January 09, 2019

USING DEVICE MOVEMENT FOR MULTI-FACTOR COMPUTING DEVICE AUTHENTICATION

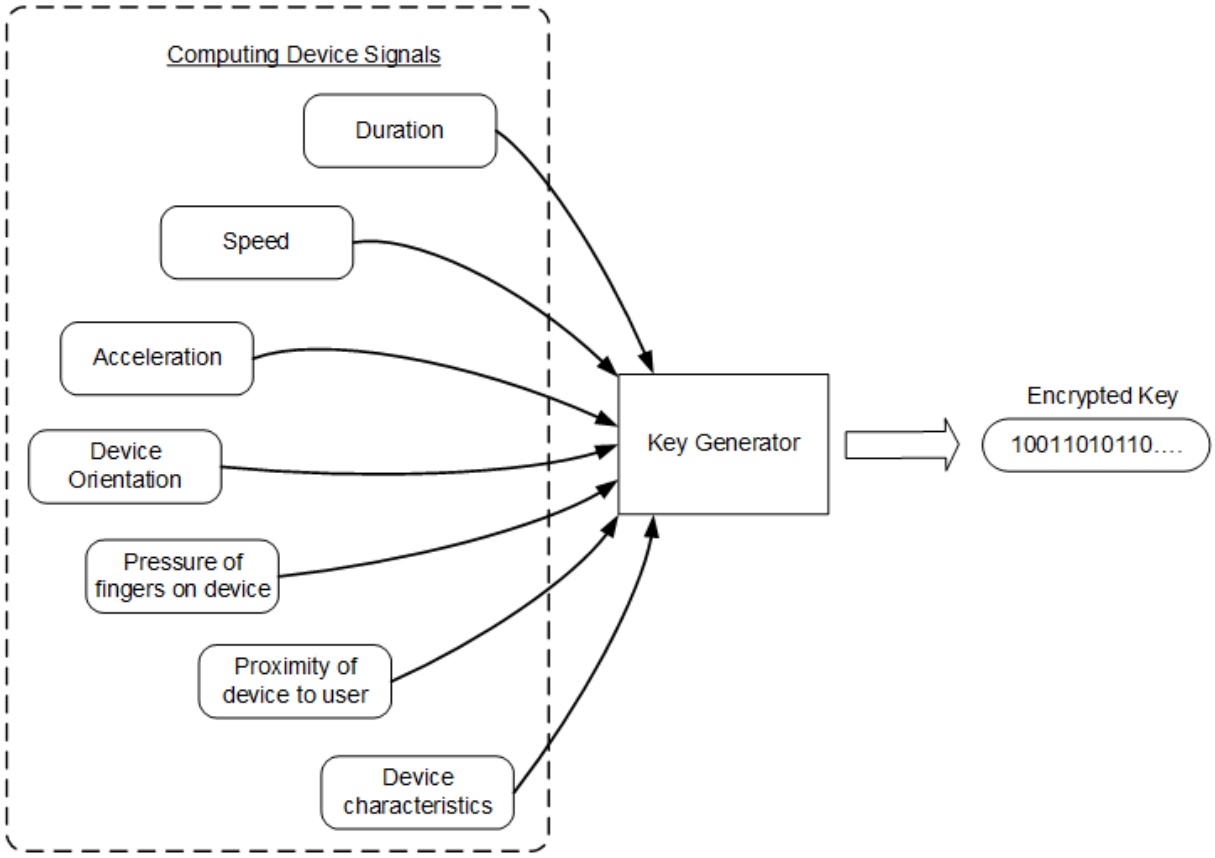
Isaac Andres

USING DEVICE MOVEMENT FOR MULTI-FACTOR COMPUTING DEVICE AUTHENTICATION

Multi-factor computing device authentication involves a user providing information in addition to their username and password in order to access a service. Common examples today include entering a temporary PIN code, answering a personal question, or touching a security key that is installed locally on a computing device. The technology described in this document enables a user to physically move their computing device in a particular pattern to verify their presence, as part of a secure multi-factor computing device authentication process.

