# Two-Factor Authentication Vulnerabilities

Stefan Ćertić

https://www.certic.info

University of Belgrade

## Author Note

Stefan Ćertić, Internet Topology Security Issues, University of Belgrade.

This research was supported IN PART by a grant from Science Consortium.

Correspondence concerning this article should be addressed to Stefan Ćertić, Internet Topology Security Issues, University of Belgrade.

Contact: stefan@certic.info web: https://www.certic.info

## Abstract

Corporative giants of the internet, such as Google, Facebook, Various Banks have being using the two-factor authentication technique to ensure security to its users. Although, this companies don't make this kind operations by themselves, they hire third part companies to do so, integrating the API products for onwards delivery. Because of this, technique have serious breaches that can be explored by a ill-intentioned company.  The third part companies stays between the client and the website being in a privileged place to attack any unsuspecting victim.

*Keywords:* internet, 2FA, data security, attacks, breaches.

Two-Factor Authentication Vulnerabilities

## Introduction

How would you recover your password if you simply forget it today? The answer for this question has being the two-factor authentication (2FA) for a while now. The vast majority of the biggest websites companies are using it, it has turned into a pattern.

It is perfect as it allows the user to recover its credentials in a practical way, simply receiving a message in the cellphone on a call from the company you desire to retrieve you credentials from. However, this study shows that, in most cases, this is not as secure as it might be. In fact, it carries a dangerous threat within. According to (Toorani & Beheshti, 2008) “Data confidentiality, integrity, authentication, and non-repudiation are the most important security services in the security criteria that should be taken into account in many secure applications. However, such requirements are not provided by the traditional SMS messaging”.

Private user and various companies trust the leading players in the internet – Google, Facebook, LinkedIn, Twitter, etc. – by giving them permission to hold and process their sensitive data. Still, more and more people provide their data to these large enterprises, but a limited number of them take into account the existence of some background companies, the ones who sell the two-factor authentication solutions.

These background companies position themselves in a privileged spot, they are able to either give what they were hired to do or to pick up accounts and sell the access to these accounts to someone else.

Considering the following assumptions:

- Company A specializes in PIN code deliveries through Phone Calls or SMS;
- Company A grows big through merges and acquisitions;
- Company A starts providing services to Facebook, Google, LinkedIn, Twitter and Banks;

Consequently, every time one decides to change its password or login through phone, by call or by SMS, Company A would have to be called to send the code via API.

## Normal Flow versus Attack Pattern

Internet security and information technology are too centralized and the current implementation of double securing accounts have to be discussed. According to (Rosenblatt & Cipriani, 2015) “Account recovery works as a tool for breaking two-factor authentication because it "bypasses" 2FA entirely”. So, instead of securing the users’ account, the current model of 2FA makes it even more vulnerable.

This idea is described in the following descriptions of the normal 2FA flow and of the Attack Pattern. The steps of the normal flow, as seen in Figure 1, can be described as:

- Person X asks for a password reset via 2FA, to a bank;
- The bank requests the 2FA provider,  Company A, to generate a PIN code via API;
- Person X receives the code;
- Person X enters the code;
- The bank validates the code.

