CERIAS

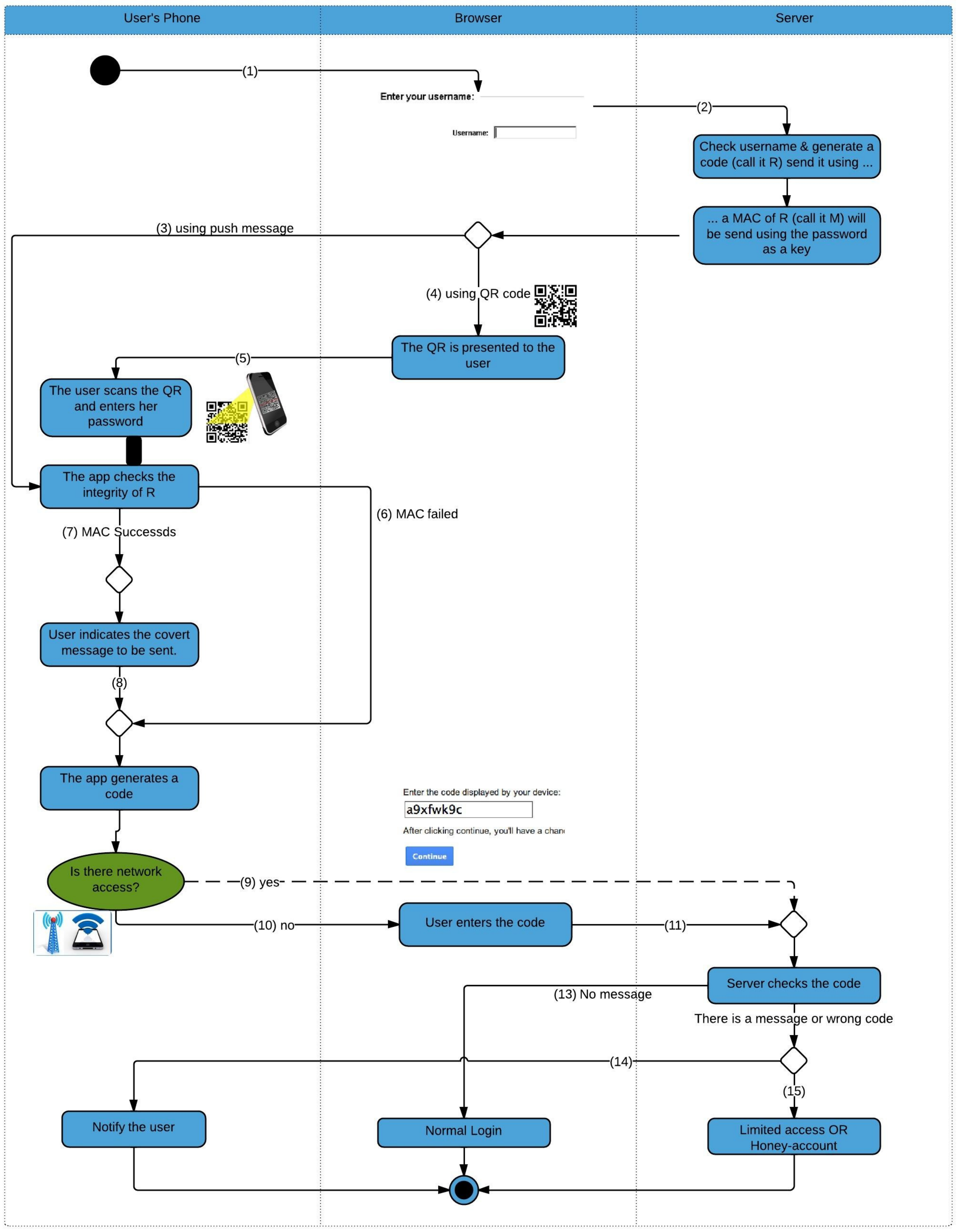
The Center for Education and Research in Information Assurance and Security

The Password Wall — A Better Defense against Password Exposure

Mohammed H. Almeshekah and Mikhail J. Atallah

Abstract

We present an authentication scheme that better protects users' passwords than in currently deployed password-based schemes, without taxing the users' memory or damaging the user-friendliness of the login process. Our scheme maintains comparability with traditional password-based authentication, without any additional storage requirements, giving service providers the ability to selectively enroll users and fall-back to traditional methods if needed. The scheme utilizes the ubiquity of smartphones, however, unlike previous proposals it does not require registration or connectivity of the used phones. In addition, no long-term secrets are stored in the user's phone, mitigating the consequences of losing it. The scheme significantly increases the difficulty of launching a phishing attack; by automating the decisions of whether a website should be trusted and introducing additional risk at the adversary side of being detected and deceived. In addition, the scheme is resilient against Man-in-the-Browser (MitB) attacks and compromised client machines. Finally, we incorporate a user-friendly covert communication between the user and the service provider giving the user the ability to have different levels of access (instead of the traditional all-or-nothing), and the use of deception (honeyaccounts) that make it possible to dismantle a large-scale attack infrastructure before it succeeds (rather than after the painful and slow forensics that follow a successful phishing attack). As an added feature, the scheme gives service providers the ability to have full-transaction authentication.



User's Phone

Browser

Server

(1)

Enter your username:

Username:

(2)

Check username & generate a code (call it R) send it using ...

... a MAC of R (call it M) will be send using the password as a key

(3) using push message

(4) using QR code

The QR is presented to the user

(5)

The user scans the QR and enters her password

The app checks the integrity of R

(6) MAC failed

(7) MAC Successds

User indicates the covert message to be sent.

(8)

The app generates a code

Enter the code displayed by your device:

a9xfwk9c

After clicking continue, you'll have a chan

Continue

Is there network access?

(9) yes

(10) no

User enters the code

(11)

Server checks the code

(13) No message

There is a message or wrong code

(14)

(15)

Notify the user

Normal Login

Limited access OR Honey-account

Characteristics

1. It helps the user to make the right decision whether a website should be trusted before the user submits her password.
2. Resilience against the (unfortunately) common use of using an untrusted computer.
3. A covert channel facility for users to convey information to the server about their status (e.g. under duress) or doubts they harbor.
4. No phone registration, long-term storage, computer connectivity and/or network connectivity.
5. The use of honeyaccounts.
6. Full compatibility (with fall-back ability) with currently deployed password management schemes.

Security Features

1. **The use of Software Protection**.
   Our scheme uses a specific phone application that can have some intrinsic software protection against tampering.
2. **Automated Trust Decision**.
   The scheme aids user in making trust decision about the authenticity of a web page mandating that the website provides a cryptographic proof of their knowledge of the user's shared secret; namely the password.
3. **Transparent Security**.
   The process of validating the authenticity of the website is done in total transparency to the user and the user is only asked to capture the picture of a QR code.
4. **No Stored Secrets on the User’s Phone**.

Comparison with Other Schemes

	no phone enrollment	no long-term secret	resists MitB	no special hardware	no phone connectivity	compatible with existing
Our Scheme	✓	✓	✓	✓	✓	✓
CrontoSign	✠	✠	✓	✓	✓	✠
QR-Tan	✠	✠	✓	✓	✓	✠
hPin/hTan	N/A	✠	✓	✠	N/A	✠
QRP	✠	✠	✓	✓	✓	✠

CERIAS

PURDUE
UNIVERSITY