Forbes / Security
MAR 5, 2015 @ 08:33 AM 9,075

Hacking Putin's Eyes: How To Bypass Biometrics The Cheap And Dirty Way With Google Images

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. **FULL BIO**

Alongside the abundance of phones and apps on show at the mad Mobile World Congress this week were some devices that offered a special way to secure devices. Namely, eye scan logins. Both ZTE and Fujitsu let attendees loose on their versions of the authentication technology, though the commercial releases aren't ready yet.

Though it might seem secure, this form of biometrics in its various manifestations has been bypassed by some remarkably simple techniques in the past. Security researcher Jan “Starbug” Krissler, from the famous Chaos Computer Club, told FORBES this kind of attack can be carried out against some iris-scanning kit just using high-resolution images found in Google searches. He believes that where photos are vivid and large enough, it’s possible to simply print copies of people’s eyes and bypass biometric authentication.

Krissler, who is employed by Telekom Innovation Laboratories (T-Labs), has history in the biometrics space. In December, he showed off a “clone” of the thumbprint of German defense minister Ursula von der Leyen. He’d created the fake print by taking a number of his own snaps of the politician's hand and using commercial fingerprint software from Verifinger to get accurate readings of the minister’s unique print. Krissler could then apply a layer of latex milk or wood glue over the top of an inverted image of the print on a transparent sheet to create an accurate clone, though he was unable to ascertain whether it was a genuine copy of von der Leyen’s thumb; he hadn't gotten her permission to carry out further tests.

As he will detail in an upcoming talk at the CanSecWest conference in Vancouver this month, Krissler said he can do similar work with eyes simply using pictures gathered off the internet. To get a useful image, he had to rely on a number of

factors. First, the target's eyes must had to be bright because of the way the infrared-based system his company bought for him used light. In his tests in December, Krissler messed with Panasonic's Authenticam BM-ET200 iris recognition technology, a product that has been discontinued but the only system he said he has seen in common use today.

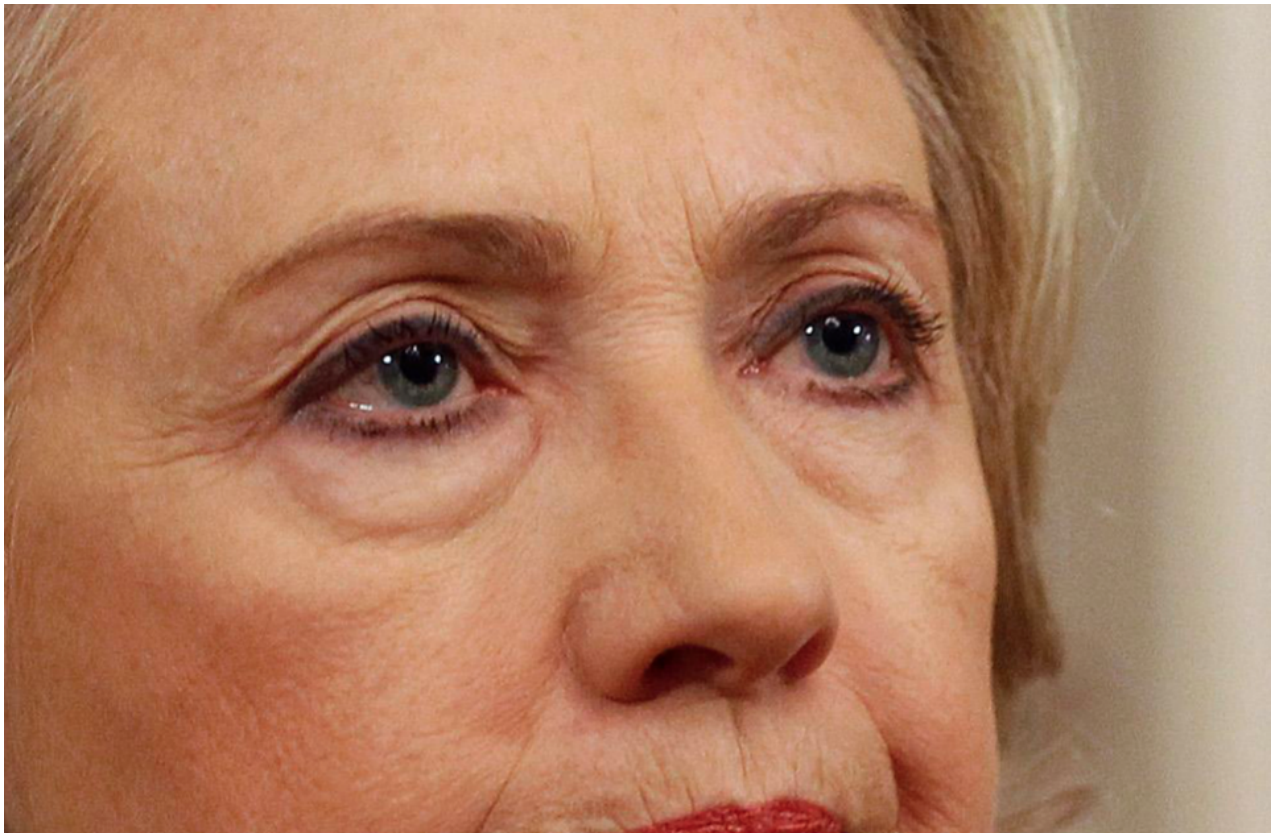
The image also had to be large and clear enough, though Krissler didn't see that as much of a barrier. "We have managed to fool a commercial system with a print out down to an iris diameter of 75 pixels," he told FORBES over Jabber instant messaging. "I did tests with different people and can say that an iris image with a diameter down to 75 pixel worked on our tests." The print out had to have a resolution of 1200 dpi too, though it's easy to find printers able to hit that specification today, and ideally at least 75 per cent of the iris was visible.