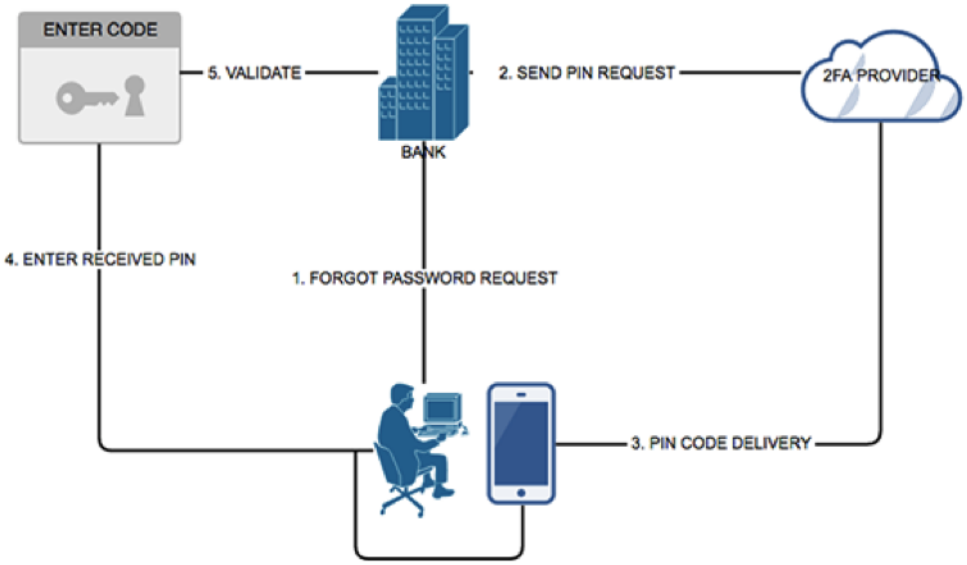


*Figure 1.* Regular request flow.

As seemed, every time Person X decides to change its password or login through phone, by call or by SMS, Company A have to be called to send the code. Therefore, a Person Y, working for Company A, will see all personal data regarding Person X.

