QR Code Assisted OTP Mutual Authentication Scheme

Researchers: Esia Yosupov, Pradip Karki

Faculty Mentor: Dr. Xiaowen Zhang

Computer Science Department

ABSTRACT

With the increasing security risks of using password for authentication, we propose a secure one-time password (OPT) mutual authentication scheme with the assistant of the quick response (QR) code. QR code is a small two-dimensional barcode image that conveys much more information than the traditional barcode and can be read/decoded by many mobile phones. Our scheme involves two channels for communicating between a web server and a user. When a user logs into a site from a PC, through Internet channel the web server sends the PC browser a QR code image that encodes a one-time cryptographic challenge. The user takes a picture of the QR code image with his mobile phone camera to decode the challenge. Once the server is authenticated, the user's phone generates a cryptographic response which is sent back to the server via wireless channel. The server checks the user's response, if it's verified, the user is authenticated by the server. Finally, server allows the user access his account from that PC's browser. The standard secure cryptographic primitives are used for strong security. The implementation of this secure scheme on the user side is done by using mobile application.

OUR SYSTEM

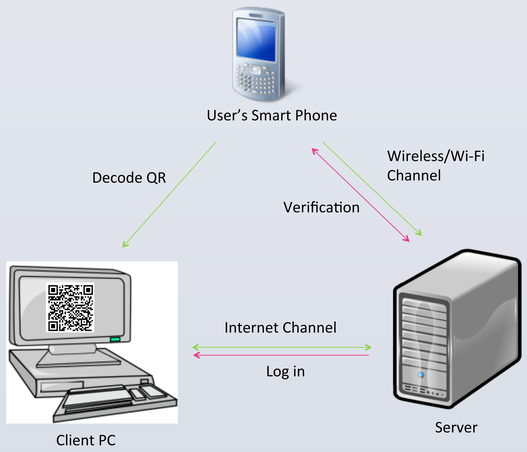

Figure 1: Three way Communication Diagram

METHODS

Account Login:

The login page, a website displays a QR code which carries the information of a random number challenge R_b; and asks the user to snap the picture with his iPhone's camera to log in. Figure 1 shows a mock up of what a website login screen would look like using the QR Code Assisted Mutual Authentication Scheme.

The challenge consists of the HMAC-SHA2 hash of the random number, which is generated each time unique and fresh, using the pre-shared secret as key K_a. The QR code is generated based on the information:

$(HMACK_a(R_b) \| \mathbf{R_b})$

{

protocol: "USER_AUTHENTICATION"

provider: "https://bobbank.com"

random_number: $\mathbf{R_b}$ = "049488575738933838759493 4"

challenge: HMAC $K_a(R_b)$ = "12124627d1166b275696cd6d5322636759283c1fef50aed516d4cbb9f2996685"

}

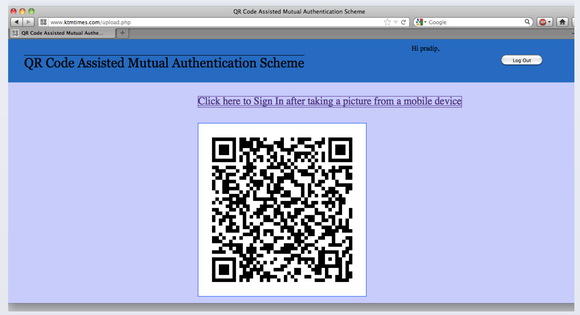

Figure 2: A mockup of *ktmtimes.com* login page displaying QR code for account login

After taking the QR challenge picture, the iPhone decodes the picture and retrieves $(HMACK_a(R_b) \| \mathbf{R_b})$ back. The iPhone calculates the $HMACK_a(R_b)$ and compares the result with the received $HMACK_a(R_b)$. If they match, then iPhone authenticates the website. Figure 2 shows the User Windows Form Application.

The iPhone creates a response $(HMACK_a(R_b \| \mathbf{ID_a})$, which consists of the HMAC-SHA2 hash (using the pre-shared secret as key) of the random number concatenated with username. Then the phone sends the response back to the website via wireless phone channel.

