Multi-factor Authentication

Student: Colin Wingfield Callahan

Advisor Dr. Eduardo B. Fernandez

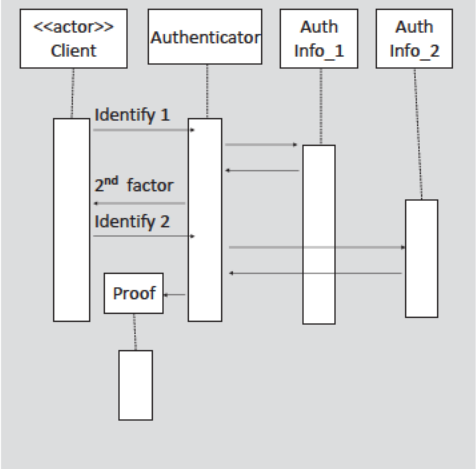
FAU
DEPARTMENT OF COMPUTER & ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
College of Engineering & Computer Science
Florida Atlantic University

Abstract

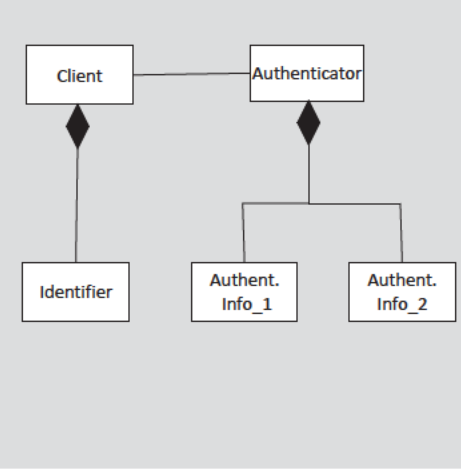
An important authentication method is multi-factor authentication (MFA). Products such as Enterprise Office 365 are already using it, available for any user in Office 365 Midsize Business, Enterprise, Academic, and Nonprofit plans as well as the standalone versions of Exchange Online and SharePoint Online. The log-in verification feature is aimed at reducing users' vulnerability to online identity theft, phishing, and other scams by adding a second level of authentication to an account log-in. After correctly entering their username and password, users need to acknowledge a phone call, text message, or an app notification on their smartphone before they can gain access to their account. Two-factor authentication is the most common form of MFA and requires the use of two of the three types of authentication factors: Something only the user knows, something the user has, and something only the user is. In this work we will analyze some varieties, build UML models of their structure and dynamics, and compare MFA to other authentication approaches.

Introduction

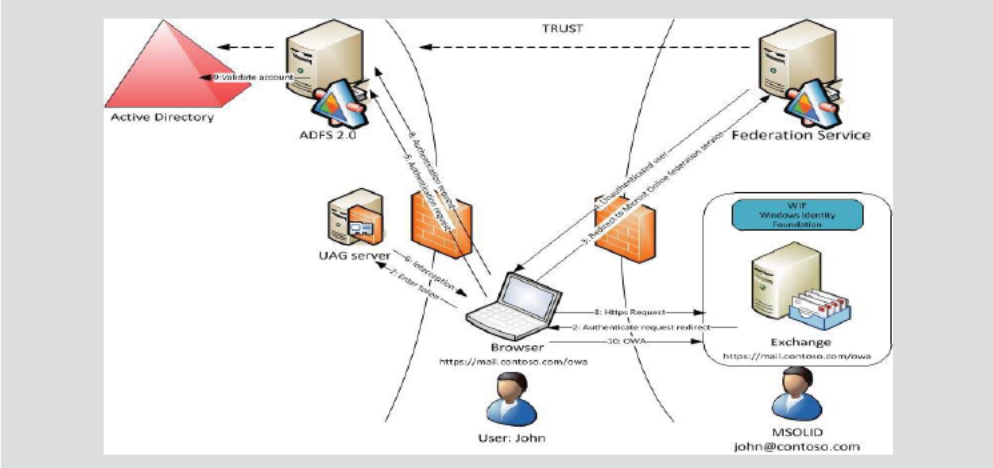
Authentication is needed to make sure that legitimate users access a system. Most vendors use a single-factor authentication, typically passwords. However, most users undermine this security method by selecting bad passwords (easy to guess) making it easy for attackers to hack in a system. Instead, we can use two-factor Authentication, using two of the three authentication factors: something the user has, something the user knows, and something the user is, to make systems more secure by adding another factor to the log-in verification so even if the attacker guesses the password he still has to go though anther verification to get in. For example, Google can send you text messages, with a code sent to your phone every time you log in (something the user has) or as most banks use for their online banking a security question that only you can answer(something a user knows). We will analyze the value of this approach as compared to a single-factor Authentication



Sequence diagram for use case Request Authentication



Class diagram for Two-Factor authentication



Office 365 Multi-factor authentication

Known Uses

-Windows

Will send a new security code to your phone or your alternate email address

-Google

a code will be sent to your phone via text, voice call, or our mobile app. Or, if you have a Security Key, you can insert it into your computer's USB port.

-Bank of America

You will be asked three random questions that only you know the answer to.

-Apple

You can only sigh in through an approved device and your Apple Id.

-Department of Defense

Uses the YubiKey along with a one time password

Conclusion

This analysis will help us understand why **Multi-factor authentication** can be used as a secure, cost effective, and flexible way to prove users identity in a reasonable time frame in comparison to biometric or smart cards. And though the single-factor does cost less and is faster it does not have the same level of security that the two-factor can provide.

References

Two-step verification: FAQ - Windows Help (windows.microsoft.com)http://windows.microsoft.com/en-us/windows/two-step-verification-faq

2-Step Verification (Google) https://www.google.com/landing/2step/#tab=how-it-works

Apple (FAQs about two-step verification for ID) https://support.apple.com/en-us/HT204152

Department of Defense Contractors Replacing Legacy Two-factor Authentication with YubiKey (Yubico) https://www.yubico.com/press/press-releases/department-defense-contractors-replacing-legacy-two-factor-authentication-yubikey-2/

E.B.Fernandez, *Security Patterns in Practice: Designing Secure Architectures Using Software Patterns*. Wiley, 2013.

DISTINCTION THROUGH DISCOVERY