Therefore, the Attack Pattern, as seen in Figure 2, is as follows:

- Person Y, at Company A, starts, in Person X’s name, a password reset;
- Person Y intercepts the password reset message;
- Person Y login into Person X account without Person X noticing.

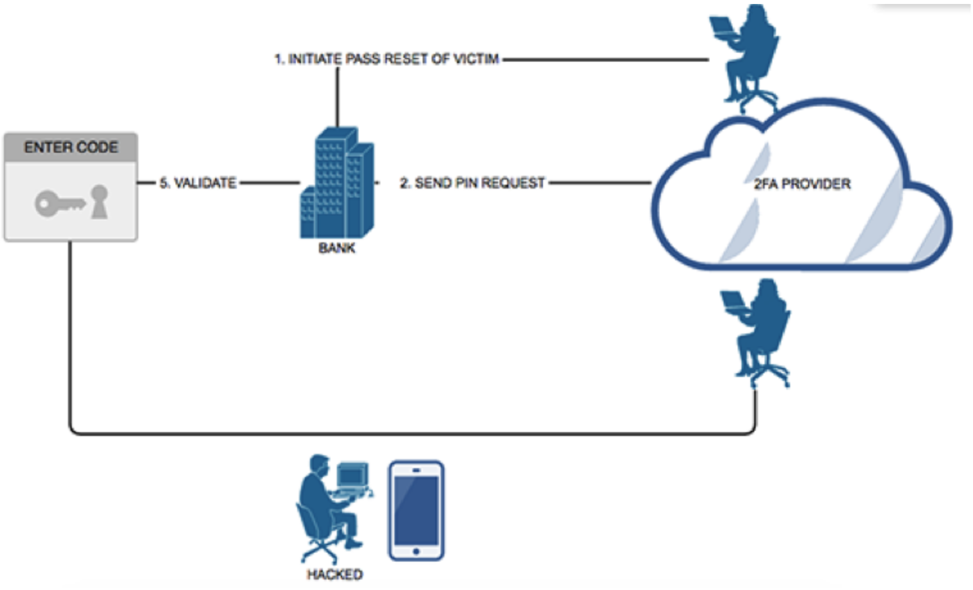
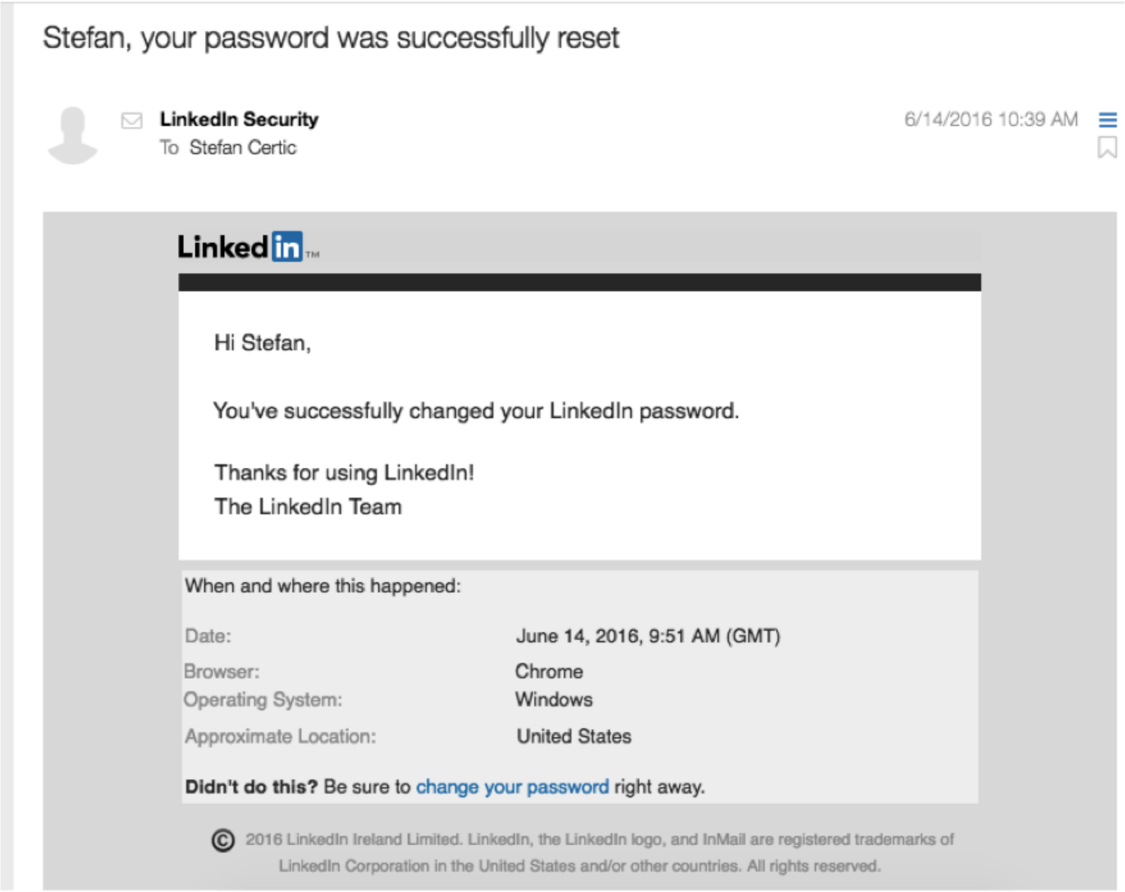


