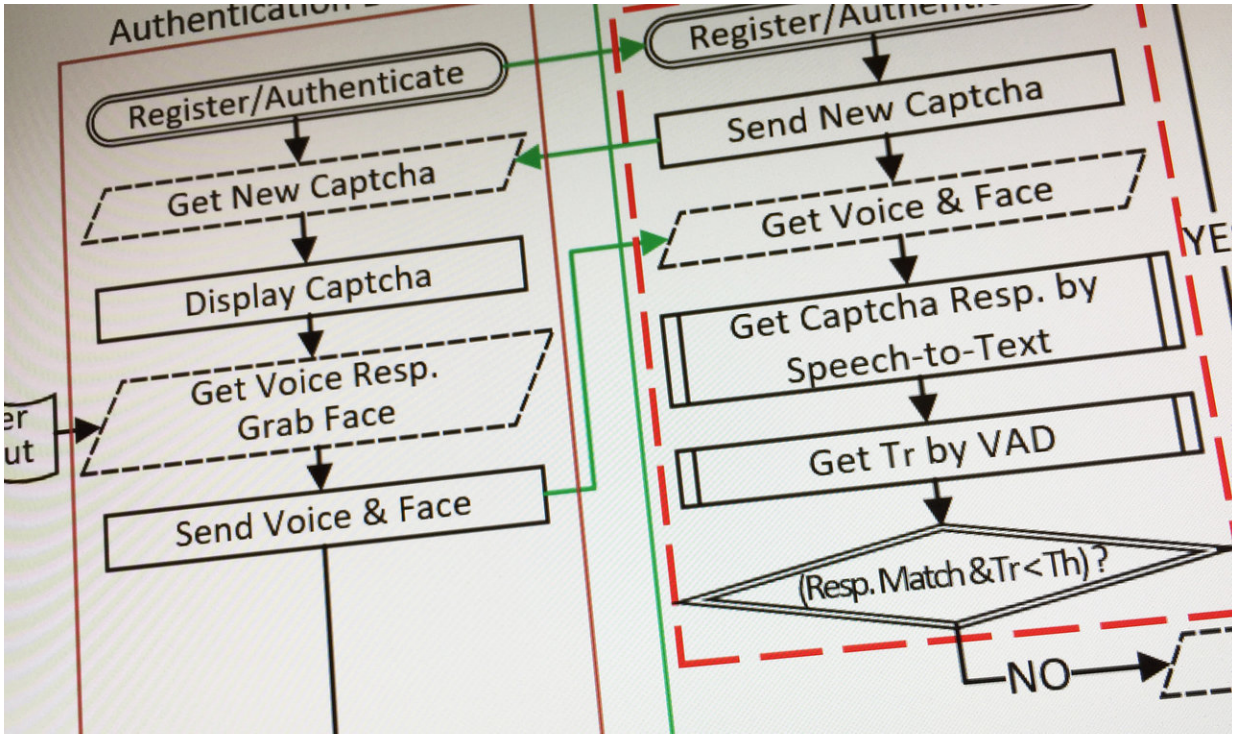
TechXplore

Real-time Captcha technique improves biometric authentication

February 19 2018



Part of the flow diagram of the Real-Time Captcha system. Credit: Georgia Tech

A new login authentication approach could improve the security of current biometric techniques that rely on video or images of users' faces. Known as Real-Time Captcha, the technique uses a unique "challenge" that's easy for humans—but difficult for attackers who may be using machine learning and image generation software to spoof legitimate users.

The Real-Time Captcha requires users to look into their mobile phone's built-in camera while answering a randomly-selected question that appears within a Captcha on the screens of the devices. The response must be given within a limited period of time that's too short for artificial intelligence or machine learning programs to respond. The Captcha would supplement image- and audio-based authentication techniques that can be spoofed by attackers who may be able to find and modify images, video and audio of users—or steal them from mobile devices.

The technique will be described February 19th at the Network and Distributed Systems Security (NDSS) Symposium 2018 in San Diego, Calif. Supported by the Office of Naval Research (ONR) and the Defense Advanced Research Projects Agency (DARPA), the research was conducted by cyber security specialists at the Georgia Institute of Technology.

"The attackers now know what to expect with authentication that asks them to smile or blink, so they can produce a blinking model or smiling face in real time relatively easily," said Erkam Uzun, a graduate research assistant in Georgia Tech's School of Computer Science and the paper's first author. "We are making the challenge harder by sending users unpredictable requests and limiting the response time to rule out machine interaction."

