October 2021

Crown-based Authentication for Smartwatches

N/A

Crown-based Authentication for Smartwatches

ABSTRACT

At present, a smartwatch can authenticate a user by using a nearby phone controlled by the owner of the smartwatch. However, requiring a nearby phone defeats portability. Also, a watch that retains authentication for purposes of payment constitutes a security risk. This disclosure describes techniques that leverage the haptic crown of a smartwatch to enter numbers in a rotary fashion on the smartwatch screen to authenticate the user for payment or contexts where authentication is necessary. Authentication can be retained on the device until the watch is removed.

KEYWORDS

- Smartwatch
- Watch crown
- Haptic knob
- User authentication
- Combination lock
- Fingerprint sensor
- Touchscreen code entry
- PPG sensor

BACKGROUND

Smartwatches and other wearable devices such as fitness bands are popular for their easy portability and are typically always available to a user, e.g., even in situations when the user does not carry her smartphone or other device. This makes such devices particularly suitable for on-

the-go payments. However, the touchscreen on such devices is often too small to enable the user to quickly enter a passcode.

At present, a smartwatch can authenticate a user by using a nearby phone controlled by the owner of the smartwatch. However, requiring a nearby phone (for example, connected over Bluetooth) defeats portability. Also, a watch that retains authentication for purposes of payment constitutes a security risk. Mitigating such security risk, e.g., by incorporating an additional fingerprint sensor within the smartwatch, increases device costs. Moreover, in the event of a smartwatch that has retained user authentication being lost or stolen, immediate and multi-step action by the user is unnecessary to de-authenticate the device.

DESCRIPTION

This disclosure describes techniques that leverage the haptic crown of a smartwatch to enter numbers in a rotary fashion on the smartwatch screen to authenticate the user for payment or contexts where authentication is necessary. Authentication can be retained on the device until the watch is removed. Watch removal can be detected by photoplethysmography (PPG) sensors, inertial measurement unit (IMU) sensors, or other suitable mechanisms.

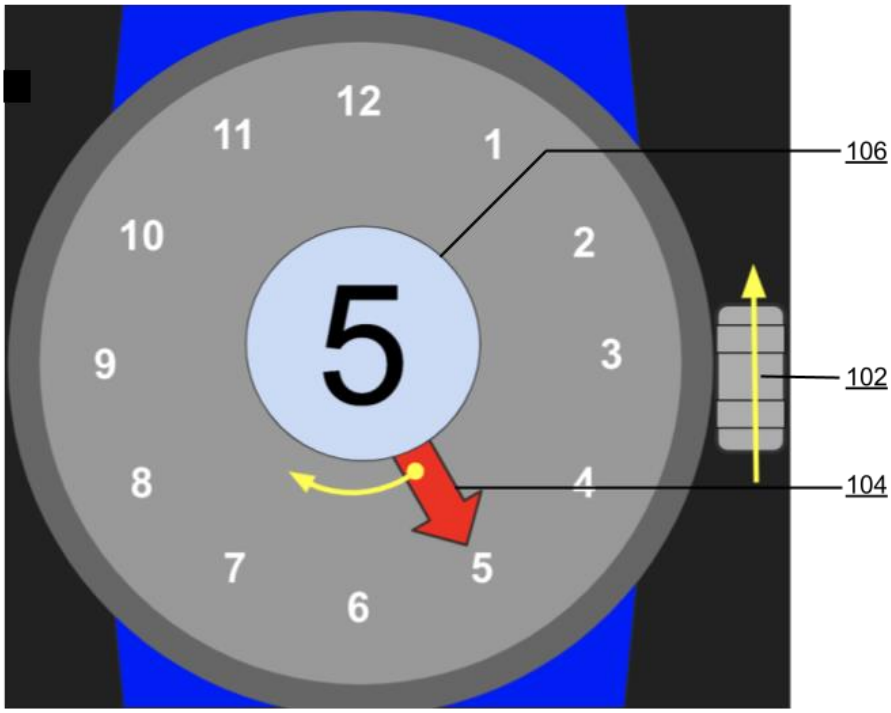

Fig. 1: Crown-based authentication on a smartwatch

Fig. 1 illustrates crown-based authentication on a smartwatch. Using the crown (102), which can be, e.g., a haptic knob, the user rotates a pointer (104) on the screen to reach a displayed number (106). The movement of the pointer can be regulated using detents. The pointer can be rotated clockwise or anti-clockwise. A change in direction of movement of the pointer indicates that the number has been entered. Similar to a combination lock for a safe, a sequence of numbers constitutes a security code, the completed entry of which can be indicated, e.g., using a screen-tap.