*Figure 2*. Attack Pattern.

This Attack Pattern is in use, many people have reported that they had their LinkedIn and Facebook accounts hacked.

## Actual Attacks

Realizing a forensic investigation of the systems, it has being revealed that the following scenario is being used to successfully hack accounts.



Stefan, your password was successfully reset

LinkedIn Security
To Stefan Certic

6/14/2016 10:39 AM

Hi Stefan,

You've successfully changed your LinkedIn password.

Thanks for using LinkedIn!
The LinkedIn Team

When and where this happened:

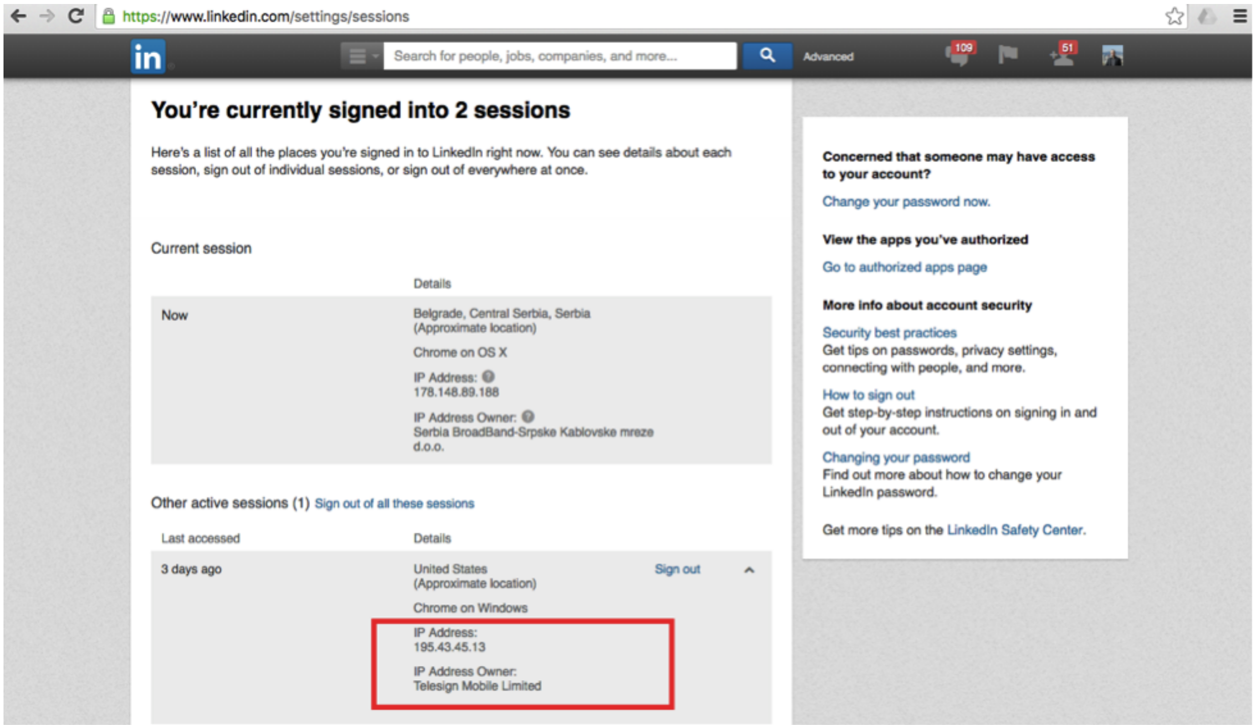
| | |
|---|---|
| Date: | June 14, 2016, 9:51 AM (GMT) |
| Browser: | Chrome |
| Operating System: | Windows |
| Approximate Location: | United States |

**Didn't do this?** Be sure to change your password right away.

© 2016 LinkedIn Ireland Limited. LinkedIn, the LinkedIn logo, and InMail are registered trademarks of LinkedIn Corporation in the United States and/or other countries. All rights reserved.

Figure 3. Successfully changing password screen.

From the above image, it is clear that the email shows that a password reset had been done using Chrome on a windows device located in the United States. The login sessions can also be used to detect cases of successful account hacking as can be seen in the screenshot below.


https://www.linkedin.com/settings/sessions
in
Search for people, jobs, companies, and more...
Advanced
109
51

**You're currently signed into 2 sessions**

Here's a list of all the places you're signed in to LinkedIn right now. You can see details about each session, sign out of individual sessions, or sign out of everywhere at once.

Current session

Details

Now

Belgrade, Central Serbia, Serbia
(Approximate location)

Chrome on OS X

IP Address:
178.148.89.188

IP Address Owner:
Serbia BroadBand-Srpske Kablovske mreze d.o.o.

Other active sessions (1) Sign out of all these sessions

Last accessed

Details

3 days ago

United States
(Approximate location)

Sign out

Chrome on Windows

IP Address:
195.43.45.13

IP Address Owner:
Telesign Mobile Limited

**Concerned that someone may have access to your account?**

Change your password now.

**View the apps you've authorized**

Go to authorized apps page

**More info about account security**

Security best practices
Get tips on passwords, privacy settings, connecting with people, and more.

How to sign out
Get step-by-step instructions on signing in and out of your account.

Changing your password
Find out more about how to change your LinkedIn password.

