December 19, 2016

System And Method For Authenticating A Speaker Across The Surfaces Of A Security System

Daniel Raffel

SYSTEM AND METHOD FOR AUTHENTICATING A SPEAKER ACROSS THE SURFACES OF A SECURITY SYSTEM

ABSTRACT

A system and method are disclosed of authenticating a user to a security system based on voice recognition. The method could be implemented in a system including a user with a smartphone device at a security access system connected to a Cloud-based authentication server. The method matches a spoken voice picked up locally by the access system to a registered account on the server. The server could have another registered hardware device such as a smartphone or tablet locally connected to the security system using a mechanism such as Bluetooth, WiFi, etc. that is used to identify the user. The system determines that the user is a privileged account holder on the alarm with the permission being verbally requested. The authentication server then matches this command to a trained voice in an appropriate server record. The system then allows the user to arm or disarm the alarm.

BACKGROUND

Badging in/out of a security access system is a nuisance when hands are full. Most security access and alarm systems require a user to do one of the following to arm/disarm: either type a code, launch an app on their phone, and/or swipe a NFC/RFID tag at the access system.

DESCRIPTION

This disclosure presents a system and a method of authenticating a user to a security system based on voice recognition. Such security system may be a traditional alarm system or any smart device (that may be connected) which requires user authentication and authorization. The method could be implemented in a system as illustrated in FIG. 1, which shows a user with a smartphone device at a security access system connected to a Cloud-based authentication server. The method, as illustrated in FIG. 2 matches a spoken voice

picked up locally by the access system to a registered account (step 1). The server could have other registered hardware devices such as a smartphone or tablet locally connected to the alarm system using a mechanism such as Bluetooth, WiFi, etc. that is used to identify the user (step 2). The system then determines that the user is a privileged account holder on the alarm with the permission being verbally requested (step 3). For example, a user could say "<catchword>, Turn on(/off) the alarm". The authentication server then matches this command to a trained voice in an appropriate server record (step 5). The system then verifies that the user has a device that is currently connected to the access system which received the verbal command AND is an authorized user on the alarm system with permissions to arm or disarm the access alarm. The system then allows the user to arm or disarm the alarm.

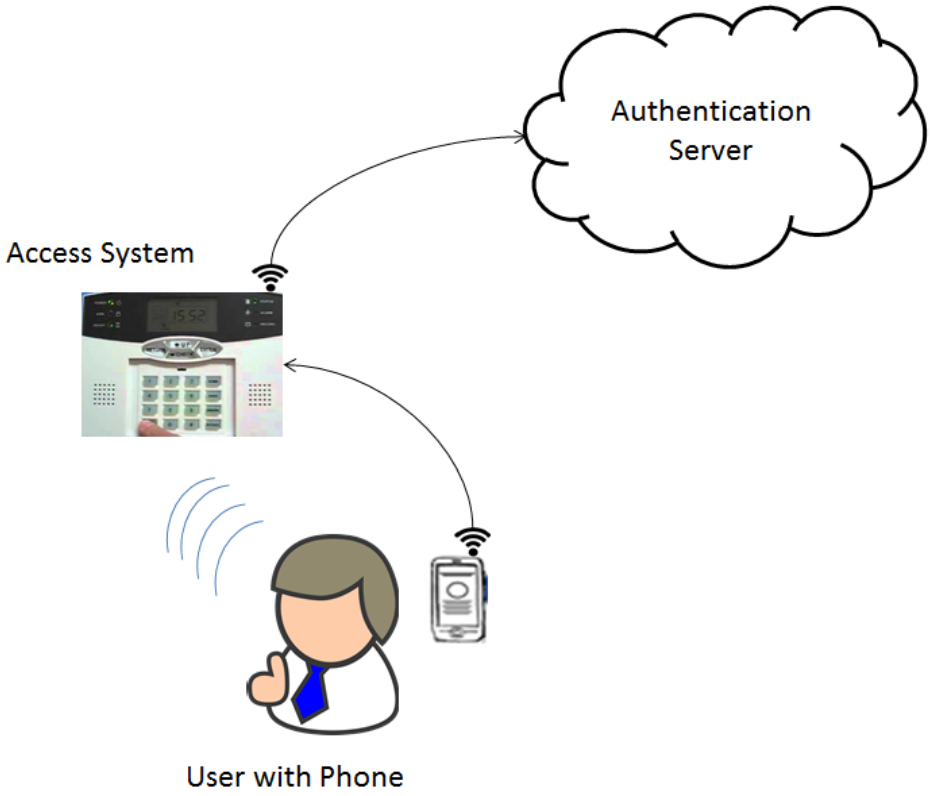

FIG. 1: System for authenticating a speaker across secure access

The system and method require a series of connected services: voice fingerprinting of the speaker, a strong user account authentication system, voice command biasing and speech recognition, device registry, and an alarm with mic/speaker running a client app. The voice

