Approach on Fraud Detection in Voice over IP Networks using Call Destination Profiling Based on an Analysis of Recent Attacks on Fritz!Box Units

Anton Wiens, Torsten Wiens and Michael Massoth
Department of Computer Science
Hochschule Darmstadt – University of Applied Science
Darmstadt, Germany
{anton.wiens | torsten.wiens | michael.massoth}@h-da.de

***Abstract*—Recently, massive attacks on Fritz!Box hardware units have been disclosed, caused by a security vulnerability. The Fritz!Box by AVM is an multifunctional routing device, offering Voice over IP-(VoIP) and internet connectivity to private users, which is in wide use in Germany. By first taking over the units and in a second step using the units to conduct toll fraud attacks on VoIP providers and their customers, significant financial damage has been caused. In this work, these attacks are analyzed and attack patterns as well as their characteristic traits are described. Based on these results, a novel method for toll fraud detection is devised and evaluated. The method is capable of detecting this kind of attack, as well as similar attack patterns. Results of a prototype implementation show successful detection of these attacks, enabling to prevent them in the future. This work is based on real-life traffic data from a cooperating telecommunication service provider.**

Keywords—Fraud Detection; Voice Over IP Networks; Fritz!Box; User Profiling; Statistical detection methods.

I. INTRODUCTION

Today's voice communication by Voice over IP (VoIP) mostly uses the internet for data transport. There are the drawbacks that the internet can basically be accessed by anyone, and that it links anyone to anyone. For example, it is possible for third parties with criminal intent to access private branch exchange (PBX) systems connected to the internet.

Fraudsters may have multiple options to abuse these systems. Systems that are insufficiently secured may be tapped. Access data that has been saved in these systems could be used to abuse, compromise or even take over the whole PBX. If the PBX system has been taken over, a fraudster will be able to conduct telephone calls to premium rate service numbers or comparable call destinations, generating profit. The resulting cost, on the other hand, will often be charged to the victim or its telecommunication service provider, because of a general rule in telecommunication service providing, called "Calling Party Pays".

The Communications Fraud Control Association (CFCA) reports losses of about 46 billion USD caused by telecommunication fraud in 2013, an increase by 15% compared to 2011 [1]. Not only financial damage is a problem caused by fraud attacks. Small providers may also suffer from reputation losses, causing customers to change the provider because of decreased trust and fear of repeated fraud attempts in the future.

To detect and counter these attacks, respectively fraud attempts, fraud detection systems are used. Often, these systems apply methods based on the generation of statistical profiles for each user. User profiles are generated that describe their behavior. These profiles will then be used as input for machine learning techniques, allowing for the detection of fraud [2] [3][4] [5].

The German company "Deutsche Telekom" reported a huge success in the prevention of fraud cases with potential damages of about 200 million Euro, using an automated fraud detection system [6]. The research project "Trusted Telephony" at the University of Applied Sciences Darmstadt, from which the work at hand originates, pursues the goal to increase security in VoIP telephony, cooperating with the German telecom service provider toplink GmbH. A key objective of the project is the development of a fraud detection system.

Recently, fraud cases were caused by security exploits in Fritz!Box hardware (from the company AVM GmbH), which is often used in Germany [7][8]. The Fritz!Box is an integrated, multifunctional routing device, offering internet connectivity, VoIP capabilities and other services in local area networks. This unit is very popular in Germany. Because of the large amount of units in use, there is an increased risk in case of security vulnerabilities, especially for private users.

On the other hand, an exploitation of the recently disclosed security vulnerability of this unit is only one possibility to start such attacks. The security vulnerability has been patched by the manufacturer in the mean time, but in the future, comparable vulnerabilities in similar hardware could turn up. Therefore, it is important to be able to detect these situations and devise measures to counter them.

In the work at hand, an analysis of the recent attacks on Fritz!Box units is presented. Characteristic traits of these attacks are described, classified and analyzed. Additionally, it is discussed if the usual methods for the detection of fraud cases are also applicable in these cases. Resulting from this analysis, a new fraud detection method is devised. The basic idea is not to apply a variant of user profiling techniques, as usual, but to use statistical profiles of call destination numbers. This way, it is possible to detect certain attacks that would go undetected if user profiling techniques were applied. The general problem with this kind of attack pattern is a distribution of single attacks over multiple users, whose

 ISBN: 978-1-61208-357-5

router units have been compromised by a primary attack. Therefore, this pattern cannot be detected as a fraud attack from the perspective of a single user.

The new method uses two profiles, as described in our preliminary work for a different case [9]. These profiles are used to describe the behavior of destination call numbers in defined time spans in the past and present. Changes in behavior are statistically evaluated. Fraud attempts are detected by the investigation of major changes in this data.