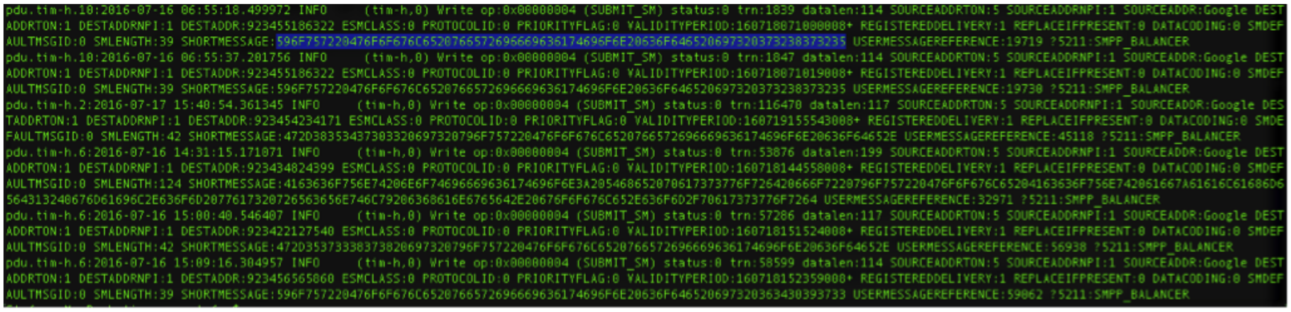
Get more tips on the LinkedIn Safety Center.

*Figure 4.* IP Address Owner.

Figure 4 shows two active logins using Chrome, from Windows, and the location is in the United States, and more important from the RIPE allocated IP block that has been assigned to one of the biggest 2FA providers on the world that process Google, Facebook, Instagram, Twitter and many other Services.

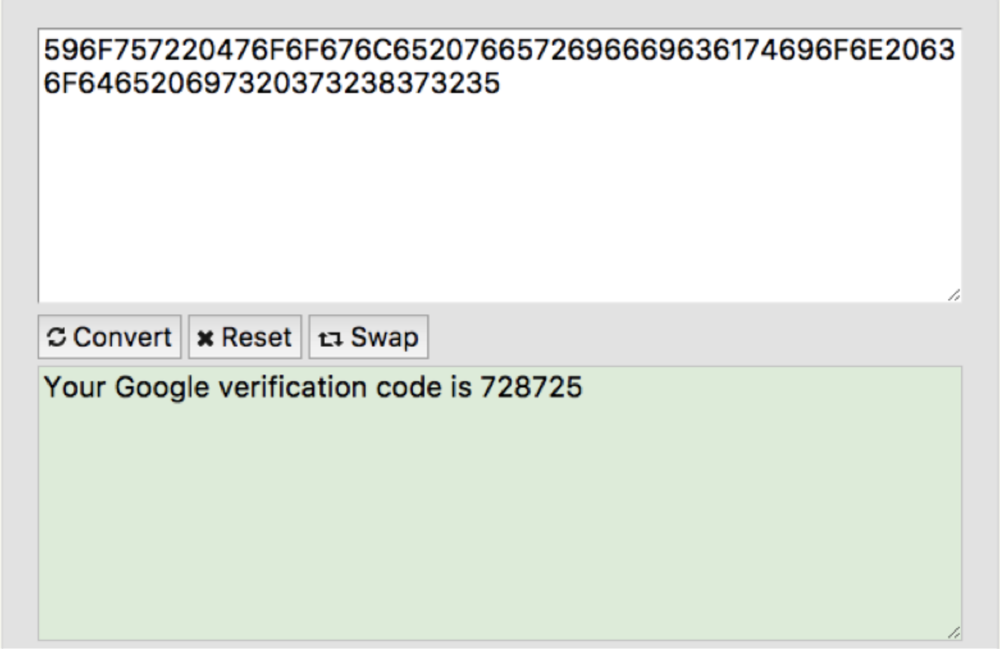
SMS/Voice MSU market works just like a stock market, each call has a price and, considering this price, after the code is submitted from the social network for upward delivery, the delivery company chooses the “least cost route” / less expensive 2FA provider.

