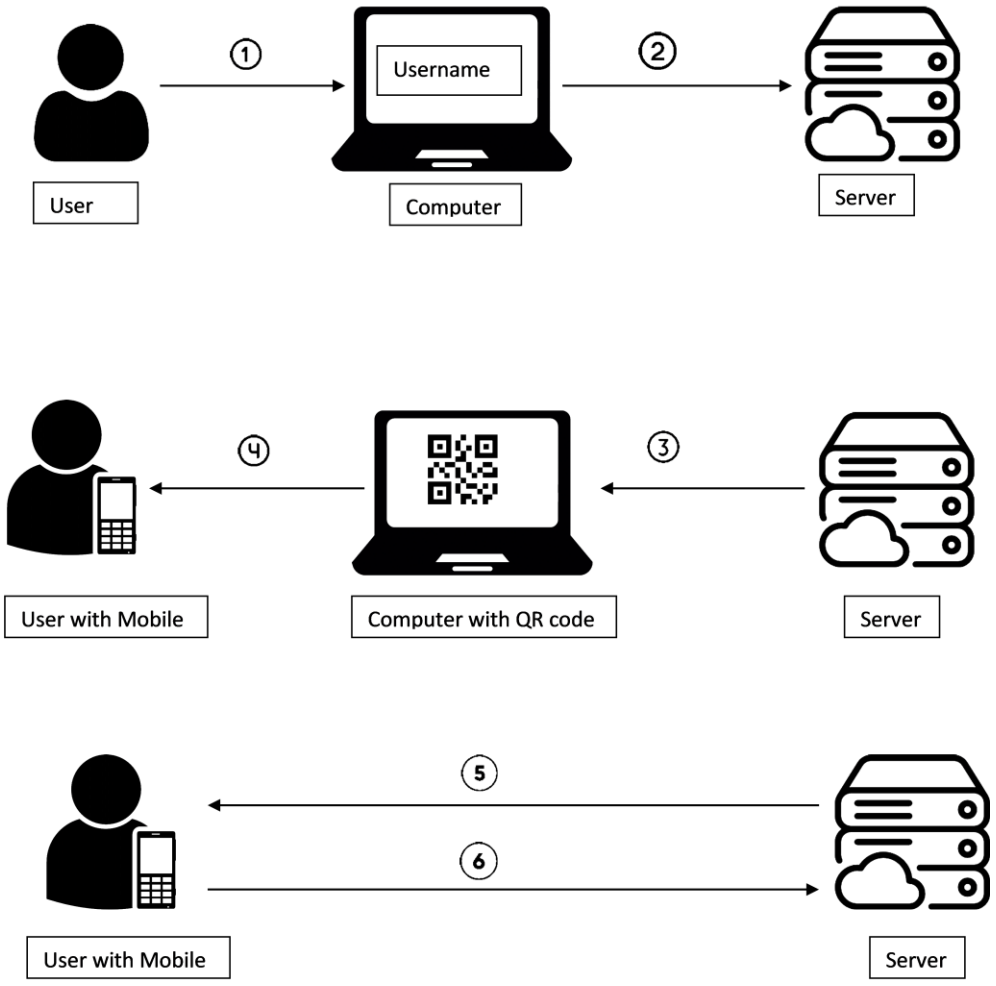
Anti-Spoofing

Sign Up Process



0 Spoofing, Sign Up Process:

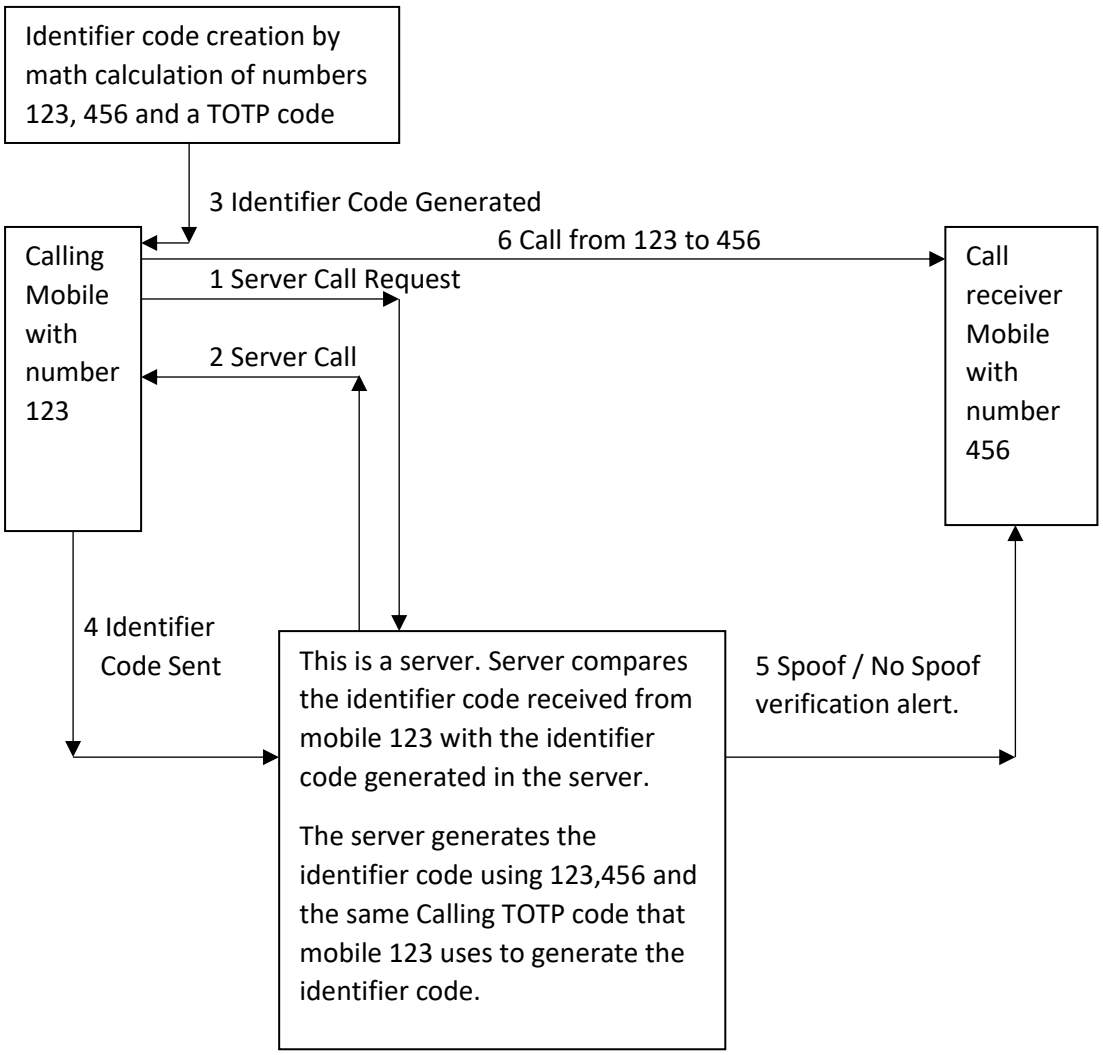
1. User inputs his username and other details on a website.
2. This username is sent to the server.
3. The server responds back to the website with a QR code containing seed record of a TOTP Time based one-time password generator, called as Signup TOTP.
4. The user scans this QR code with his mobile. So that now both the mobile and the server contain the same seed record of the Signup TOTP code generator.
5. The server calls the mobile in 5th step.
6. In 6th step the user enters the generated Signup TOTP code by pressing the code on his keypad using DTMF Dual tone multi frequency. The server now receives and verifies the generated Signup TOTP code.

There can be other ways the Signup TOTP can be sent to the server in 6th step. Also, the user can input his username / email directly in the mobile itself instead of the website on desktop.

These 6 steps complete the sign process so that the same TOTP will be present in both the server and the mobile at any given moment of time.

0 Spoofing, in action

Fig 1



Explanation of Fig Number 1:

Block diagram is that of two mobiles apps working with 0 spoof system.

Note: Every 30 seconds a new random number is generated by the Time-Based One-Time Password or TOTP code generator, known as Calling TOTP code. The seed records of Calling TOTP are same in mobile 123 and the server. So, the same TOTP is generated at any given moment in mobile 123 and server.

Step 1: In this step when the mobile number 123 calls mobile 456 then it also simultaneously sends a call request to server.

Step 2: The server gives back a missed call to the mobile number 123. This ensures that the mobile has the sim card 123 inside it.

Aniket Deshpande aniketd1@gmail.com 8767061161