A. Call detail records

The data being analyzed in this work comprises fraud attacks that have been enabled by the recently discussed security vulnerability of the Fritz!Box units. The data, consisting of Call Detail Records (CDR) has been supplied by toplink GmbH.

A CDR is a text file, containing all parameters of single telephone calls. Each CDR is written by the primary VoIP routing system TELES.iSwitch at toplink as calls are set up [10]. CDRs contains information on caller, callee, call duration, starting time as well as technical network parameters.

B. Structure of the Paper

After the introduction, an overview of related work is given in Section II, its relevance is described as well. In Section III, the concept of behavior profiling is introduced, on which the method presented in this paper is based. In Section IV, Call Detail Records are introduced. Section V contains an analysis of attacks on telecommunication systems that are enabled by the known security vulnerability of Fritz!Box hardware. In Section VI, a method to identify and counter such attacks is presented. First evaluation results of this method, based on real-life CDR traffic data, are presented in Section VII. Section VIII contains a conclusion to this paper, and Section IX presents possible future work.

II. Related work

This work is partially based on findings from preliminary work of the authors [9], as well as additional ideas that arose during the recent announcement of the attacks on Fritz!Box hardware [8].

In [9], a method for toll fraud detection using statistical user profiling has been described, which can especially be applied when no significant amount of training data is available. Additionally, the method can be run in a mostly autonomous way, requiring only a minimum amount of external administration. The method applies two user profiles, one for a past period of time and one for a present period of time, each containing statistical features. The profiles are used to identify suspicious deviations of the users' behavior, by which toll fraud attempts are detected. In this work, the attacks on Fritz!Box hardware and the possibility to detect these using the presented method had already been mentioned.

In the work at hand, the method from the preliminary work is adapted more closely to this attack pattern. The new method again uses two profiles of statistical features for each user, but differing in contents and their actual use for the detection of attacks.

Furthermore, other related work also describes different methods of user profiling for the detection and prevention of toll fraud in VoIP telecommunication [2] [3] [5] [11] [12] [13]. In contrast to this work, the work at hand does not apply simple user profiles, but a new kind of profile specified as Call Destination Profile. These profiles are used to characterize the behavior of a destination telephone number instead of a user's behavior. It is intended to detect special kinds of attacks this way.

These attacks cannot be detected with user profiling techniques alone and hence would go undetected if the method from [9] was applied. Section V contains a more in-depth description of the idea.

III. Behavior Profiling

The term „behavior profiling" describes a technique for differential analysis where the behavior of a given object is represented by a statistical profile. In the profile, data from the object is accumulated, which is then used to generate statistics that describe the object's behavior, which are called features. Often, behavior profiles are applied in the form of user profiles [2] [3] [5] [11] [12] [13]. In most cases, a differential analysis is preferred over an absolute analysis. This is because the absolute analysis is a subset of the differential analysis [9].

For example, three variants of user profiling methods are presented in [4]. In this work, the parameters *duration per call*, *number of calls per customer* and *costs per call* are arranged in different ways into the group's *national calls*, *international calls* and *mobile calls.* These are used to generate statistics for the profiles.

User profiles are utilized to describe the behavior of users in the present and in the past, enabling a comparison of behavioral patterns. By this comparison, it is possible to detect suspicious fluctuations. These are analyzed in the next step in order to generate a decision on fraudulent or non-fraudulent behavior.

In the work at hand, behavior profiling is applied for a novel profiling approach, differing from classical user profiling in the way that no profiles of the user's behavior are generated, but profiles of destination call numbers instead.

IV. Analysis of attacks on Fritz!Boxes

The recent attacks at (and by) Fritz!Boxes can be divided in two categories. The first category comprises the hostile takeover of a Fritz!Box by exploiting a security vulnerability in its firmware. The second category comprises possible results of such a takeover, especially secondary attacks that are enabled by then remotely controllable units. Both categories are described in more detail in the following subsections. It is important to note that the initially possible attacks on these units cannot be conducted anymore, since the firmware has been updated by the manufacturer in the mean time [8]. The focus of the work at hand is at the possibility of fraud attacks on telecommunication systems by

 ISBN: 978-1-61208-357-5

utilizing taken over secondary hardware, which is not unlikely to happen again in the future, and detecting it.

A. Primary hostile take-over of a Fritz!Box

The basic idea to perform a hostile take-over of a Fritz!Box was as follows: An attacker would set up a web site, which is to be visited by potential victims. The attacker would then be able to exploit the known security vulnerability of the Fritz!Box in order to extract the master password. Using this password, the attacker would be able to access the command shell. Once this is done, the attacker could then deploy system commands, e.g., to make the unit call premium-rate service numbers at the cost of the unit's owner [8].

