February 04, 2019

Visual approach for secure transfer of user credentials

Patrick Georgi

Visual approach for secure transfer of user credentials

ABSTRACT

This disclosure describes techniques to set up a user account, such as a single sign on account, on a new user device with the use of another device on which the user is already authenticated. The authenticated device displays a QR code that includes encrypted data that includes user credentials and optionally, other information such as wireless access point name and credentials. For example, the data is encrypted using a public key of the new device. The new device decrypts the data using its own private key. The described techniques eliminate the need for a user to enter credentials on the new device.

KEYWORDS

- user authentication
- user credentials
- password
- single sign on (SSO)
- QR code
- barcode
- device setup
- smartphone setup

BACKGROUND

Setting up a new device, e.g., a smartphone, tablet, computer, or wearable device, for the first time requires a user to enter their account password, even when using a single sign-on (SSO) account to log in to the device. Such data entry can be cumbersome, e.g., when attempting

to enter strong passwords (e.g., that use long passwords with letters, numerals, and special characters) on devices with limited data entry capability, e.g., touchscreen devices. While subsequent logins on the new device can be simplified by setting up a device-specific PIN or a registered biometric, there are no such currently no easy options available for initial setup of a device.

DESCRIPTION

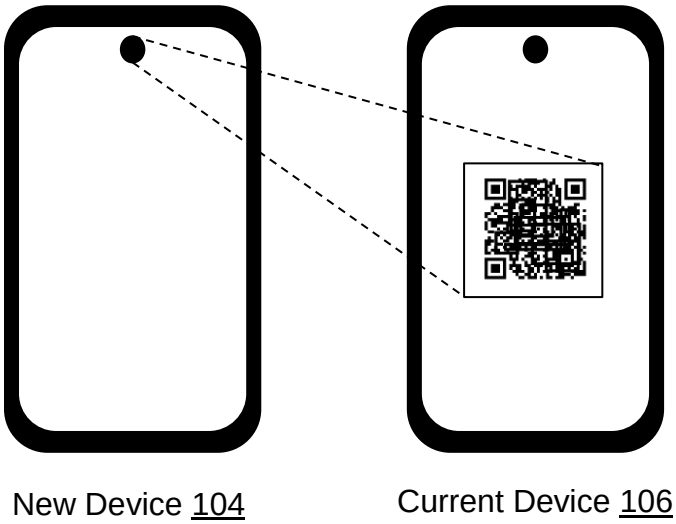

Fig. 1: Copying credentials between a current device and a new device

An example process of user authentication at the time of setup of a new device is illustrated in Fig.1 and described below:

1. The user setting up a new device (104) (e.g., a smartphone with no physical keyboard) has a current device that is logged into a single sign on account. The new device includes a camera. On the new device, the user is prompted with a list of current devices that are available to copy credentials from.
2. Upon user selection of one of the current devices, e.g., current device (106), from which credentials are to be transferred, the user is instructed to operate the current device to

display a QR code that includes user credentials, and optionally, wireless network credentials or other information. The information in the QR code is encrypted using a public key associated with the new device. Generation of the encrypted QR code can be performed on the current device (if the device has capabilities for such operation) or on a server, e.g., that provides user authentication.

3. The camera on the new device is activated and utilized to scan the QR code displayed on the current device. The new device then decrypts the information, and utilizes the user credentials to complete the login process.

Providing key pairs

A new device that utilizes the process described above stores a private key locally, e.g., in a trusted platform module (TPM) or secure enclave. A corresponding public key is made available to the current device or the server. For example, an OEM of the new device may provide public keys. New devices may ship with a short code that the user can enter on the current device, the short code corresponding to the public key of the new device that is being set up.

Generation of QR code

The current device or the server utilizes the selected public key to encrypt user credentials and other information. A QR code is generated based on the encrypted information and is displayed on the current device. For example, the server can provide the QR code to the current device, if not generated locally. Capabilities for generation and display of the QR code may be built into the current device (e.g., as part of the device operating system) or may be provided via an application that can be installed. Local generation of the QR code is performed upon user permission to access plain text user credentials. To generate the code locally, the

current device can obtain the public key of the new device, e.g., via hardcoded values in the application that generates the QR code or by obtaining the public key from a key server. Generation and display of QR code is performed only upon user authentication the current device, e.g., via a biometric or a password. The generated QR code may include a prefix that identifies the purpose of the code and the encrypted credentials. For example, a QR code that includes wireless credentials may be of the form QR(prefix | encrypt(username | password | wifi AP name | wifi password)).

When the QR code is generated on the server, the server accesses the public key of the new device, e.g., based on a short code provided by the user via the new device. The server encrypts the user authentication data including data sent by the client (e.g., encrypted WiFi information), e.g., in the form E=encrypt(username | password | encrypted-wifiinfo), which can then be wrapped with a prefix and a client-specified passphrase (e.g., provided by the current device and usable to decrypt the additional information generated by the current device) in the form QR(prefix | E | passphrase-to-device-encrypted-wifiinfo).

Decryption of QR code

The QR code is scanned by a device camera of the new device and then decrypted on the new device using the device private key. For example, the decryption may be performed by the TPM or secure enclave that includes cryptographic capabilities.

Alternative to use of QR codes, the described encryption-based techniques can also be performed by utilizing device microphone and speaker of the new device and the current device. The audio that encodes user credentials can be output by the speaker, e.g., in the audible spectrum or at higher frequencies that speakers and microphones typically support but are

inaudible to humans. The new device can be set up to send its public key to the current device via the same medium.

As another alternative, ad-hoc networking e.g., Wifi and/or Bluetooth, can be used to provide bidirectional authentication. Further, the visual approach (use of QR code) can be combined with audio or ad-hoc networking based approaches, e.g., the new device can initially attempt to obtain credentials via audio or ad-hoc networking, and if those techniques fail, resort to the QR code based data exchange.

The QR-code based techniques described herein allow presentation of an easy to understand and robust user interface to establish user credentials on a new device. Such techniques can also be more reliable than audio or ad-hoc networking based techniques. The techniques also allow bundling additional information such as wireless network credentials which can further ease setup of a new device. Unlike current new device setup, the techniques do not require a network connection to be established prior to user authentication. Transfer of user credentials as described herein can be used to set up phones, tablets, laptops, and other devices that include a camera, and are compatible with different types of single sign on systems.

CONCLUSION

This disclosure describes techniques to set up a user account, such as a single sign on account, on a new user device with the use of another device on which the user is already authenticated. The authenticated device displays a QR code that includes encrypted data that includes user credentials and optionally, other information such as wireless access point name and credentials. For example, the data is encrypted using a public key of the new device. The new device decrypts the data using its own private key. The described techniques eliminate the need for a user to enter credentials on the new device.

REFERENCES

1. https://chirp.io/