Unlike the fingerprint attack, where it was necessary to create a proper clone, all that he needed in his iris recognition hacks was the print out, the researcher claims. "It's nothing more. I punched a hole in the middle, but only for orientation. It's not needed," Starbug added.

Hacking presidents... kind of

Any attacker willing to carry out such a brazen attack would have to find some suitable targets first. Fortunately (or unfortunately), some of the most powerful people in the world are often pictured in high definition and happen to have lovely bright eyes. Krissler found an election poster of Angela Merkel with an iris diameter of 175 pixels that was ideal. A simple search on Google Images brought up other attractive targets from the political world, including Russian president Vladmir Putin, former Secretary of State and First Lady Hillary Clinton and UK prime minister David Cameron.

Vladmir Putin's eyes - NBC



Hilary Clinton's eyes - MSNBC

David Cameron's eyes - The Spectator

There are, unsurprisingly, a vast number of high quality images that would be useful for assuming the identity of others. Krissler has been looking at some 4K resolution pornography (which may or may not make the conference talk) and found some startlingly clear eye images too.

With so many people sharing images of their lovely visages across the web in high definition and with tech giants starting to make iris scanners more commercially viable, such attacks are becoming increasingly feasible. Whilst the EyePrint ID technology going into the ZTE Grand S3 phone looks at the veins in the whites of people's eyes, the Fujitsu technology uses an infrared-based system just as the Panasonic scanner did. Samsung has also been eyeing up iris scanning. Hopefully, the technology has advanced in the last decade to prevent such obvious attacks, rather than just being miniaturized, though successful attempts to get around Apple's Touch ID would indicate security might come second to convenience for many of the world's top smartphone manufacturers.

Per Thorsheim, authentication expert, told FORBES, iris scanning is "a nice party trick and sales pitch [but is] not ready for the mass market". Whilst it might be suitable for some high security environments, it's not for smartphones, he added.

It might prove tricky to get access to targets' hardware, of course, and there's no guarantee online images haven't been tampered with to protect against such evil attacks. But whether his attacks would work on modern systems or not, Krissler

claims to have proven it’s possible to mix open source intelligence, gathered from all those high-resolution images of people's sensory organs found across the web, with biometric authentication to start hacking hardware of famous people and everyday folk alike. Bypassing biometrics sounds sophisticated but breaking it sure isn't.