B. Secondary attacks after the take-over

Attack attempts on other systems that had been conducted using taken-over Fritz!Boxes seem to be very similar in their basic approach. For an in-depth analysis, anonymized data on such attack attempts has been provided by toplink GmbH. The data being used is in accordance to the Federal German Data Protection Act (Bundesdatenschutzgesetz) [14]. All results from this analysis are based on this data and may not represent attack patterns that appeared at other telecommunication providers.

1) From a single user's view

From the perspective of a single user, an attack attempt may look as follows: An attacker tries to set up a call to a premium-rate service number or a comparably expensive call destination, possibly also in another country. This is done multiple times during a short time span. As soon as the attacker has successfully set up a call to a given number, he will try to call this number again, as often as possible, and also in a short period of time. If the call attempts fail (e.g., because the number is not available), the attacker will try another number,

The difficulty to detect such attack attempts lies in the low frequency and the low duration of these calls seen from a single user's point of view. Attackers will avoid a detection using these two parameters by applying an approach described in the next section.

2) Exploiting multiple users

By exploiting the security vulnerability at multiple victims' Fritz!Box units, attackers are able to hide their attack attempts neatly. The attack attempts are distributed across multiple taken-over units. So, it becomes possible to mask obvious evidence of attack attempts, such as frequency and duration of calls. This will be illustrated by the following examples:

1. Attacker A conducts a hostile take-over of victim C and causes C's unit to start 30 calls to destination number B. The duration of each call is 20 seconds.
2. Attacker A conducts a hostile take-over of victim C and causes C's unit to start 5 calls to destination number B. The duration of each call is 5 minutes.
3. Attacker A conducts hostile take-overs of 30 victims and causes each victim's unit to conduct one call to destination number B. The duration of each call is 20 seconds.

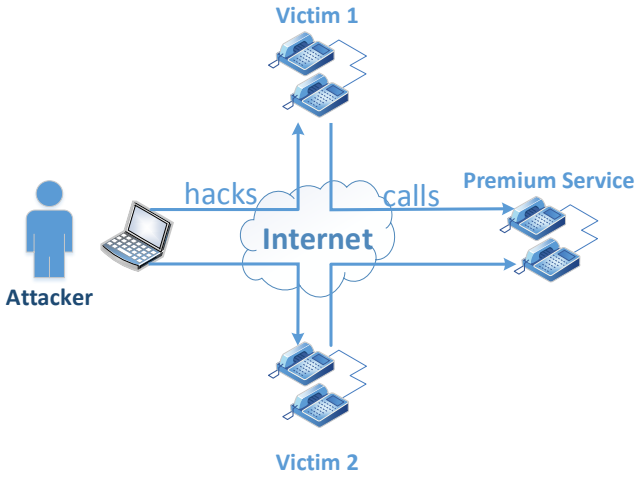

Figure 1. Depiction of example three with just two victims of an attacker calling a premium service number

In the first example, the attack at victim C can be detected by the frequency of the calls. In the second example, the attack can be detected by the extraordinarily long duration of the calls. In the third example, the features used before cannot be used again. Existing methods often apply user profiling to detect suspicious behavior and potential attack- or fraud cases. This way, distributed attacks as described in example three, cannot be detected. Therefore, it is necessary to apply a different method for detection. Figure 1 shows a depiction of example three with just two victims of an attacker calling a premium service number.

Existing methods often apply user profiling to detect suspicious behavior and potential attack- or fraud cases. This way, distributed attacks as described in example 3, cannot be detected. Therefore, it is necessary to apply a different method for detection.

C. Characteristic traits for detection

From the results of the preceding section, the following characteristic traits for detection can be deduced:

- **Duration of call for a certain user**: The call duration is significantly higher in comparison to the known behavior of that user.
- **Number of calls for a certain user**: The number of calls in a given time span is significantly higher in comparison with the known behavior of that user
- **Number of calls for a certain destination number:** The number of calls that has been conducted to a given (premium rate service-) destination number in a given time span is suspicious

The first two of these characteristic traits can be detected by applying user profiling if the perspective of a single user is applied. To be able to detect attack attempts using the number of calls, a new method has to be devised. This will be described in Section VI.

 ISBN: 978-1-61208-357-5

V. BASIC CONCEPT OF DETECTION METHOD

Because of the large amount of call attempts that are distributed to many users, it is necessary to devise a profiling method that does not differentiate single users, but destination numbers. This method is named *Call Destination Profiling* and will be described in this section.

Call Destination Profiling differentiates single Call Detail Records (see Section IV) by destination number. Compared to user profiling, a destination number is been looked upon as a "user". For each destination number, two profiles are generated and analyzed to detect attack- or fraud attempts. The *Past Behavior Profile (PBP)* is used to describe the behavior in the past. The *Current Behavior Profile (CBP)* is used to describe the behavior in the present.