Step 3: The mobile 123 generates an identifier code. This identifier code is generated by applying a mathematical formula on the numbers 123, 456 and the Calling TOTP code.

Step 4: This identifier code & number 456 is then sent to the server. Also, the Signup TOTP generated by sign up seed record, as seen in sign up process, is sent to this server.

In the server same numbers are used with same math formula 123, 456 & it has the same Calling TOTP code generator seed record, generating the same Calling TOTP code, as in the first mobile 123. Hence ideally the server should generate the same identifier code in it.

After the server receives the identifier code from mobile 123 it then compares the identifier code generated inside it and the identifier code received from the mobile 123.

Step 5: If both are same then it sends a no spoofing alert, else a spoofing possibility is sent.

Step 6: The mobile number 123 calls the mobile number 456 after a delay of say 3 to 5 seconds since the step 1 of call request to server was conducted. The delay is there so that steps 1 to 5 get completed.

The dialer tone will be heard by the user of mobile number 123, though actual call will be placed after say 3 to 5 seconds, during completion of operation.

Anti-Spam

Anti-Spam score calculation:

Primarily there is an anti-Spam score this anti-spam score is the filter using which the incoming calls are to be filtered.

Anti-spam score consists of two scores. The whitelisting score and the spam score.

The higher the whitelisting score the better and the lower the spam score the better.

Whitelisting score is the score that gets increment by one, if that phone number is saved by another person in his phone book. For example, if a person A is saved by B, C and D in their respective phone books. Then A gets whitelisted by them. Hence A's whitelisting score becomes 3.

