June 05, 2017

Defense Against Biometric Reproduction Attacks

Nicholas Peterson

Jesper Johansson

Hunter King

DEFENSE AGAINST BIOMETRIC REPRODUCTION ATTACKS

ABSTRACT

Systems and methods for defense against biometric reproduction attack are disclosed. The system includes one or more mobile devices installed with a security feature integrated to the operating system or installed to the device as an app. The security feature is in communication with a server installed with a mobile device management solution. The device includes a multi-factor authentication system including at least one biometric authenticator and at least one non-biometric authenticator. The method includes prompting for biometric authentication, if the network is reachable. In the absence of an active network, the server may instruct the device to stop using a biometric authentication and request the user for a multifactor authentication. The systems and methods provide for full enterprise connectivity on devices with a biometric authentication system. The present disclosure allows the network administrators to address biometric reproduction attacks with variable levels of risk tolerance.

BACKGROUND

Biometric authentication factors (e.g. fingerprint authentication) are becoming increasingly commonplace for use in systems such as mobile devices including phones and tablets, computers, and various government resources. However, biometrics may be fooled through a reproduction attack where the attacker creates a replica of the biometric authenticator. For instance, a conductive ink or a thin film may be used to reproduce a fingerprint. The requisite information may be lifted from a device itself, from some other object or system that stores a representation of a fingerprint, or reproduced from a photo.

As revocation of the biometric authenticator in the system is not possible, the mitigation against reproduction attacks requires an administrator to disable using a biometric authenticator on a device that may no longer be in the possession of the rightful owner. To do that, the device must be reachable across the network, unless it can make its own decisions that biometric authentication should be prevented. Once an attacker is in possession of the device that accepts a biometric authenticator, it becomes a race against time to disable use of biometric authentication on the device before the attacker manages to reproduce the authenticator. For instance, mobile phones that accept fingerprint authentication require the user to enter a PIN code or password if the device has been out of use for 24 to 48 h. However, 24 to 48 h is more than enough time than is needed for a skilled attacker to reproduce a biometric authenticator. Additionally, network administrators may be able to disable a device remotely when the loss is reported by the user. However, this relies on an active network connection. Currently, it remains possible for an attacker to easily defeat such protection measures by placing the device in airplane mode, or to block network connectivity by going into a shielded facility.

DESCRIPTION

Systems and methods for defense against biometric reproduction attack are disclosed. The system is depicted in FIG. 1 and includes one or more mobile devices installed with a security feature enabled for mobile device management. The security feature may be integrated to the operating system or installed to the device as an app. The device is in communication with a server installed with a mobile device management solution. The device has a multi-factor authentication system including at least one biometric authenticator and at least one non-biometric authenticator. In one example, the biometric authenticator may be a fingerprint, iris or facial recognition authenticator. The non-biometric authenticator may include something-you-know authenticator, or a something-you-have authenticator. The something-you-know authenticator may be a PIN, password or pattern. The server is under the control of a network administrator that may issue commands to the security application remotely.

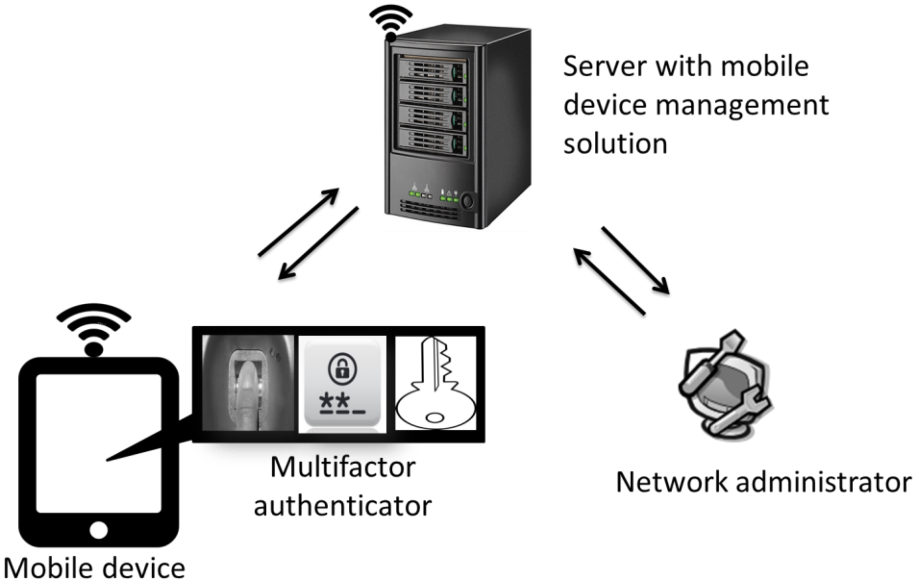
Server with mobile device management solution
Multifactor authenticator
Network administrator
Mobile device

FIG. 1: A system for defense against biometric reproduction attacks

The method of mounting a defense against a biometric reproduction attack is depicted in FIG. 2. The device prompts for a biometric authentication if the network is reachable. In the absence of an active network, the device prompts the user for a non-biometric authentication, such as a something-you-know or something-you-have authentication, to unlock the device. The device may request for a multi-factor authentication if the user attempts to disable the network stack in the device. The security feature can disable access to the device or delete files in the device based on predefined criteria that detects or defines an intruder attack. The device may continue to accept biometric authentication under certain circumstances, such as for a specific time after network connectivity is lost, or if the network connectivity was manually disabled after presenting a something-you-know/have authenticator, or if the device is expected to be on a plane at this time.

