Security in Gaming, How Protecting Your Gamers Can Be as Simple as 1.2.3 by Simon Thorpe

Author: Gruber Thomas

February 14, 2017

Tags: Gaming, Security, Passwords, 2FA, Cloud Service
Track: GDC 2016 - Programming
Url: http://www.gdcvault.com/play/1023595/Security-in-gaming-how-protecting
Speaker: Simon Thorpe, Authy a Twilio company

Abstract

This paper deals with the problem of using passwords for the authentication in games and introduces a new two factor authentication service called Authy. In addition some common guidelines for players are discussed when dealing with accounts. Finally a new approach to user authentication for mobile devices is presented that could be used to enhance security in many applications.

1 Summary of Talk

Security has become a main issue in nearly all applications that we use nowadays. In most of the systems we have to authenticate us before we can use any service. Since there are more and more online games and standalone games were some data has to be stored on the servers, security is also very important in gaming. Many games also use in game purchases, where the gamers could buy some items or unlock features by paying with real money. Due to that fact, attacks on game accounts increased drastically over the past few years. If a password is stolen, some private data could be extracted from the corresponding game account. The main problem in authentication is that all users hate passwords and should remember passwords for different accounts. A survey showed that most of the users use very weak passwords because they are more likely to be remembered. But on the other hand unwanted persons could easily steal these passwords, and that is the core problem.

1.1 Two Factor Authentication

Two Factor Authentication (2FA) uses two pieces of information for authentication. The typical form of 2FA is that you know this information, for example a username or email and a password. The problem here is that also other could probably know this information. Another way of doing 2FA is that you have something physical like a chipcard or an encrypted token generator. The third possibility would be to use unique aspects of yourself to authenticate.

Over the last decades there had been many different approaches to perform 2FA. At the beginning there were hardware based token generators. After the invention of mobile phones, it was possible to send voice or text messages with one time password codes. Since the evolution of smart phones, applications on that mobile devices could be used to do 2FA. The problem of older 2FA mechanisms was that someone had to either buy these token generators as used for example in World of Warcraft or that the authentication was not secure when using email verification for logging in. Another disadvantage of such approaches is a very bad end user experience because the user often does not know what is actually really going on.

1.2 Better way of 2FA

With a newly presented application called "Authy" there is a better way of doing 2FA in modern use cases. To demonstrate the capabilities of Authy it was integrated in a Minecraft server to authenticate the user in the game. If the user wants to login onto the server, a push notification is sent to the user's mobile phone. On the smart phone some details about the authentication

process are shown and the user is able to approve or deny the request. The main advantages of this mechanism are that the end user is informed in detail what is happening and he can respond immediately. Apart from the login process, it is also possible to protect in game actions or any kind of process with this approach.

Authy was designed to provide stronger authentication for comsumers, communites and administrators. It could also be used for transaction security, for example to protect worlds or for in game purchases. The service also supports older 2FA methods for one time password codes like voice or sms.

The service can be integrated in any kind of application where calls via a REST API are supported. So Authy is a cloud service that it accessible from everywhere. There is also a client app available for all mobile platforms that handles the push notifications and interacts with the end user to approve or deny the authentication request. Further there exists an Authy SDK to support the creation of own mobile apps that handle the user interaction. The service itself manages security, monitoring and 2FA support through API. Especially the push logic is very likely to be attacked so in this part secure communication is provided by Authy. The main thing to remember when integrating Authy in your application is that you own the application and the users in terms of software design and just use the cloud service to perform 2FA.

Using Authy is very easy und just requires three main steps to be performed. There are interfaces for many common programming languages, so performing these steps will work throughout a variety of projects. First a user has to be registered in Authy with corresponding email and of course a phone number. This call returns an authy id for this registered user that should be stored in the current application (e.g database). If authentication of a user is required at some point, an approval request is sent using the stored authy id from before. In the last step the callback of the request is used to get the result and perform some action. Following this approach Authy can be used in different applications and games to provide user authentication in a more convenient way.

2 Overview and Relevance

In the year 2016 there have been many cybersecurity incidents where organizations, companies and also individuals were involved. It was a bad year for password security because a lot of data was leaked or stolen by cybercriminalists. The attacks exploit the fact that users still prefer passwords that can be easily remembered instead of secure passwords. So the current developements in authentication methods explore other methods that reduce the reliance on passwords to reach a higher security level. Two Factor Authentication, biometrics and other techniques are becoming even more popular. [1]

With the growth of online gaming, game accounts also became a huge target for cybercriminal attacks. Virtual economies evolved inside games where players are trading with virtual items and currency. These items are then selled outside the game causing some exchange of real world money. Due to that fact, stealing an identity or getting access into one's game account is a main issue for cybercriminalists. There are a few tips aside from authentication mechanisms that players could follow to ensure privacy and security. When signing up for a game account, players should determine whether it is really necessary to provide their real name, address or email address for this purpose. Another very important point is that players should not link credit or debit cards to a gaming account if they are not interested in buying in-game items or things like that. Using security software on every system and not using game account credentials to log into unverified or untrusted sites or apps are general recommendations to protect the privacy in any case. [2]

2.1 Multi-faceted approach to user authentication for mobile devices

In the two factor authentication service called Authy, which was introduced above, a mobile device is used to approve or deny an authentication request. In the worst case this mechanism could also fail if any unauthorized user gets access to the mobile device, for example if it is stolen. Therefore a new multi factor authentication approach for mobile devices called mAuth could be really helpful. With this approach, the user is continously and unobtrusively authenticated while the device is being used. Low-level sensor data is used to extract some typical behavior of the end user in the high-level context via machine learning algorithms. In detail, frequently visited places, physical proximity with the device and gait patterns are fused to create a dynamic trust score. This score determines whether the user is trustworthy or not to access different applications. It turned out that if sufficient sensor data is available, the system is able to detect an adversary in less than one minute. [3]

So when combining an appropriate 2FA mechanism with this method for mobile devices it would be possible to make many applications and games more secure.

3 References and Further Sources

[1] Looking Back, Moving Forward: Cybersecurity Resolutions for 2017
https://www.trendmicro.com/vinfo/us/security/news/online-privacy/looking-back-moving-forward-cybersecurity-resolutions-for-2017
last visited: 14.02.2017

[2] Data Privacy and Online Gaming: Why Gamers Make for Ideal Targets
https://www.trendmicro.com/vinfo/us/security/news/online-privacy/data-privacy-and-online-gaming-why-gamers-make-for-ideal-targets
last visited: 14.02.2017

[3] Devu Manikantan Shila, Kunal Srivastava, Paul O'Neill, Kishore Reddy, Vincent Sritapan. "A multi-faceted approach to user authentication for mobile devices - using human movement, usage, and location patterns". *2016 IEEE Symposium on Technologies for Homeland Security (HST), 2016*