KEY GENERATION

To implement such a technology, a Movement Service could be developed and loaded into local memory on a mobile computing device. The Movement Service may be part of the operating system of the computing device, and may encode movement into an encrypted movement key. The encrypted movement key may be a hash of various signals that the computing device captures while the user is moving the computing device in a particular pattern during an authentication process. The various signals that form the basis for an encrypted movement key may include (i) duration of the movement, (ii) speed of the movement, (iii) acceleration during the movement, (iv) orientation of the computing device during the movement, (v) pressure of user fingers on the computing device during the movement, (vi) proximity of the computing device to the user during the movement, (vii) device connectivity characteristics such as WIFI and data connection, and (viii) device characteristics, such as phone model and operating system version.



FIRST IMPLEMENTATION

A user may be prompted during enrollment for a multi-factor authentication process to imagine a particular movement/gesture that is secret to the user, and then to move their mobile computing device in the intended manner responsive to a computing device prompt. The mobile computing device may record any combination of the above described sensor signals and device characteristics (and potentially other sensor signals and device characteristics) during the movement, and the mobile computing device can store those characteristics as an encrypted movement key on the computing device.

Upon the user attempting to access a service that requires multi-factor computing device authentication, such a service can request that the user verify their authenticity by reproducing

the movement that the user provided during the enrollment process. In response, the user can move the computing device in the same manner that the user performed during the enrollment process, in order to verify that the individual attempting to access the service is the actual user and not an unauthorized individual. This movement will be referenced in this document as an authentication gesture, and can include a single movement or multiple different types of movements over a period of time. The Movement Service on the phone may encode movements recorded by the sensors of the computing device after the user is prompted to provide an authentication gesture, and the computing device can compare those encoded movements to the stored encrypted movement key that was generated during enrollment. If the data generated during entry of the authentication gesture matches the encrypted movement key, the computing device can provide a "PASS" signal to the requesting service by way of the Movement Service. If the encoded movements do not match the encrypted movement key, the user may be prompted to provide the authentication gesture another time. After some N amount of failed attempts to provide a valid authentication gesture, the Movement Service may send a "FAIL" signal back to the requesting service.

SECOND IMPLEMENTATION

A second implementation allows for non-permanent movement verification to be specified by the requesting service. For example, a user may attempt to log into their bank's web service. The bank's web service could verify the authenticity of the user with a multi-factor computing device authentication process that relies on user entry of an authentication gesture similar to that provided above. But, instead of the user having to perform an authentication

gesture that the user previously specified during an enrollment process, the bank web service could specify the authentication gesture for the user to perform.

As an example, a user may visit a web service for the bank and enter his username and password into the appropriate fields. After doing so, the bank web service may ask the user to perform the following sequence of movements: (1) Flip the phone upside down for 1 second, (2) Shake the phone gently for 3 seconds, and (3) Rotate the phone right side up. The Movement Service on the mobile computing device may encode signals generated by sensors on the computing device during entry of the authentication gesture in the manner described above with a hash value that forms the encrypted movement key. The Movement Service may then compare the encrypted movement key against a library of movement keys that represent different types of authentication gestures. A result of the comparison process may be passed back to the bank's web service. For example, the computing device may indicate whether the user-entered authentication gesture matches the authentication gesture specified by the web service, by providing either a "PASS" or "FAIL" signal to the bank web service.

THIRD IMPLEMENTATION

A third implementation enables users to encode multiple authentication gestures during enrollment. In this implementation, the user may perform multiple iterations of the enrollment process and may specify a different authentication gesture during each iteration, with the Movement Process generating a different encrypted movement key during each iteration. A service may specify the type of authentication gesture that the user has to perform to access the service, or may simply request that the user perform any authentication gestures that the user specified during enrollment. For example, the Movement Service can select an authentication

gesture randomly from the multiple authentication gestures that the user previously specified, or the Movement Service can select the authentication gesture that the user must perform based on a context of the computing device (e.g., a location of the computing device or a time of the day).

