An Analysis of Twitter's App Based Two-Factor Authentication and Recovery System

By Alexander Tong
December 2014

Abstract

This paper attempts to analyze the potential of app based two-factor authentication systems that move away from the now well-known SMS-based one time password (OTP) two-factor authentication systems. Despite the popularity of such systems, and their acclaimed security, this paper will discuss the security flaws in these SMS-based (OTP) two-factor authentication systems, and the costs and benefits of moving towards app-based systems that use public and private key pairs for identity authentication.

Introduction

Background

In May of 2013 Twitter rolled out SMS-based two-factor authentication as an introduction of two-factor authentication to the Twitter community. This SMS-based authentication system was meant only as a stop gap for users as the developers at Twitter had their eyes set on a new type of two-factor authentication, one that might mitigate the problems of the already well used OTP systems like the Google Authenticator. In August of 2013 Twitter released their app-based two-factor authentication, along with a system allowing access without access to the linked mobile device, one of the most notable problems of OTP two-factor authentication systems.

Authentication

At its heart, authentication is verifying identity. It is the mechanism to prove that you are who you claim you are. There are a few accepted verification categories: what you know, what you have, and what you are. There are many ways to use each of these categories to verify identity, providing authentication for the server. Some examples below (Aloul):

What you know:	Username/Password, Security questions
What you have:	Credit card, RFID key
What you are:	Biometrics, unique device IDs

These three categories have been traditionally used standalone, and in their own right are fairly secure, but nowhere near completely secure. With two-factor authentication, we use multiple authentication systems using distinct categories to increase the difficulty of malicious attacks. Two-factor authentication, as we know it today, is generally a combination of what you know and what you have, requiring both a password, and access to a physical device.

Google Authenticator

Google Authenticator is project which uses SMS based two-factor authentication to log on to Google based apps and third party applications. Older versions are open source, while Google owns newer versions. The Google Authenticator manages the sending and use of one-time, time-based passwords sent over SMS to a specified mobile phone owned by the user. The one time password expires over a short time period to prevent attackers from

gaining access using that passcode. While this sort of two-factor authentication is certainly more secure than a simple password based system in that it also requires access to another code, it is still vulnerable to a man in the middle attack (MITM), where it is possible to capture the one-time password (OTP) sent by the server to the phone of the user. This vulnerability to a MITM attack is inherent in all SMS based two-factor authentication system.

Authy

Authy is an app-based two-factor authentication system, which is based on the original Google Authenticator, it uses OTP authentication but with the added ability to sync across devices including PCs. This function successfully mitigates the problems associated with lost and broken mobile devices allowing two-factor authentication to take place on a laptop or any other device. The main problem with such a service is that critical keys must be stored on Authy's servers, and while this information is only ever transmitted and stored in encrypted format, there is still the possibility of an attacker gaining access to this data.

SMS-based two-factor authentication drawbacks

One time passwords sent over SMS have a few drawbacks, which are inherent in the system

1. The cost of sending SMS, for each login attempt the server must send an SMS to a phone, which as the system scales, because a large cost consideration.
2. SMS messages may get delayed, especially roaming internationally; there is no time guarantee of SMS delivery.
3. International Roaming, SMS is not available over the entire globe, and even in the future, where SMS may be available everywhere, the international roaming and data charges may restrict the ability for the user to receive an SMS message.
4. SMS accessibility, if the user loses or breaks the associated phone than in most SMS based systems it is very hard to access the account.

Two-Factor Authentication MITM vulnerability

If an attacker can gain access to the first level of protection in the two-factor authentication scheme, the main password, then it is not that much harder to gain access to the second form of authentication if the second factor is a one-time generated password because this generated password is a shared secret between the user's mobile device and the server. This means that an attacker, who has gained access to the server, can still compromise this one-time password, even if it is sent over an encrypted stream.

To The Community

Two-factor authentication is an important step towards secure authentication, but it is by no means the end all of authentication. While it is more secure than traditional one-factor methods, it only will slightly increase the overall security of the system. We come to a paradox where if we had a secure, foolproof method of single method of authentication,

then we would never need a two-factor system. However, since two-factor authentication is built upon two inherently insecure factors, the two-factor system, while possibly more secure, is still inherently insecure. Thus while two-factor authentication is an important step in the process, in the long run it provides no more assurance than single factor systems.

