Research paper about 3D Secure Authentication v2 for IoT devices. Waves Application

Semih Yönet
Information Systems Engineering
Istanbul Technical University
İstanbul,Türkiye
semihyonet@gmail.com

***Abstract*—Current authentication systems are very lacking, fraudulent attempts are still penetrating the system even with the advancements made with their high security walls and impossible to access databases. The reason of these fraud attempts succeeding is not the fault of the system, it's the fault of the user because of the passwords they pick. The passwords are formed with guessable already existing words perfectly copied from dictionaries. When the account is penetrated all of the user data can be accessed including credit cards. This is where the 3D secure authentication kicks in. Even if you have access in to an account you can't purchase anything with the account if 3D secure is implemented in to the system. But that's not good enough.**

In this paper I would like to give a proposal for a better and safer authentication mechanism for using 3D Secure.

I. INTRODUCTION

3D Secure has been the additional security layer for online transactions. It was developed by Arcod Systems and first used in the systems of Visa. Since its development it has been implemented in most of the current bank systems and it is been a widely used feature because of it's benefits.

This protocol has 3 different domains. These three domains are the following:

1. Acquirer Domain
2. Issuer Domain
3. Interoperability Domain

1) Its where the merchant and the bank is, for getting money from the user.

2) User is located in this domain.

3)This is the domain between the Acquirer Domain and Issuer Domain. The infrastructure of this part is gathered from the debit, credit, prepaid or any other types of cards. This domain has Internet, Merchant Plug in, access control server and any other providers for softwares.

This 3D secure protocol also includes a pop-up window for online transaction processes. This is how the authorization happens in this system. In most cases there is a verification code required which has been sent to the user in ways like E-Mail or SMS code. User enters the code and proceeds to the transaction. However this pop-up window has the banks Interface which can be copied and make the user think that a fraud site is a legitimate site since there is no extra work required for different sites. The bank interface for this purchase is the same for any 3D Secure available web site.

To prevent fraud attempts in these pop-ups the banks have implemented 90 second countdowns and also more specific messages for with the details of the specific purchase to be sent in to the mails and phones. To help users to identify fraud attempts.

The problem I want to focus in this paper is the lack of ways in identifications for 3D Secure authorizations in all IoT. It's really easy to pass this 3D Secure System if the personal phone of the user is stolen. Since most of the personal phones have already sign in into the web sites which already have credit cards of the user and even if 3D Secure authentication is required since the thief has the possession of the users phone it is really easy to access into SMS messages and already log on e-mail accounts to get the verification code for 3D secure and authenticate copying the users information.

It is needed to accept that every security measurement can be passed by frauds. In the case of 3D secure since all required steps for authorization are mostly the same for all banks and systems and the required steps are way less to call it secure since the banks priorities are also for fast transactions therefore they don't require more than 2 steps in 3D Secure transactions.

In this paper the proposed solution to prevent these kind of fraud attempts and making 3D Secure more Secure by giving more steps and creating another domain focusing solely on authentication for IoT devices.

Contributions of this paper will be making 3D Secure more

- Secure
- Trustable
- More Undoable Mistakes

By implementing an app for users and giving the requested code from the app if the required steps are completed.

II. Related Work

To achieve the proposed solution. It is required to combine 2 different 3rd party app services. We need the system of E-Wallet applications with 3D Secure to combine with Non-payment required OTP (One Time Password) authorization systems.

A. E-Wallet Apps

E-Wallet apps are generally used for transferring money from one person to another without an interface between them. These kinds of systems also require 3D Secure Authentication for money transfer. These apps have the users credit, bank or debit card initialized or have an in-app balance which was installed by its user. If the user is using one of the available methods and has done all the authentication steps the money transfer is completed within its money transfer bank system.

An example for a popular E-Wallet app is "Tosla Kart" which originates from Turkey and has been widely used by university students all over Turkey and have been preferred because of its fast – easy to use nature. It also offers 3D secure protocols. Can be used to send money between people with only a click.

B. One Time Password Authorization Systems

Non-Payment Required Authorization apps with OTP (One Time Password) are widely popular as an addition for secure Logins to accounts. This system is built specifictly for a product and before use it needs the user details for authorization and setting up the system. After set-up is done it links the authorization app with the service and in every log in into the service it requires the One Time Password from the app which resets in mostly a minute in to a new password. So with the help of this app there are more steps required to log in therefore its harder to crack.

Most bank apps give this service for people who request safer approach for logging in purposes in to their app. Google also operates this service named Google Authenticator which provides a 2 Step Login mechanism for new devices requesting to use its app. This app is available on both Google play and App Store. Once authenticated it prints out 9-digit string codes including the alphabet and integers which changes every 90 seconds.

C. Why my project is needed

Since the version 2 of the 3D secure, the protocol has been prioritizing speed over security since that makes banks earn more money but the system should prioritize secure transactions and trusted authentications since that's what the users want from 3D secure. There needs to be a system which prevents unwanted transactions even in the extreme scenarios like getting your phone stolen with no passcode in your phone. This is what users are scared of and to prevent that scenario what we need is the combination of the previously told systems with a user-friendly approach.