As an example, a user may attempt to log into his bank's web service. The web service may decide to verify that the user is who he says that he is using a multi-factor computing device authentication process that requires user entry of an authentication gesture, and can relay a request to the Movement Service to perform the authentication process. The Movement Service may analyze a context of the computing device, recognize that the device is on a WIFI network that corresponds to a home of the user, and therefore may prompt the user to provide a "Lite" authentication gesture. During a previous enrollment process, the user may have been prompted to perform a "Lite" authentication gesture and may have performed a simple shake of the phone for 2 seconds. As such, the user may simply shake the phone for 2 seconds, the Movement Service may determine that this movement matches the "Lite" authentication gesture that the user previously entered, and the Movement Service may send a PASS signal to the bank web service.

The user may later attempt to log into the same bank web service, but this time from a friend's house. The Movement Service may recognize that the device is on an unfamiliar WIFI network and therefore may prompt the user to perform a "Complex" movement that the user previously specified during an enrollment process. The "Complex" movement may involve more motions and/or a longer duration of each movement.

An advantage of allowing users to enter multiple verification movements is that a computing device can prompt a user to provide contextually-relevant authentication gestures depending on the situation. Users may not be annoyed with entering complex authentication

gestures when accessing a service in environments that pose less threat of attack by a malicious entity, but may have the additional security and peace of mind that comes with having to provide a complex movement sequence when in an environment that poses a greater threat of attack by a malicious entity.

CONCLUSIONS

An interesting aspect of this technology is that authentication can require physical control of the computing device. It would be difficult for a malicious individual to hack a series of movements, given the significant number of data points that are collected by device sensors during user entry of a verification gesture. Consider, for example, an authentication gesture that lasts 5 seconds and involves 4 different position changes. The number of data points collected by the Movement Service during the authentication movement would be based on the number of sensors that capture the movement, multiplied by a rate at which the Movement Service is capturing data. The number of data points could be in the hundreds of thousands, rendering brute-force attacks difficult.

A comparable example in the offline world would be attempting to forge a handwritten signature, but being required to do so at the same speed at which the signature was originally written, using the same pen pressure and stroke, and using the same pen angles and orientation of the pen with respect to the user. An advantage of having physical control over the device into which an authentication gesture must be specified is that a hack or leak of movement data could be remedied fairly easily by a user simply creating a new authentication gesture. In contrast, a data leak that exposes answers to personal history questions can compromise such information forever.

Another advantage of having physical movement encoded and hashed locally on a mobile computing device is that it avoids an attack vector in which a malicious entity attempts to intercept a PIN code that is emailed or texted to a mobile number. Another advantage of the approaches described in this document is that they can provide reduced latency for a user, which provides a faster and more streamlined approach to multi-factor authentication. For example, consider the time difference between a user waiting for a PIN to be emailed or texted to the user and then manually entered into the service application, in distinction to a user being able to immediately move their device in a specific pattern.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when a computing device would record movement of the computing device. For example, a user may need to enroll in a movement verification process before any service is able to ask the user to perform an authentication gesture as its form of multi-factor device authentication. A computing device may not analyze movement of a computing device during an authentication process unless a user has previously requested that an authentication gesture be an option for multi-factor authentication.

As described above, the movement data and various other signals may be stored on the computing device as a hash value, such that the original movement data cannot be recovered from the hash, and movement and context that relate to the authentication gesture cannot be deciphered even were the hash value to be accessed. In summary, the system may be designed so that the user has control over what information is collected about the user, how that information is used, and what information is provided to the user.

ABSTRACT

A mobile computing device such as a smartphone may allow a user to confirm their identity during an authentication process by moving their phone according to a specified authentication gesture. The authentication gesture may be one that the user previously specified during an enrollment process and may otherwise be secret (e.g., the computing device may prompt the user to "Move the phone according to your secret authentication gesture"). In another example, the computing device may specify a type of authentication gesture for the user to perform (e.g., the computing device may prompt the user to "Move the phone in a star shape"). A user may provide an authentication gesture in addition to a username and a password in a multi-factor authentication scheme.