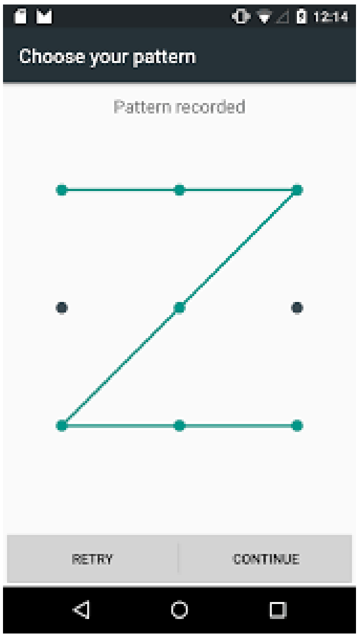
TASC talk presented by Dr Harin Sellahewa of Buckingham University

“Touch Gesture-based Authentication on Smart Devices: how secure is Pattern Unlock”



You know how difficult it is to sometime remember your passwords for the many smart devices you have. So, over some time developers have been trying to think of better and less stressful ways for you to access your devices without having a meltdown trying to remember these passwords or PIN numbers. Now as touch screen technology has improved greatly from its inception, gestures can be used to authenticate users on their devices, rather than passwords or PINs.

One of the problems with password and PIN authentication is that a significant number of people use “password” as their password or “1234” as their PIN number! Not very secure. People also sometimes write their password or PIN number down and keep it with their device. Also not very secure. There are other ways your devices can be hacked, one is by someone surreptitiously looking over your shoulder when you are typing in your code and then nabbing your device and using what they have learned to access your whole life story. Another way is to steal/borrow the device first then work out, from the finger print smudges on the screen, which are there because of you typing in your access code, what it is.

Using gesture Android mobiles, for instance, have a 3 x 3 grid of dots for you to program in a continuous path to transcribe every time you want to unlock your phone. The only problem is, research has shown, that most people start and finish on particular dots, top left and bottom right, and there are a limited number of paths that can be used to get from one to the other. So, in fact, using gestures works out at being less secure than using passwords or PINs. However by using the latest touch screen technology biometric information could also be used to strengthen this method of authentication. For instance by measuring the pressure and angle that some one’s finger makes when drawing a path between the points, and also detecting timings for their finger movement, greatly enhances the security.

Some of Dr Sellahewa’s students are currently investigating utilising these and other methods to increase the security of gesture authentication and are working with industry to see if these methods can be rolled out to all devices in the future. So far they have been working with only a small sample of users and devices but intend to widen their scope to also include measuring the differences between male and female users, old and young and left and right handed people amongst other factors.

To end the talk Dr Sellahewa brought along a Microsoft Hololens for us to experience. Apart from an initial difficulty in placing it on one’s head so that you could see the projected image on the built in screens, the Hololens was very impressive. The Hololens is an “Augmented Reality”, as opposed to a virtual reality, headset, so you can see through the display as if you were wearing a pair of specs. But the built in Windows 10 computer is able to overlay computer generated images on the “real” background. I can see that this device would be very useful in many engineering i.e. civil and construction environments, as well as for many design purposes. One thing I found that was really impressive was its ability to place virtual objects anywhere in the surrounding environment and for them to be positioned absolutely rock solidly, so no matter how you twisted and turned, those objects stayed exactly where you put them. You can even walk around and view the objects from just about any position. Definitely impressive, there are only two drawbacks that I can see currently. The first is the price, somewhere between two and four thousand pounds and the second being its weight and size, though both of these, I’m certain, will improve dramatically over time.

Marius Stuart