. Case closed? They thought so.

What if you are not focused on cloning a SIM card but destroying it? You can perform a remote attack on the SIM card and ensure that it will destroy itself if you can control the phone performing those tasks. It might seem like an even more ridiculous task at first glance. It is however not as tough as it may seem. You don't have to attack the iOS, or Android operating system, or install an application. You have the power of the radio waves.

Historically it was expensive, difficult, or required a lot of technical ability to manipulate the radio frequencies around you. It is very simple to find cellular jammers, software defined radios, and other technology now. This creates a whole new attack surface that these technologies didn't consider whenever they were built.

In this case you can use an off the shelf, or eBay-able jammer to disconnect the mobile handset from its provider, and then allowing it to reconnect which will increase the counter by one. If your feel that this is a tedious task then you'll soon realize how much of a nightmare this is. You can easily build a small device, or buy one that can cycle power controlled by a Raspberry Pi, or other small computer which would allow you to automate this process.

Let's assume you are targeting an administrator of a company, and want to destroy the SIM before you attack the corporate network. This would block their SMS monitoring, or other applications from refreshing and possibly give you a good eight hours of exfiltration. You could even coordinate and target every administrator, or employee at once.

You could begin attacking the mobiles and if you began, and timed it correctly then you would ensure that their SIM is dead before they fall asleep allowing you to use the rest of the night to perform whatever duties your attack entails. This is only using an off the shelf power supply with a reed relay that is controlled by some pins from an Arduino, or Raspberry Pi. You would have to move it around, or plan it correctly.

If you used this simple trick then it would take roughly 18 hours. If you think that this is a long time then you could perform it only at night near their homes in a hidden manner, and split the 18 hours across several days. The important thing to remember is that this counter doesn't reset unless the phone is power cycled. You actually will have as much time as it takes, and if you perform the attack at their home then it wouldn't affect too many other subscribers. The phone would disconnect every few seconds while doing this. Thats an example of targeted, and yes it is illegal so you should understand that this is just an example.

It gets better… or worse? Let's say you wanted to target an entire region, or city. You could actually increment the counters of everyone near a tower on a mass scale. If you research into LTE then you will recognize that the handset will communicate with the tower using 1900 MHz to 1920 MHz. This is even easier than the commercial jammers. If you were to use a hack RF and create an application to focus, and cycle these ranges of frequencies in specific coordination then you could perform the attack along that entire cellular tower. If you wanted to be invisible then you would have to analyze the protocol and focus on various telecoms separately, or use other tricks to determine how often, or not to disconnect mobiles on a particular telecom. The point is that a $100 hack RF with any laptop available regardless of 2016, or 2010 could perform this attack.

Let's say a city has X towers, and you would like to perform the attack across the entire city in the most invisible way possible. It would take a hackRF ($299), any mobile phone (android rooted) even an older one ($50?-$300), and a battery pack ($50), or power outlet. This would allow you to create an application with specific timing which would disconnect all users near the tower using LTE at the same time. This is a small fee for such as massive attack.

If you wanted to create a small custom breadboard with an AttinyX5 MCU then you could modify a handheld cellular jammer with a reed relay to perform this attack anywhere at any time.

Do you feel that every telecom within a city has the ability, or inventory to replace every subscribers SIM card momentarily? I think that you may understand how big of a problem this vulnerability can be. It is also going to be an issue with the replacement SIM card as well.

This may even be possible to perform on these console identification cards. If you forced everyones console access card to be destroyed shortly after lunch then wouldn't that give you a lot of time to exfiltrate data without administrators being able to gain access to perform the duties required?

If you were to sit next to someone then you may even be able to destroy their credit card remotely using a similar concept. It opens a lot of opportunities where these cards, and similar limitations exist which could be used to destroy the Smart Card in question.

This is my first example of several which will express how security mechanisms actually become attack vectors.