Currently, we know of no sure method of authentication—any system, which we can put in place to authenticate a user, can be bypassed. A password is 100% secure, until it's cracked. Similarly, all authentication systems work correctly, until someone manages a way around that system, and by definition, that system will have no knowledge of that bypass. Two-factor authentication, since in a perfect world it requires authentication of two types, knowledge and physical, it might stay secure for longer and for more accounts, but it will eventually be circumvented.

Essentially, the message here is that no matter what kind of authentication we use, there will still be successful imposters. Whatever system is in place will deter some malicious attacks, but that system is never 100% secure. While two-factor authentication is an important step towards securing any system, it only reduces the probability of a successful attack, and all the systems that respond to such an attack must still be in place whatever authentication is used.

Twitter's new two-factor authentication system is a step in the right direction for two-factor systems, but it will not solve the underlying problem and tradeoff of such systems—usability vs. security. While two-factor systems are certainly a more secure option, all currently available options are harder to use than traditional single-factor systems. The security provided by two-factor authentication makes any service that uses it harder for the average user to access and this fact alone will probably prevent the wide spread adoption of two-factor systems.

By removing the shared secret required by time based OTP systems for two-factor systems twitter has improved both the usability, the user isn't required to enter in an extra string of characters during each login, and security, the one time password cannot be intercepted in transit.

How it Works

Twitter's solution

Twitter's solution to the drawback of OTP based two-factor authentication is based on the premise of removing the need for a shared secret between the server and the user, as any authentication system that relies on a shared secret between the user and the server is inherently vulnerable to a MITM attack. Following this premise, Twitter developed a method using the well-known system of RSA private and public key pairs to keep the "secret" on the user's mobile device. When a user attempts to login to twitter's services using two-factor authentication, the server is able to send a login request to the user's mobile device with information about when and where the request was made. Then the

user is able to either approve or deny the requested access from the mobile device knowing some contextual information about the login attempt. This system means that the server never needs anything other than a public key to the user's mobile device for successful two-factor authentication. Therefore, in the event of a compromised server, an attacker can gain no useful login information and the relevant accounts will stay secure.

In the case that the user loses access to the device the account can still be accessed with a separate backup authentication system, which uses multiple hashing to provide a one-way function allowing the system to be accessed up to n times, where n is the number of hashes used, before the password is compromised. This backup authentication system has been used before and is the S/KEY one-time password authentication system (Aloul).

The backup system's main disadvantage is the computational power required by the client side device. The client must recalculate up to n-1 rehashes for each access of account using this method, and for this reason it is too computationally intensive to be used as a primary method of account access. Its benefits, however, are in its security of the client password, which need never leave the user's device.

Conclusion

Only a small percentage of total users are currently using two-factor authentication, even though all signs point to two-factor authentication as an important step towards more secure systems. Most users simply cannot be bothered with two-factor authentication. In a study posted by SafeNet, they raised the statistic that at over 80% of the companies surveyed, less than 20% of employees used two-factor systems (Whitepages)

Two-factor authentication is an important step in the direction of higher security systems. However, we will not see widespread adaptation of this technology as long as it substantially decreases usability. The only way to increase use of two-factor systems is to make those systems easier, simpler, and faster to use. Twitter makes a step in the right direction by allowing two-factor authentication without the use of unreliable SMS communication of an OTP, and without the need for a user to enter such a password, no matter how simple.

There exists a general consensus that two-factor authentication is more secure than traditional systems. So the question is, why don't more people use two-factor systems? It comes down to usability and an unwillingness to adopt a less proven method. A common question that most new two-factor authentication users have is what happens if I lose my two-factor device? Twitter has a better solution to that problem, but not a complete one. In the end two-factor system's are continuously evolving, Twitter's method is an example of a well thought-out contemporary implementation, but there is no doubt that in the future there will be more useable and secure methods of two-factor authentication, and hopefully along with it, more users.