MOTOROLA SOLUTIONS

Enhanced Radio Authentication using a camera Kiosk

By Ketki Hardas, Melanie King, Jari Jarvinen, Ryan Nilsen, and Charles Colman
Motorola Solutions, Inc.

ABSTRACT

This paper proposes and explains an innovative method to enhance the authentication process on radios without jeopardizing security. It highlights two key elements: 1) Repurpose a device kiosk to serve as an access token after a user has logged in. 2) Dynamically assigning hardware access token on the body worn camera assigned to an officer to be used as an authenticator for other devices.

PROBLEM

Entering username and password using a handheld portable radio is difficult, because of the small on screen QWERTY keyboard.

The case sensitive passwords or usernames with the requirement of including numbers or special characters is very slow with a high error rate.

The high error rate can lead to users being locked out from the device after several attempts.

If an application requiring multi-factor authentication (MFA) is needed when the user is in the field, user safety may be compromised due to eyes-down time and cognitive overload when focusing on the username and password entry with the small onscreen keyboard.

SOLUTION

The following method uses a device kiosk, such as the Motorola Solution Watchguard (that provides cameras to a customer) as a means to authenticate the radio

Kiosk itself becomes a factor to authenticate the radio/s within proximity (something they have) and the second factor would be a PIN (something they know)

Alternatively, the kiosk configures the camera (something they have) as a security hardware token, so that the first responder can use the camera as one of the factors to authenticate with the portable or mobile radio and the second factor would be again a PIN (something they know)

Once the body-worn camera is checked in/returned, the user profile and authentication tokens are cleared. Below is a diagram demonstrating the mapping between factor of authentication, alternate authenticator and the device to be authenticated :

OPERATION

A system consisting of a kiosk, first mobile device (such as Body Worn Camera) and a second mobile device (such as radio) is presented. The second device is using MFA based on username/password and a PIN. All devices communicate between them using wireless radio transmission such as (but not only) Bluetooth, NFC and WiFi. PIN is known by the user.

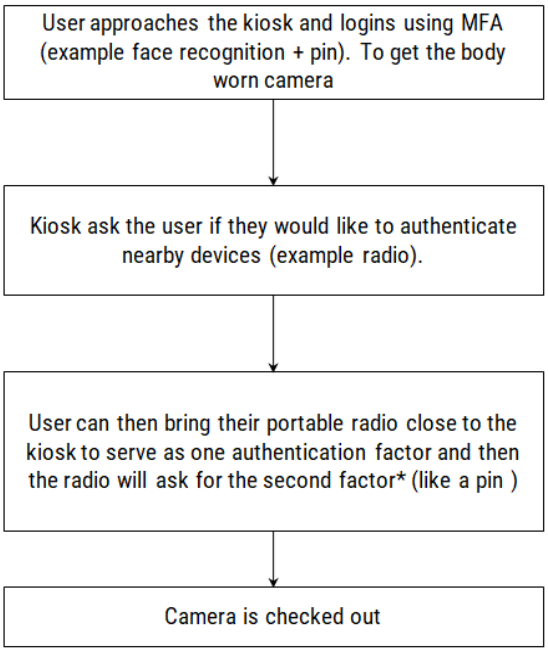
2.User does MFA with the kiosk (example: username/password and face recognition). User then starts authenticating himself to the second device by confirming his authenticity to the second device based on the authentication done on the kiosk. For example (but not only) requesting the kiosk to share a token with the second device using the wireless transmission. User is then only asked to enter the PIN to finish the authentication with the second device.

3. Alternatively, the first device and the second device communicate with each other using secure wireless communication (example Bluetooth). The user is authenticated for the first device based on his authentication to the kiosk and then the second device authenticates the user based on the authenticity with the first device. For example (but not only) Kiosk shares a token with the first device which in turn forwards it to the second device as the first

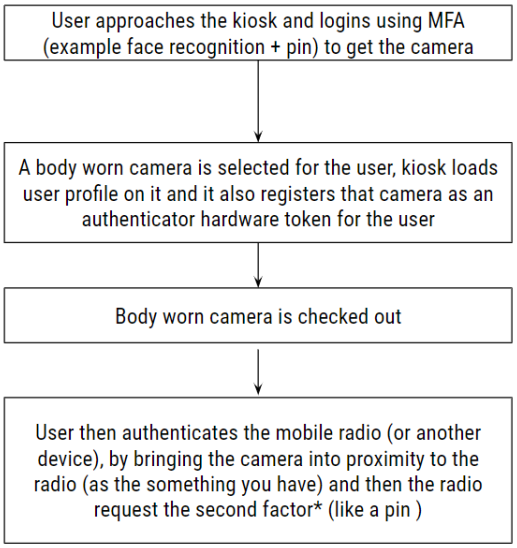
authentication stage. User is then only asked to enter the PIN to finish the authentication with the second device.

5. Same process as above where the PIN is replaced by biometric factor (for example voice authentication).

Below is a flowchart showing the enhanced Portable radio Authentication through the kiosk:



The following flowchart shows the enhanced Portable radio Authentication through a camera configured by the kiosk for that user:



CONCLUSION

This method presents an improved authentication method on a portable radio device, when the user is already authenticating at a kiosk for another device.