The problem resides in the fact that there is no encryption in this submission from the social media service so, the entire 2FA transmission is made openly. Figure 5 shows a captured traffic from one of these submissions.  Figure 6 shows the translation from the code captured to the code received by the user.



```
pdu.tim-h.10:2016-07-16 06:55:18.499972 INFO     (tim-h,0) Write op:0x00000004 (SUBMIT_SM) status:0 trn:1839 datalen:114 SOURCEADDRTON:5 SOURCEADDRNPI:1 SOURCEADDR:Google DEST
ADDRTON:1 DESTADDRNPI:1 DESTADDR:923455186322 ESMCLASS:0 PROTOCOLID:0 PRIORITYFLAG:0 VALIDITYPERIOD:160718071000008+ REGISTEREDDELIVERY:1 REPLACEIFPRESENT:0 DATACODING:0 SMDEF
AULTMSGID:0 SMLENGTH:39 SHORTMESSAGE:596F757220476F6F676C6520766572696669636174696F6E20636F646520697320373238373235 USERMESSAGEREFERENCE:19719 ?5211:SMPP_BALANCER
pdu.tim-h.10:2016-07-16 06:55:37.201756 INFO     (tim-h,0) Write op:0x00000004 (SUBMIT_SM) status:0 trn:1847 datalen:114 SOURCEADDRTON:5 SOURCEADDRNPI:1 SOURCEADDR:Google DEST
ADDRTON:1 DESTADDRNPI:1 DESTADDR:923455186322 ESMCLASS:0 PROTOCOLID:0 PRIORITYFLAG:0 VALIDITYPERIOD:160718071019008+ REGISTEREDDELIVERY:1 REPLACEIFPRESENT:0 DATACODING:0 SMDEF
AULTMSGID:0 SMLENGTH:39 SHORTMESSAGE:596F757220476F6F676C6520766572696669636174696F6E20636F646520697320373238373235 USERMESSAGEREFERENCE:19730 ?5211:SMPP_BALANCER
pdu.tim-h.2:2016-07-17 15:40:54.361345 INFO     (tim-h,0) Write op:0x00000004 (SUBMIT_SM) status:0 trn:116470 datalen:117 SOURCEADDRTON:5 SOURCEADDRNPI:1 SOURCEADDR:Google DES
TADDRTON:1 DESTADDRNPI:1 DESTADDR:923454234171 ESMCLASS:0 PROTOCOLID:0 PRIORITYFLAG:0 VALIDITYPERIOD:160719155543008+ REGISTEREDDELIVERY:1 REPLACEIFPRESENT:0 DATACODING:0 SMDE
FAULTMSGID:0 SMLENGTH:42 SHORTMESSAGE:472D38353437303320697320796F757220476F6F676C6520766572696669636174696F6E20636F64652E USERMESSAGEREFERENCE:45118 ?5211:SMPP_BALANCER
pdu.tim-h.6:2016-07-16 14:31:15.171071 INFO     (tim-h,0) Write op:0x00000004 (SUBMIT_SM) status:0 trn:53876 datalen:199 SOURCEADDRTON:5 SOURCEADDRNPI:1 SOURCEADDR:Google DEST
ADDRTON:1 DESTADDRNPI:1 DESTADDR:923434824399 ESMCLASS:0 PROTOCOLID:0 PRIORITYFLAG:0 VALIDITYPERIOD:160718144558008+ REGISTEREDDELIVERY:1 REPLACEIFPRESENT:0 DATACODING:0 SMDEF
AULTMSGID:0 SMLENGTH:124 SHORTMESSAGE:4163636F756E74206E6F74696669636174696F6E3A205468652070617373776F726420666F7220796F757220476F6F676C65204163636F756E742061667A61616C61686D6
564313240676D61696C2E636F6D2077617320726563656E746C79206368616E6765642E20676F6F676C652E636F6D2F70617373776F7264 USERMESSAGEREFERENCE:32971 ?5211:SMPP_BALANCER
pdu.tim-h.6:2016-07-16 15:00:40.546407 INFO     (tim-h,0) Write op:0x00000004 (SUBMIT_SM) status:0 trn:57286 datalen:117 SOURCEADDRTON:5 SOURCEADDRNPI:1 SOURCEADDR:Google DEST
ADDRTON:1 DESTADDRNPI:1 DESTADDR:923422127540 ESMCLASS:0 PROTOCOLID:0 PRIORITYFLAG:0 VALIDITYPERIOD:160718151524008+ REGISTEREDDELIVERY:1 REPLACEIFPRESENT:0 DATACODING:0 SMDEF
AULTMSGID:0 SMLENGTH:42 SHORTMESSAGE:472D35373338373820697320796F757220476F6F676C6520766572696669636174696F6E20636F64652E USERMESSAGEREFERENCE:56938 ?5211:SMPP_BALANCER
pdu.tim-h.6:2016-07-16 15:09:16.304957 INFO     (tim-h,0) Write op:0x00000004 (SUBMIT_SM) status:0 trn:58599 datalen:114 SOURCEADDRTON:5 SOURCEADDRNPI:1 SOURCEADDR:Google DEST
ADDRTON:1 DESTADDRNPI:1 DESTADDR:923456565060 ESMCLASS:0 PROTOCOLID:0 PRIORITYFLAG:0 VALIDITYPERIOD:160718152359008+ REGISTEREDDELIVERY:1 REPLACEIFPRESENT:0 DATACODING:0 SMDEF
AULTMSGID:0 SMLENGTH:39 SHORTMESSAGE:596F757220476F6F676C6520766572696669636174696F6E20636F646520697320363430393733 USERMESSAGEREFERENCE:59062 ?5211:SMPP_BALANCER
```

