Cellphone 'fingerprints' can stop criminal.

While cellphones have made our world smaller, they have expanded the criminal underworld. There are roughly 60 million cellphones being used in South Africa, eight million more than the country’s population. This means people own and use several phones, making it tricky for law enforcement to tell whether a phone is possibly being used for malicious activities. To make things worse, cellphones’ identities can be manipulated by criminals to increase their anonymity.

Cellphones normally prove their identity on a network by sending a key, which is a 15-digit number, that identifies them. But this key resides on the phone’s memory and can be easily changed, especially by criminals when they want to avoid being tracked and wiretapped, or when they don’t want phones they have stolen to be blocked off the network.

Most governments in the world have outlawed changing this key. South Africa, for example, passed the Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002, to attach a user’s identity to a cellphone when they purchase it. This was done in an attempt to reduce anonymity among cellphone users and to allow law enforcement to trace and track criminals via their cellphones.

But since it is possible to change the identifying key of a cellphone, criminals can co-ordinate criminal activities, ranging from kidnapping to rhino-poaching, without worrying about being caught. Research at the University of Pretoria’s electronic warfare department aims to address this problem by investigating a new method for identifying cellphones using an old military trick referred to as specific emitter identification.

Specific emitter identification allows cellphone networks to identify cellphones and their users in an interesting way: rather than reading a key encoded in a radio signal, it works by using the radio signal itself as the key.

The hardware components making up wireless devices differ slightly from device to device, even if they are the same make and model. These differences do not affect the operation of the device and are thus left in by the manufacturer, allowing them to manifest in the signals they produce.

These variations create unique patterns in the radio signal that can be extracted and used for identification.

Historically, specific emitter identification was used to identify and track enemy radars in the military. Now, it is being researched as a means of making wireless devices, such as wi-fi chips which are used in laptops, less susceptible to forgery. Applying this technology to cellphones is a new frontier in the research. A few institutes abroad have shown that it is possible to identify cellphones this way.

However, the research done by these researchers only investigates its applications to a few phones, most of which are not the same make and model. The research at the University of Pretoria, under the supervision of Professor Warren du Plessis, is trying to figure out if it is possible to identify lots of different phones of the same make and model.

It will also investigate whether a cellphone’s emitter signature is affected by the power and frequency channel it uses when transmitting a signal, and whether environmental conditions influence the cellphone’s emitter signature.

We plan to set up a proof-of-concept specific emitter identification system. This involves firstly acquiring and storing radio signals from a number of cellphones. These stored signals are filtered to remove unwanted noise in them. The filtered signals are then passed through a feature extractor, a software algorithm. The feature extractor serves to find unique patterns within the different radio signals. It does this by using statistics to calculate numbers that define the shape of a specific region of the radio signal.

We can then use this information to form a string of numbers, which are collectively referred to as a “feature vector”, which is essentially a fingerprint of the cellphone’s transmitter.

A database stores this feature vector or fingerprint together with a label of its associated phone so that it can be used later to identify the phone.

When a new cellphone signal is presented to the system, it undergoes the same process to produce a “feature vector”.

The system then matches this feature vector to the existing database of feature vectors and returns the label of the cellphone whose feature vector most accurately matches the newly formed feature vector. Should the proof-of-concept system consistently and correctly identify the cellphones, even those that are the same make and model, it will prove that it is possible to identify phones by specific emitter identification. Moreover, it will show that it is accurate enough to distinguish between same make and model devices and could supplant current identification methods.

If specific emitter identification proves feasible in the real world, it will make it significantly more difficult to change the identity of a cellphone: it ties a cellphone’s identity directly to its hardware, which is practically unchangeable.

This should in turn deter criminals from using cellphones to conduct their malicious activities as they are now more likely to get caught.

Should they decide to use some other wireless device to co-ordinate criminal activities, this technology can be readily adapted using the knowledge gained by the current research. Overall, the future looks dim for criminals who have been hiding behind their phones for protection.

23
Specific Emitter Identification of GSM Cellular Telephones
Importance of the project

Jeevan Ninan Samuel attends the University of Pretoria.