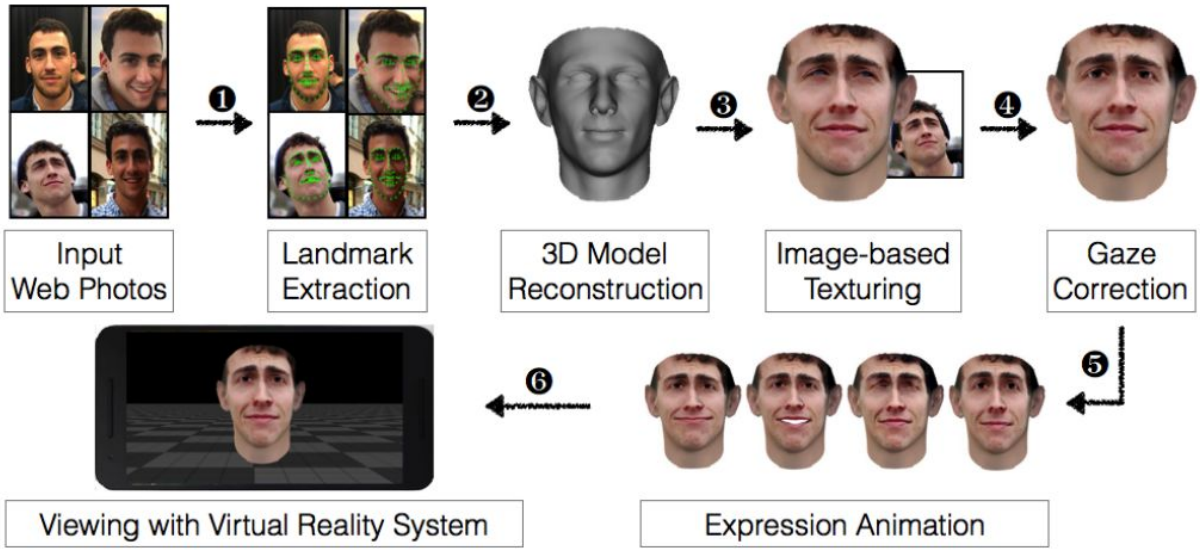
VR rendering software used to trick facial security systems

August 23 2016, by Bob Yirka



Overview of our proposed approach. Credit: Yi Xu et al.

(Tech Xplore)—A small team of researchers with The University of North Carolina has given a demonstration at this year's Usenix symposium showing a means for easily defeating facial security systems. They have outlined their work in a paper published on the Usenix site.

Computer makers and software creators alike have heard complaints from users who have grown weary of having to type in passwords for their computer systems and applications. One possible solution has been

the creation of facial security systems that replace password entry systems—a person simply looks at their screen while their face is examined and when the system recognizes them, allows them entry. Such systems are still in development, however, as some users have found that they can be circumvented by a person who resembles them. And now it appears that someone wishing to gain access to another person's system could simply do a quick image search on the Internet, use a piece of virtual reality rendering software and then use the result to gain entry.

The research team showed how easy it was by asking 20 people at the symposium to volunteer for a test of five of the top facial security systems for sale in online stores. Researchers used the names of volunteers to search the web for images—unsurprisingly, the team was able to find at least three photographs of each volunteer. Those pictures were then input into a VR rendering software system that recreated their faces in 3-D—the team then manipulated the VR results slightly to make sure they conformed to what a facial security system looks for, i.e. movement, eyes that focus at a certain point, etc. They then displayed the results to another device running a facial security system that had been trained to recognize the actual user and found that they could gain access 97.5 percent of the time overall.

The five facial security systems tested were Mobius, True Key, KeyLemon, BioID and 1U. Only 1U successfully foiled the VR rendering trick, which the researchers suggested was due to low performance by the application—it did not do very well even when the real user was staring at the screen. The researchers also found that when they took pictures of the faces of the volunteers and ran them through the VR software, they were able to circumvent all of the systems every time they tried.

More information: Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos, Proceedings of the

25th USENIX Security Symposium, www.usenix.org/conference/usen … ions/presentation/xu

Abstract

In this paper, we introduce a novel approach to bypass modern face authentication systems. More specifically, by leveraging a handful of pictures of the target user taken from social media, we show how to create realistic, textured, 3D facial models that undermine the security of widely used face authentication solutions. Our framework makes use of virtual reality (VR) systems, incorporating along the way the ability to perform animations (e.g., raising an eyebrow or smiling) of the facial model, in order to trick liveness detectors into believing that the 3D model is a real human face. The synthetic face of the user is displayed on the screen of the VR device, and as the device rotates and translates in the real world, the 3D face moves accordingly. To an observing face authentication system, the depth and motion cues of the display match what would be expected for a human face.

We argue that such VR-based spoofing attacks constitute a fundamentally new class of attacks that point to a serious weaknesses in camera-based authentication systems: Unless they incorporate other sources of verifiable data, systems relying on color image data and camera motion are prone to attacks via virtual realism. To demonstrate the practical nature of this threat, we conduct thorough experiments using an end-to-end implementation of our approach and show how it undermines the security of several face authentication solutions that include both motion-based and liveness detectors.