*Figure 5.* 2FA transmission.



```
596F757220476F6F676C6520766572696669636174696F6E2063
6F646520697320373238373235
```

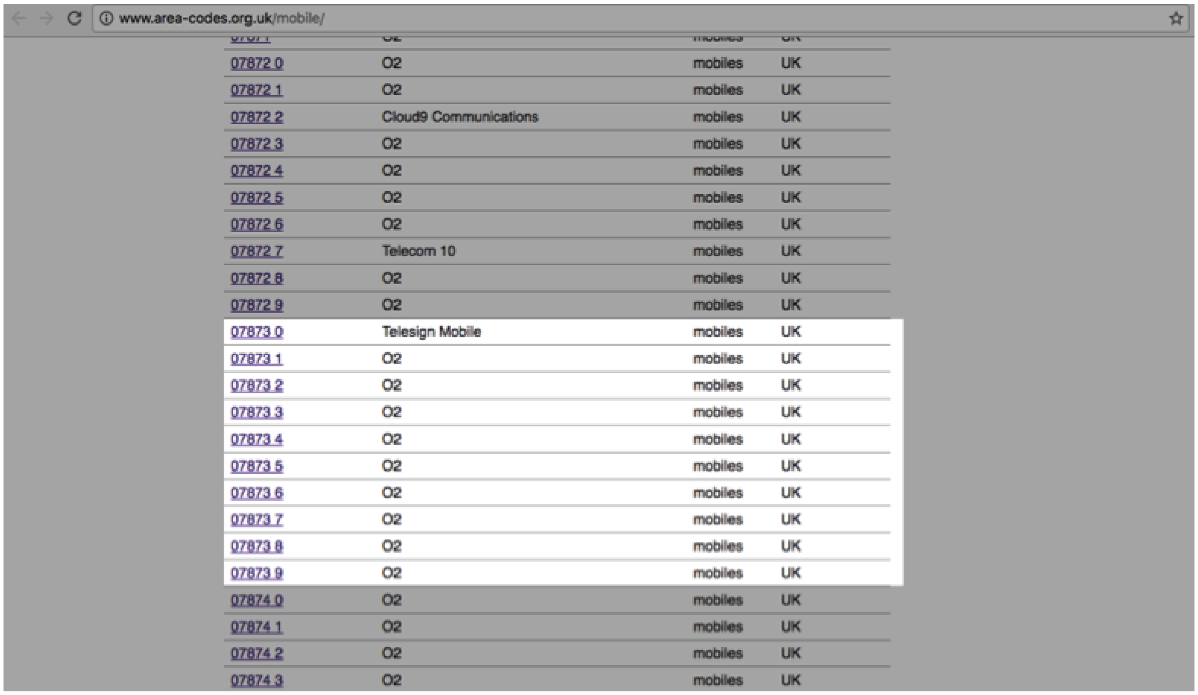
Your Google verification code is 728725

*Figure 6.* Google verification code.

## Methods to achieve targeted attack

As mentioned before, the call through the "least cost route" to the 2FA provider, using the price of the SMS/Voice calls. Thus, a targeted attack can be achieved by dropping these SMS/Voice calls prices on the global market by single 2FA provider. The attacker (the ill-intentioned 2FA provider) chooses a victim, then, drops the price for the victim's specific country and operator. Therefore, because of the least cost routing, it is a matter of minutes until the traffic is re-routed towards the attacker platform.

