What biometric threats concern you?

Andrew Bud, CEO & Founder

Faces make wonderful security credentials. They are permanently attached to us. We carry them around with us at all times and they can't be stolen. But they can be copied. Our faces are completely public they're all over LinkedIn, they're all over Facebook, people can photograph us in the streets, they're in our identity documents.

So our faces are public, but the genuine face, well that's unique. So the key to using face as a security credential is to be able to distinguish the unique, genuine article from any kind of a copy. And today there are lots of ways of making copies and really we can divide them into two sorts. There are the artifacts, these are physical objects that an attacker will thrust in front of the camera of the device that they're using. And those physical objects can range from simple things like photographs that they printed out or high resolution pictures that they've put onto a high quality tablet. To something that maybe they've animated, maybe they've socially engineered and stolen a recording of the victim. Or, they've used modern synthetic imagery technology to animate a photograph and again, they've put it onto a high quality tablet, which they've put in front of the camera. Maybe they spent hundreds or perhaps thousands of dollars to make a mask of the victim. There's an artist in Japan who is making a profession out of producing quality masks that are exquisite in their precision right down to the poor structure of the user -works of art.

These all artifacts, which have to be crafted one by one. Traditionally one uses liveness technology to distinguish between these so-called presentation attacks and the real object. But then there's another class of attack, which is much more insidious, much more scalable, increasingly easy and low-cost to mount and therefore far more dangerous... and that's the digital injection attack. In a digital injection attack imagery that has been, say stolen during a social engineering attack or using deep fake technology synthesized so that it looks like the victim is moving and talking in a way that is indistinguishable to the naked human eye.

That imagery is directly digitally injected into the data stream fed to the face matcher and the genuine presence assurance system. And the horror of this is that it's missing all of those cues. All of those little signals that are created when a physical artifact is put in front of the camera, because there is no artifact, there is no camera.

This is a naked digital data stream. So it's much harder detect, and it's far more scalable. This can be mounted by banks of computers, feeding in tens of thousands or hundreds of thousands of attacks simultaneously in order to assure genuine

presence both detect against artifacts using liveness, and you have to defend against digital injection attacks using far more advanced technology.

And there were various ways of doing so there were biometric methods which look at the imagery itself to find implicit or created cues of genuineness. And then there are other methods, so called technical methods, which try more or less effectively to stop the attacker from ever successfully introducing such I imagery. That makes life harder, but it can never be fully effective, which is why which is why biometric methods are so much more powerful for assuring the genuine presence of a face when it's being used as a security credential.