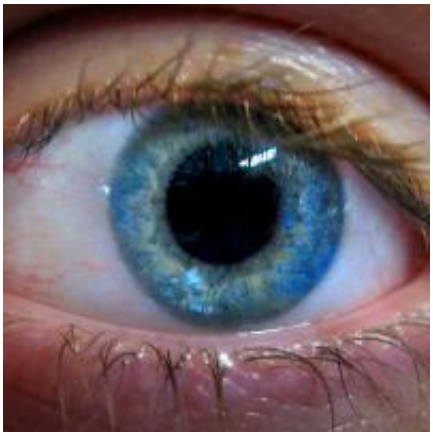
Black Hat presentation shows iris-scanning breach

July 27 2012, by Nancy Owano



(Phys.org) -- A research team from Universidad Autonoma de Madrid and West Virginia University have troubling findings for those who think iris scanning is one of the safest methods of biometric security. Their reverse-engineered, “replicated eye” image was able to bypass iris scanning, fooled into thinking the synthetic image was real and correct. Javier Galbally and his team printed out synthetic images of irises taken from codes of real irises stored in security databases to test iris-scanning vulnerabilities.

An iris code is the data stored by recognition systems when they scan a person's eye. This is information that the researchers could replicate in their synthetic images.

A commercial iris system only looks for the iris code and not an actual eye, Galbally noted. He and his team tested their fake irises against a leading commercial-recognition system. In 80 percent of attempts, the scanner believed that the attempt was a real eye.

The findings of their tests were shared at the annual Black Hat security conference that took place July 21 to July 26in Las Vegas.

“A binary iris code is a very compact representation of an iris image, and, for a long time, it has been assumed that it did not contain enough information to allow the reconstruction of the original iris,” said the Black Hat conference note. The team’s approach was described as a probabilistic approach to reconstruct iris images from binary templates, and they also sought to analyze to what extent the reconstructed samples were similar to the original ones While a human expert would not be easily deceived by them, “there is a high chance that they can break into an iris recognition system,” it was noted.

Further commenting at the Black Hat event, assistant professor Galbally, of the Biometric Recognition Group-of ATVS, said “The idea is to generate the iris image, and once you have the image you can actually print it and show it to the recognition system, and it will say okay,” determining that the image is the real person.

To carry out the exploit, a hacker would need to access the database that holds the iris scans, stored as templates or digital records of an individual's biometric features. Upon access to the templates, the hackers could use a genetic algorithm to alter the synthetic code over several iterations until a nearly identical template was produced. Creating the match would be as simple as printing it out and showing it to the recognition system. This in turn could be achieved by patching the image onto a contact lens to be worn by the attacker.

One may argue that an exploit of this nature is not likely “but the vulnerability is there," he said, and it is always useful for awareness that such vulnerabilities exist. Galbally is actively involved in European projects focused on vulnerability assessments of biometrics

The significance of the findings presented at Black Hat is that this is evidence of an identity-stealing technique where the fake image can be generated from the iris code of a real person. Past work in iris scanning vulnerabilities centered on creating synthetic iris images that had characteristics of real iris images but were not connected to real people.