However, the attackers do not want to be discovered, so, they employ cunnings tricks to stay undercover. Figure 7 shows a table of prefixes' numbers for companies in UK.



| | | | |
|---|---|---|---|
| 07872 0 | O2 | mobiles | UK |
| 07872 1 | O2 | mobiles | UK |
| 07872 2 | Cloud9 Communications | mobiles | UK |
| 07872 3 | O2 | mobiles | UK |
| 07872 4 | O2 | mobiles | UK |
| 07872 5 | O2 | mobiles | UK |
| 07872 6 | O2 | mobiles | UK |
| 07872 7 | Telecom 10 | mobiles | UK |
| 07872 8 | O2 | mobiles | UK |
| 07872 9 | O2 | mobiles | UK |
| 07873 0 | Telesign Mobile | mobiles | UK |
| 07873 1 | O2 | mobiles | UK |
| 07873 2 | O2 | mobiles | UK |
| 07873 3 | O2 | mobiles | UK |
| 07873 4 | O2 | mobiles | UK |
| 07873 5 | O2 | mobiles | UK |
| 07873 6 | O2 | mobiles | UK |
| 07873 7 | O2 | mobiles | UK |
| 07873 8 | O2 | mobiles | UK |
| 07873 9 | O2 | mobiles | UK |
| 07874 0 | O2 | mobiles | UK |
| 07874 1 | O2 | mobiles | UK |
| 07874 2 | O2 | mobiles | UK |
| 07874 3 | O2 | mobiles | UK |

*Figure 7.* UK numbering plan of prefixes issued by Ofcom.

As seen in the table, the prefixes from 078731 to 078739 are allocated to O2. But, Company X allocated the prefix 07830 from Ofcom, and this is used to send "Social Networks verifications". Operators worldwide will try to short-down the lists of Global Titles, which has similar rules to iptables, and most of them have only prefix 07873 that is assigned to O2.

With the low price strategy the traffic is accepted even there is no Roaming Agreement with X (based on O2), the operator then, thinks the invoice goes to O2, when it is going to X.

Even if O2 don't have any Roaming Agreement made, it is always good for small operators to receive messages originated in giant companies.

Using a number from the example pool, in a voip white channel, returns always the operator as O2, even for China Telecom. This allocation for “prefix in a sandwich” only occurs in this case, for UK or anywhere in the world.

## Failover approach

Due to the fact of more than 2000 operators worldwide, it’s considerable that a single entity such as Bank, Social Media Platform or any company is in unprivileged position to setup a roaming agreement with all of them, assuming the entity is operating world-wide. It’s also safe to assume, that single 2FA supplier could experience technical difficulties from time to time. In order to assure best quality at least cost, these companies do sign with multiple 2FA suppliers. According to tests committed, by monitoring message delivery SMSC (Short Messaging Service Center), it’s enough to simulate “I have not received a message” using different IP’s and accounts for a single operator via Google platform, in order for Google to change the delivery path (a company that delivers the Code). This has been determined by an SMSC changes after multiple “complaints” that the verification message is not received. Therefore, it’s just a matter of enough simulated complaints, even if there’s no technical difficulties to trick the google into changing the routing towards the attacker.

## Conclusion

This study presents forensic evidences that there is a serious breach in the 2FA authentication model. Even more, this study shows that there is a sophisticated scheme capable of controlling the whole market and getting access to any account at any time.

If this is really happening institutionally, not as a part of action of privileged employee then it is affecting the whole Internet community, with potential for strongly positioned company to exploit the vulnerability of the topology itself, present losses on the regular side of business while making enormous amount of profits by selling the targeted accounts on the blackmarket, committing sophisticated account attacks, generating enormous sum of profit, while presenting as not profitable, therefore charged less taxes, if any, leaving very little evidences to even become suspicious.

## References

Toorani, M. & Beheshti, A. (2008, September 16). SSMS - A secure SMS messaging protocol for the m-payment systems. Paper presented at the 2008 IEEE Symposium on Computers and Communications, Marrakech, Morocco.

Rosenblatt, S. & Cipriani, J. (2015, June 15). Two-factor authentication: What you need to know (FAQ).  Retrieved from https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/