Example

A user initiates payment using her smartwatch, which activates an authentication mode, using, e.g., near-field communications (NFC). Consider that the authentication code is 10-5-9. The user rotates the crown counterclockwise until the displayed number reads 10, followed by clockwise rotation of the crown until the displayed number reads 5, and counterclockwise

rotation until the displayed number reads 9. The user then taps the screen to indicate that entry of the authentication code has been completed. The device confirms the authentication and authorizes the payment .

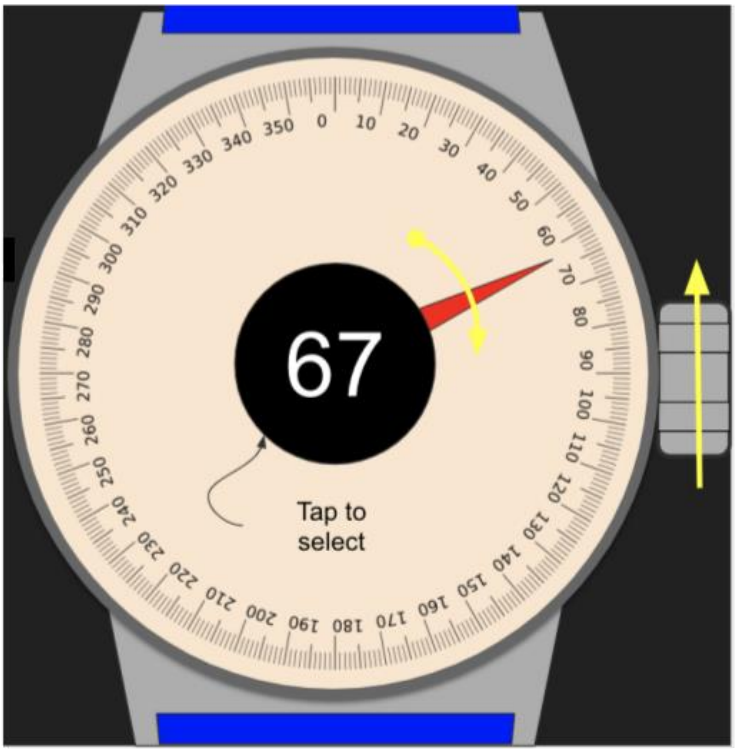

Fig. 2: A variation on crown-based authentication in a smartwatch

Fig. 2 illustrates one of several possible variations on crown-based authentication in smartwatches. For example, the number of digits displayed on the circumference of the screen can be 12, 60, 360, etc. The number selected by moving the pointer is displayed at the center, e.g., the indicator can be the moving pointer and/or a digital display. The authentication mode can be initiated either by NFC or by twisting (winding) the crown a predetermined number of times, e.g., three.

Similar to the combination lock of a safe, a number in the code sequence can require a full rotation or multiple 360-degree rotations. For example, the first number in the security code

sequence can require four rotations before selection, the second number in the code sequence can require three rotations before selection, etc. Alternatively, a screen-tap, pause, or change in the direction of rotation of the pointer can indicate the entry of a number of the security code. Haptics can be used to aid in the detent and the acceptance of entered numbers. Authentication can be required at various events, e.g., at every payment, and/or when the watch is worn, and/or when a timer expires after the most recent authentication. Authentication expires automatically if removal of the watch from the hand is detected, e.g., via PPG sensors, IMU sensors, or other mechanisms.

CONCLUSION

This disclosure describes techniques that leverage the haptic crown of a smartwatch to enter numbers in a rotary fashion on the smartwatch screen to authenticate the user for payment or other secure use-cases.

REFERENCES

[1] Guerar, Meriem, Luca Verderame, Mauro Migliardi, and Alessio Merlo. "2GesturePIN: securing PIN-based authentication on smartwatches." In *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, pp. 327-333. IEEE, 2019.