D. Difference from already existing systems

My project will combine the sections A and B. Main difference from the 3D secure will be that my projects main priority will be security and will have increasing amount of steps to go through for transactions. Lost time on increased number of steps will be neutralized by the user friendliness of the user interface therefore it will provide a better User experience even if there are more steps and will be more pleasant to work with then the 10 year old pop-up HTML pages which was designed for fast back-end - front-end connection which, most of its users consider "Hard to navigate with.".

By giving customization options to the users, this project will be nearly impossible to replicate; since its different with all of its users. It will be user friendly, customizable and most importantly secure. Requiring more steps to complete for this system.

III. My Solution- name:WAVES

My solution for the previously mentioned problems of 3D secure will be Waves. This name symbolizes the priorities of this system. This app will handle every wave different. Wave symbolizes each different transaction. Each wave has its own height and the height of each transaction is determined by the following:

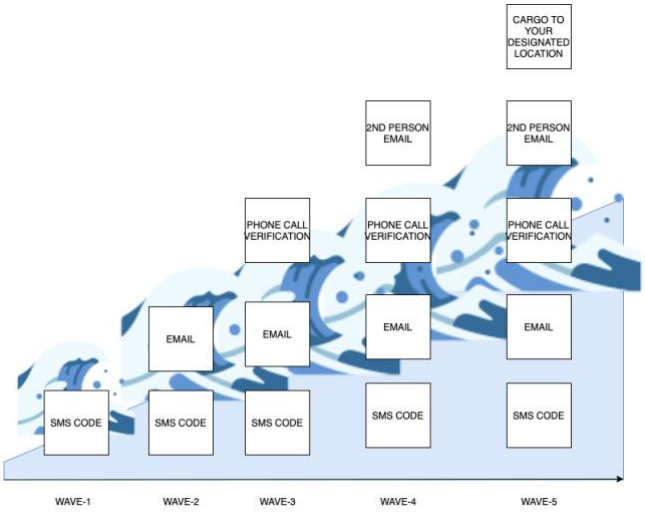
1) Amount of money requested.
2) IP of the request.
3) Last time app has been used.

Whether you are buying a 1000$ guitar or a 150,000$ art piece, 3D Secure version 2 will request a phone verification or a email verification but that's it. Maybe the bank might block this purchase but if the 3D Secure handles these different scenarios with different protocols fraud attempts could be prevented in a more secure and different manner.

What my solution provides is a reactive platform changing request with the change of the transactions. This solution is designed to be an Application available for App Store and Google Play which provides accessibility for all of its users.

This app will provide a One Time Password (OTP) at the end of its authorization processes and it will be used just like the default SMS or Email verification but way more secure since if your phone is stolen then it is very likely for the thief having access to your SMS Codes with the help of Waves ,3D secure can be secure for both the client side and the user side for every user.

A. Different Requirement Steps for Each



(Figure1) Wave Schema

As iterated in Figure1 different waves have different approaches for them. These wave attributes change with the elements of 1), 2) and 3) iterated at the start of this (III) section. These will determine the height of the wave and how many confirmations does it need to be completed for the OTP to be given.

For an understandable measurement on how does the algorithm of the app decide between which wave formula to assign for the transaction, I've given the difference between the amount of the transaction if the section 2) and 3) have the best possible value; What I mean by that is if the transaction IP has been the same for a while and the app has been frequently used over a long period of time and no problem or fraud attempts hasn't been recorded about these transactions then only thing changing a wave formula would be the amount of money which will be spent. Here are the values:

Wave 1	0-500$
Wave 2	501$-3,000$
Wave 3	3,001$ - 15,000$
Wave 4	15,001$ - 50,000$
Wave 5	50,001$ and more

(Table 1)

Note: these values are default values and can be changed

B. Breakdown of Waves

These wave intervals have been decided considering the price of daily needed items, hobby items and items needed after long periods of time. Wave 1 is designed to be fast for daily needs therefore it does not require more than 1 requirement in its formula. Wave 2 is designed for hobbies and rents. Wave 3 and wave 4 are designed for Cars, Rents, Hotels and expensive hobbies generally. Wave 5 is designed for mainly Real estate and Cars

With different wave formulas there are different requirements. Currently there are 5 types of different requirements available in combinations within a formula. These requirements have been decided and formulated by these standards:

- Accessibility
- How Personal it is
- Correct Authentication percentage.

These attributes indicate these following procedures to past the authentication:

SMS Code: It's a code sent through Short Message Service. This type is highly accessible and most likely will be delivered to the Phone where the app is open.

E-MAIL: It is sent to the preferred mail address of the user. This is more complicated and less accessible than Short Message Service (SMS) code.