recognition at the authentication server could serve as primary authentication. However, data about a user in terms of the ‘digital footprint’ could be used as a set of multiple second factor authentication mechanisms. For example, the logic used by the system prior to making a positive authentication in step 6 of the system could be as follows: Is the voice Daniel? Is Daniel likely to be present based on his primary phone data? Is Daniel's phone connected to the alarm system right now? Does Daniel have permission on the alarm? These secondary authentications require a tremendous amount of knowledge about the user, where they are, where they've been and what access they have right now. By solving these problems, customers could unlock a number of unique security challenges which today require using hands and/or traditional biometrics (i.e. fingerprint/eyeballs.) In short, this could make it easier to disarm an alarm.

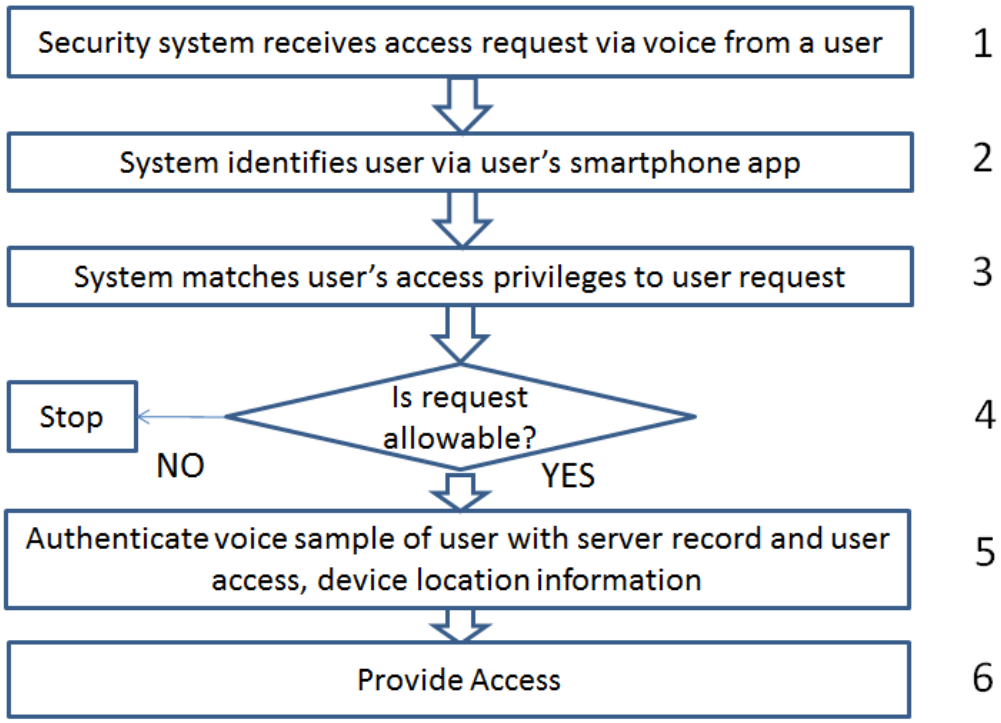

FIG. 2: Method for authenticating a speaker across a secure access system

While someone could try to record a voice it would be impossible to spoof all the data known about the user. In a variation, the method could include additional authentication via a

challenge-response. A wide variety of interactive dialogues could be created that are user-specific to help provide the security challenge using the digital footprint of the user. For example: "What movie did you watch last night on <portal>? Where were you yesterday at 9am? What app did you last install on the <portal>?"

The method disclosed solves a well-documented daily pain point of having to badge in/out to arm/disarm an access/alarm system. While the method is illustrated with reference to access permissions, it could also be used to help determine whether someone has the permission for other things (purchasing, etc.) via voice activation.