In one instance, the security application requests a non-biometric authenticator to be entered every time the device is unlocked when the network is unreachable. Alternatively, a non-biometric authenticator is required the first time the device is unlocked within a specific timeline, but biometric authentication is then enabled for a period of time much shorter than 24-48 hours. In another instance, a non-biometric authenticator is required only the first time the device is unlocked after the network is unreachable, but biometric authentication is then re-enabled until the network is once again reachable. In some instances, certain features, such as access to certain apps and data are made unavailable by the security application unless a something-you-know/have authenticator is used to re-enable these features. In instances where maximizing the usability is desired while maintaining a slightly improved security posture, the biometric authentication system may remain enabled if the network stack was disabled immediately after authentication with a non-biometric authenticator.

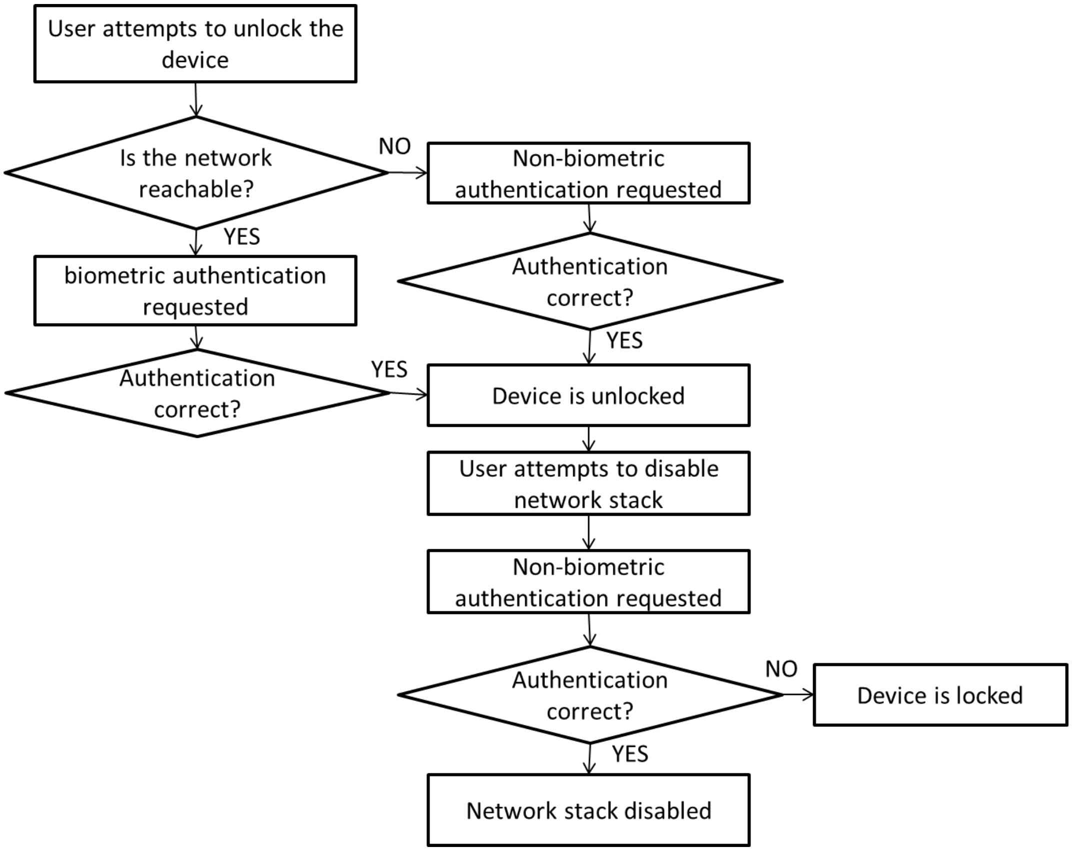
User attempts to unlock the device
Is the network reachable?
NO
Non-biometric authentication requested
YES
biometric authentication requested
Authentication correct?
YES
Authentication correct?
YES
Device is unlocked
User attempts to disable network stack
Non-biometric authentication requested
Authentication correct?
NO
Device is locked
YES
Network stack disabled

FIG. 2: A method for defense against biometric reproduction attacks

The systems and methods address an unsolved problem of biometric reproduction attacks on devices. The only related solution that is available till now is the requirement for something-you-know authentication after an idle period. The systems and methods provide for full enterprise connectivity on devices with biometric authentication system. The present disclosure allows the network administrators to address biometric reproduction attacks with variable levels of risk tolerance.