Phone Call Verification: This action requires a phone call with an automated voice line. It will give the transactions details and end with asking for a verification word just like a password. Since voice recognition A.I.'s are highly developed and automated search engines are currently working as an answering machine in bank lines, implementing it is not hard and can result in a better authentication. It will also record persons voice so in the case of a fraud succeeding there will be a record of the frauds voice and it will help extraordinarily in identification of the fraud in a criminal case.

2nd Person E-Mail: Even if all accounts of user is stolen and the thief can pose as the user without getting recognized. Then setting a relative or a close friend can prevent any more fraud attempts.

Cargo To your Designated Location: If everything is against all odds and the system has been tricked and the fraud has all the accounts. This measurement will be the last row of defence for the Wave Authorization system. Preventing your millions to be stolen this requirement will send your code printed in a paper within a sealed post to your preferred location. This option will also prevent bad decisions since it makes its users wait for the cargo to arrive before spending hundreds of thousands of dollars.

IV. ANALYSIS OF WAVES

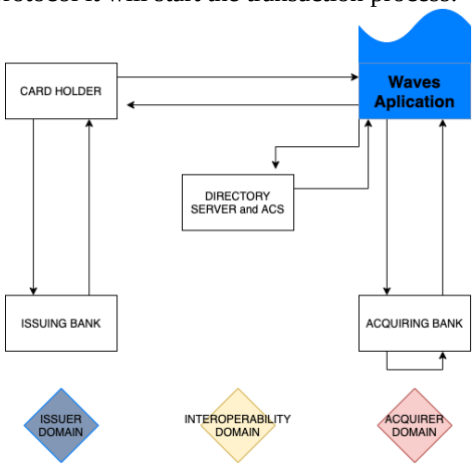
What happens behind the scenes

This part will be featuring details of what happens in back-end during a transaction process.

a) 3D Secure

For this application to work the most essential input is the input from the 3D Secure service which informs this application with the details of the transaction and if the connection has been verified and successful

Waves application will be contacted by the Card Holder and Directory Server. With the details provided by the 3D Secure protocol it will start the transaction process.



(Figure2) Waves 3D Secure FLOWCHART

b) Waves Authorization

The transaction details will be transferred in to the system of the application. Then the validity will be inspected by connecting to the interoperability domain once again from the Waves Application. If the validity is proved, then the algorithm of the application will break down the details of the transaction.

These details are used to pick a Wave considering the attributes inspected in the III.A) section. When the wave is selected, the user will be asked to authenticate in one or more ways depending on the size of the Wave.

Since authorizations will be done in various ways there needs to be many services available from cargo services to SMS send services. As the process numbers rise, the complexity of the authorization code sent will decrease. Since the users will be entering multiple codes they might be frustrated if they need to type up to 15 letter length codes with special characters within them. For example:

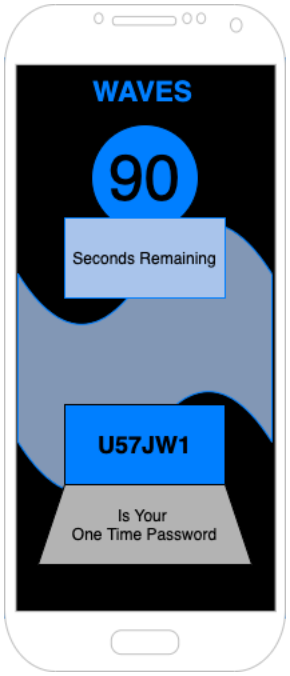
- Wave 1 SMS Code: uAdj$1*39Asgd0
- Wave 2 SMS Code: 394823

c) Back to 3D Secure

If all required steps are valid and correct then a connection between the 3D Secure System and the Waves Application will be connected. A One Time Password will be created between the system and the 3D secure.

This code will be simple since the person only has 90 seconds to enter a code into the 3D secure system. This text will mean that the person passed all authentications and is rightfully proceeding to the transaction.

How the code prints out in Waves UI:



There will be a countdown happening in both Waves application and the 3D secure application.

The code will be presented in a no special characters and no capital lettered format.

Once the code is copied into the 3D secure Protocol then the Issuing bank will send the money into card holder card holder will sent it to waves and waves will send it to the Acquiring Bank where the transaction will be completed.

a –> b -> c

V. CONCLUSION

This app will make 3D secure more secure as it puts more authentication layers into the transaction.

It might result in some lost seconds but the thanks to Waves application you will gain thousands of dollars and years work just by spending some more minutes for a transaction.

Fraud attempts will be avoided since it needs way much authorization. It will provide a flexible authentication schema since most of frequent purchases will only need an SMS code since most transactions are bellow 500$ margin.

Fraud attempts which try to phish by posing as an 3D Secure pop up window will be prevented by adding another security layer.

REFERENCES

[1] https://tosla.com
[2] https://www.google.com/landing/2step/#tab=how-it-works

3D Secure
https://securionpay.com/blog/3d-secure/
https://en.wikipedia.org/wiki/3-D_Secure
https://www.verifi.com/kb/what-is-3d-secure/