Now, if the phone number of A is saved in 100 phones then his whitelisting score will go to 100.

This is all about whitelisting score. Now let's see the second part that is the spam score.

If person A is found making spam calls then his spam score will increase. As a result of which spam report by each number will increase its score. Therefore if 2 numbers X and Y report that the number A has been calling them and doing spam calls then the spam score of A will be 2.

Therefore, the Anti-spam score of A will be 100/2. In this 100 have white listed him and 2 have marked him as spam.

Imp: Each user can keep his own cut off score. Default will be 20/5.

For example, a person Ram has kept his cut off score as 90/5. So, he can receive the calls of A since his whitelisting is above 90 which is 100 and spam score is below 5 which is 2.

If Shyam has kept his cut off score as 110/6 then he won't get calls since the whitelisting score of A is 100 which is below 110.

If Krishna has kept score of 90/1 then also the calls won't go through because Krishna allows only those people who have not made more than 1 spam calls. Whereas A has made 2 spam calls.

A. If a person buys numbers in bulk:

There can be a scenario in which a person, say, Mahesh buys phone numbers in bulk.

For example, he has bought 1000 numbers in bulk.

So first he uses his own number once it gets spammed reported by say 5 people. Supposing by default 5 will be the cut-off for spam score.

Therefore, Mahesh has a number and it gets declared as spam number.

Now he has bought 1000 numbers or pooled 1000 numbers.

Pooling means all spammers come together and whitelist each other.

Therefore, all these numbers will save and hence white list each other.

For all new numbers to be entered into the system they will have to be whitelisted means saved.

Therefore, Mahesh takes 10 numbers for spamming and rest of 990 are whitelisting these 10 numbers.

Here we use the defence as below:

1. **Check how many numbers have whitelisted a number X for example and pass its score further accordingly. Higher the numbers whitelisting a number X higher the score this whitelisted number can pass further.**
2. **Also, how much time has passed since these numbers are whitelisted, the higher the amount of time passed, the greater the whitelisting value being passed further.**

B. What if a number is whitelisting numbers again and again which turn out to be spam?

Suppose a person has bought numbers in bulk or by paying other people such that these are only for the purpose of whitelisting.

If a set of 10 numbers are found to be reporting numbers, say, as white list and which are found to be spam again and again then the antispam score of whitelisted numbers won't improve.

For example: If these 10 numbers first whitelisted a number Raju and Raju did spam and reached the cut-off score. After that Ramesh also got whitelisted and reached cut-off score.

So, the app will understand that the 10 numbers are doing false whitelisting with the intention of whitelisting spam numbers then their whitelisting score value being passed will be depleted or be revoked completely.

Here we will use the below defence:

A. **Reduce / Remove the whitelist score being sent to other numbers, of a number which has been found to be whitelisting spam numbers again and again.**

C. Rajesh can get whitelisted by paying people to whitelist / save his number:

If a person Hrishi has taken money from Rajesh and has whitelisted for Rajesh's number so that Rajesh can do spam calls.
Then after Rajesh starts doing spam calls, say, he has got five spam call reported for his number. So, he can go back to Hrishi with his new number and ask him to white list again. Then Hrishi, will deny since his number can get revoked from the app system, as mentioned earlier.

However, next time Rajesh will buy a new number and will give money to Kedar instead of Hrishi. Starting the same circle again but he can make a few calls in this case. Hence, we will need to remove the people from app who vouch for spammers.

So here we will use "spam police" these are our people only, who give out the false outlook that they are spammers and want to give money to say students or villagers so that they can whitelist the supposed spammers.

If these students or villagers fall for the false money to be offered, then here these spam police will warn the students or villagers to not share the whitelisting to unknown people in return of money. First the spam police will warn in beginning then later remove their numbers from the app system.

Here we use the defence as below: Use Spam Police: Remove from the app for an hour, two hours, a day, a week or forever.

D. If a student or any one buys a new number:

New numbers will start from scratch with 0 anti-spam score. For example, for college students.

They will gather their whitelists from relatives and friends already in the system by talking to them in real person or by messaging.

This won't be done in beginning and we will wait till the app is well known.

E. Optional Features:

If we find that a number AAA is whitelisting other numbers BBB and CCC which is doing spam then we can reduce or remove the whitelisting score being passed by number AAA to other numbers.

For example in phone book of AAA there are a several numbers like BBB, CCC, DDD & so on.
So once the app system comes to know that AAA is whitelisting BBB and CCC and these are doing spam calls then we can reduce or remove the whitelisting score being passed by AAA to all numers in its phone book. Therefore, none of the numbers BBB, CCC, DDD and SO on will receive any whitelisting scores value from AAA.

F. Exceptional Numbers:

Police, ambulance other emergency and government numbers: These exception numbers can't be put in spam list.

G. Buying New Numbers:

Buying new number which may be already marked as spam: Check by calling the new number to be bought if it's showing spam in app then don't buy it.

H. Bank and other Institution Numbers:

ICICI like calls spam for one not for another: Will use two numbers one to sell and one to call already existing clients.

With best regards,
Aniket Deshpande
8767061161 / 9850432492