{

protocol: "USER_AUTHENTICATION"

challenge $HMACK_a(R_b)$**:** "12124627d1166b275696cd6d5322636759283c1fef50aed516d4cbb9f2996685"

response $(HMACK_a(R_b \| \mathbf{ID_a})$**:** "20d468ad41c168aadd876db27ed81fe926c82d951b8c1bcdc716f6d7904a8fc3"

username: "alice@gmail.com"

respondTo: "https://bobbank.com/verify"

}

The provider of the website verifies the response by calculating HMAC-SHA2 hash of the random number with username, using the pre-shared secret as key and if successful, then the website authenticates the user. And the browser session is granted for the user's access to his account:

{

protocol: "USER_AUTHENTICATION"

response $(HMACK_a(R_b \| \mathbf{ID_a})$**:** "20d468ad41c168aadd876db27ed81fe926c82d951b8c1bcdc716f6d7904a8fc3"

username: " alice@gmail.com "

status: "OK"

session: "20d468ad41c168aadd876db27ed81fe926c82d951b8c1bcdc716f6d7904a8fc3"

}

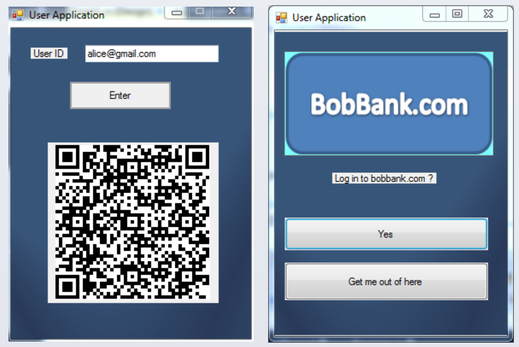

Figure 3: The mobile application
(a) The home screen, with a single button to Enter
(b) Confirmation of a Login

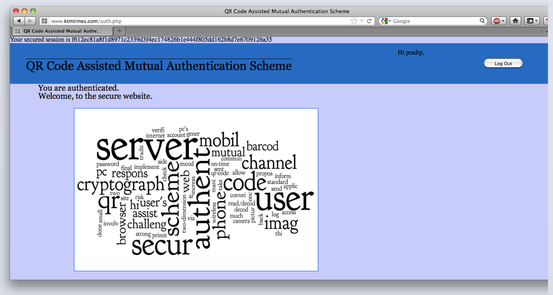

Figure 4: The browser session is granted for the user's access after the website authenticates the user.

EXPERIMENTAL RESULTS

In order to evaluate our scheme, we have created a website written in PHP and a Windows Application that could potentially run on a Windows Mobile Smartphone.

FUTURE WORK

Mobile application.

Integrate with major websites to make their users able to login through this mobile application securely with one time password.

Each component of QR Code Assisted Mutual Authentication Scheme can still be worked upon to further enhance its capabilities.

CONCLUSION

QR Code Assisted Mutual Authentication Scheme, an easy-to-use authentication system is based on one time password. A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs are computer generated random bits, user does not have to memorize them. To eliminate the use of password and to reduce the damage of phishing, spyware, dictionary, and keylogger attacks, we introduce an QR Code Assisted Mutual Authentication Scheme, where a user has "infinite" many random passwords and use each one only once. Even if a single password is compromised, it is useless to the hacker, because it has been used. However, existing practical approaches to one-time passwords are inconvenient and/or susceptible to sophisticated phishing attacks. Although, one-time password systems are already being widely deployed by banks, governments, and corporate private networks to reduce the effects of password compromise, we introduce a new approach of one-time password for a secure mutual authentication scheme with the assistant of the QR code.

REFERENCES

[1] B. Dodson, D. Sengupta, D. Boneh and M. Lam. Snap2Pass: Consumer-Friendly Challenge-Response Authentication with a Phone. http://prpl.stanford.edu/papers/soups10j.pdf

[2] K. Liao and W. Lee. A Novel User Authentication Scheme Based on QR-Code. Journal of Networks, VOL. 5 NO. 8, August 2010.

ACKNOWLEDGEMENT

This study is supported in part by NSF STEAM Award.