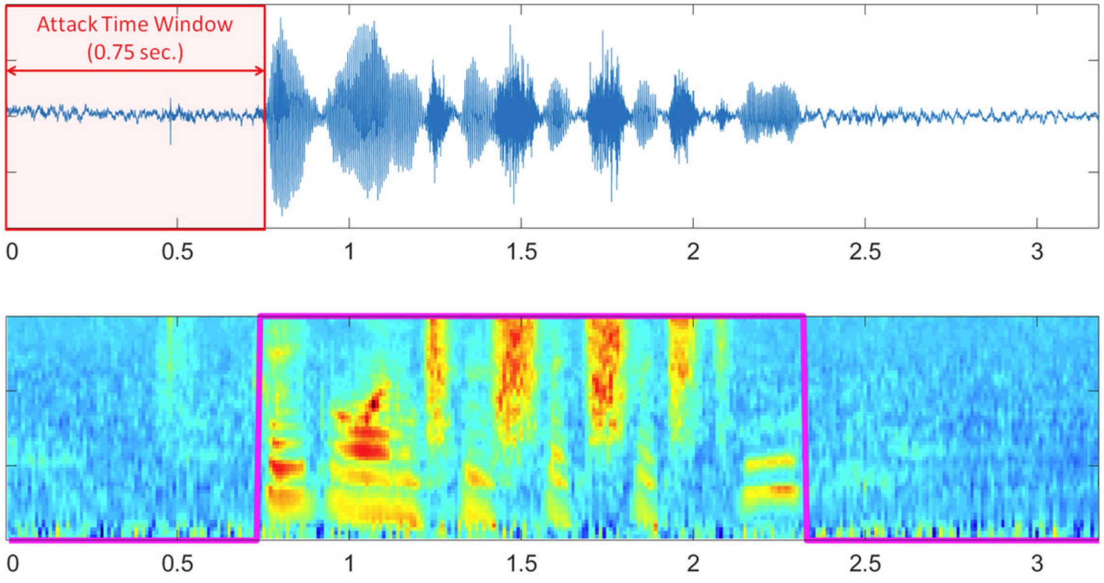
As part of efforts to eliminate traditional passwords for logins, mobile devices and online services are moving to biometric techniques that utilize a human face, retina or other biological attribute to verify who is attempting to log in. The iPhone X is designed to unlock with the user's face, for instance, while other systems utilize short video segments of a user nodding, blinking or smiling.

In the cat-and-mouse game of cyber security, those biometrics can be spoofed or stolen, which will force companies to find better approaches, said Wenke Lee, a professor in Georgia Tech's School of Computer Science and co-director of the Georgia Tech Institute for Information Security and Privacy.

"If the attacker knows that authentication is based on recognizing a face, they can use an algorithm to synthesize a fake image to impersonate the real user," Lee said. "But by presenting a randomly-selected challenge embedded in a Captcha image, we can prevent the attacker from knowing what to expect. The security of our system comes from a challenge that is easy for a human, but difficult for a machine."

In testing done with 30 subjects, the humans were able to respond to the challenges in one second or less. The best machines required between six and ten seconds to decode the question from the Captcha and respond with a faked video and audio. "This allows us to determine quickly if the response is from a machine or a human," Uzun said.

The new approach would require login requests to pass four tests: successful recognition of a challenge question from within a Captcha, response within a narrow time window that only humans can meet, and successful matches to both the legitimate user's pre-recorded image and voice.



The time window for attacks on the Real-Time Captcha system. Credit: Georgia Tech

"Using face recognition alone for authentication is probably not strong enough," said Lee. "We want to combine that with Captcha, a proven technology. If you combine the two, that will make face recognition technology much stronger."

Captcha technology - originally an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart" - is widely used to prevent bots from accessing forms on websites. It works by taking advantage of a human's superior ability to recognize patterns in images. The Real-Time Captcha approach would go beyond what's required on websites by prompting a response that will produce live video and audio that would then be matched against a user's stored security profile.

Captcha challenges might involve recognizing scrambled letters or solving simple math problems. The idea would be to allow humans to respond before machines can even recognize the question.

"Making a still image smile or blink takes a machine just a few seconds, but breaking our Captcha changes takes ten seconds or more," said Uzun.

In trying to improve authentication, the researchers studied image spoofing software and decided to try a new approach, hoping to open a new front in the battle against attackers. The approach moves the attacker's task from that of generating convincing video to breaking a Captcha.

"We looked at the problem knowing what the attackers would likely do," said Simon Pak Ho Chung, a research scientist in Georgia Tech's School of Computer Science. "Improving image quality is one possible response, but we wanted to create a whole new game."

The real-time Captcha approach shouldn't significantly change bandwidth requirements since the Captcha image sent to mobile devices is small and authentication schemes were already transmitting video and audio, Chung said.

Among the challenges going forward is overcoming the difficulty of recognizing speech in a noisy environment and securing the connection between the device camera and the authenticating server.

"For any security mechanism that we develop, we need to worry about the security of the mechanism first," Lee said. "Once you develop security technology, it becomes a target for the attackers, and that certainly applies to biometric technology."

More information: Erkam Uzun, Simon Pak Ho Chung, Irfan Essa and Wenke Lee, "rtCaptcha: A Real-Time CAPTCHA Based Liveness Detection System," Network and Distributed Systems Security (NDSS) Symposium 2018.

Provided by Georgia Institute of Technology

Citation: Real-time Captcha technique improves biometric authentication (2018, February 19) retrieved 3 May 2024 from https://techxplore.com/news/2018-02-real-time-captcha-technique-biometric-authentication.html