A. Profile

In this method, a profile describes the behavior of a destination number and not the behavior of a user. Because it is possible for different users with different behavioral patterns to conduct calls to a given destination number, it is not possible to use the same behavior-describing statistics (features) as in user profiling. In user profiling, it is often the case to collect statistical data on the duration and the frequency of calls [2] [4] [5] [11] [15]. Since different callers may conduct calls of different length, it is less reasonable to collect statistical data on the duration of calls.

As mentioned in Section V, the number of calls to certain destination numbers represents an important feature for profiles used to detect the described attacks. For this reason, the following features are used in the PBP:

- Arithmetic mean of the number of calls per hour *(MeanCalls)*
- Standard deviation of the number of calls per hour *(StdCalls)*

In addition to those features, the time span t_{PBP} that the PBP will comprise has to be determined. If t_{PBP} is too long, it will take longer to initialize it with data. On the other hand, it will offer more robust statistics.

If t_{PBP} is too short, the statistics describing the past behavior may be not robust enough, possibly introducing inaccuracies into the detection process.

Based on findings in our preliminary work [9], the following rules apply for the construction of profiles: If t_{PBP} comprises a time span of less than one week, then "gaps" in the statistics will result. These gaps will cause large deviations of the measurements in the accumulated statistics. Furthermore, if the profiles are too short, e.g., one single day, large deviations will also occur. This is because the number of measurements is too low. For this reason, t_{PBP} will be set to one week, as it has also been done in our preliminary work.

In contrast to the preliminary work, a different profile time span t_{CBP} will be applied for the CBP. This is justified by the use of a different comparison function, which is described in more detail in the following Section. For the CBP, especially the number of unique callers *(NumCallees)* and the number of calls *(NumCalls)* is of great relevance. The length of the CBP determines the effects of individual fraud cases on the statistics of the profile. If *MeanCalls* and *StdCalls* relate to calls per hour, a length of one hour is determined by this. Longer or shorter profiles are more suitable for fraud attempts that are spread farther or closer on the time scale. For the time being, a profile time span t_{CBP} of one hour was applied.

Figure 2 displays a simplified diagram of both profiles in relation to time, as well as the features used.

B. Comparison of profiles and fraud detection

As already mentioned, the comparison function for the profiles differs from the function used in our preliminary work.

$$CallLimit = MeanCalls + StdCalls \cdot G_R + A_R \quad (1)$$

If CBP comprises a shorter time span as the PBP, the comparison can obviously not be conducted in the same way as before. The comparison will now be done in the following way:

A threshold *CallLimit* for each destination number is calculated from the features *MeanCalls* and *StdCalls* of the PBP using (1). A weighting parameter G_R has been introduced for the feature *StdCalls*, to allow for a finer adjustment of the relative component $MeanCalls + StdCalls$. Additionally, an absolute component $A_R$has been added to enable the analysis of infrequently called destination numbers. This component is used to compensate for errors as well, as long as the profile is still empty. Furthermore, the absolute component A_R and the weighting parameter G_R have to be selected depending on the geographic destination region *R* of the destination number. Region *R* is distinguished into national calls, mobile calls and international calls. This is to allow for a different treatment of national, mobile and international calls, each causing different costs, and differing in regard to potential damages from the perspective of telecommunication service providers.

The threshold *CallLimit* is finally compared to the feature *NumCalls* within the CBP to decide upon fraudulent or non-fraudulent behavior using (2).

$$Fraud = \begin{cases} true, & NumCalls \geq CallLimit \\ false, & NumCalls < CallLimit \end{cases} \quad (2)$$

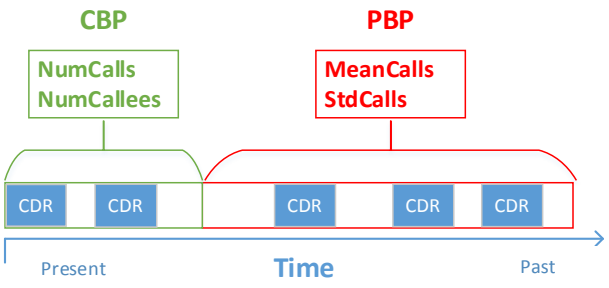

Figure 2. Depiction of the current behavior profile and the past behavior profile in relation to time

If the threshold is exceeded, the related call will be marked as fraudulent. A detection using the number of callers *(NumCallees)* can be conducted as an option. For detection, the number of calls is the most important parameter, which is very meaningful for administrative staff to support their final decision in the process.

VI. PROTOTYPE

In this section, results from a prototype implementation of the devised method are described and analyzed empirically. In Subsection A, the data set in use is specified. Subsection B describes the experimental setup. The final results are presented in Subsection C.

A. Used Data Set

To evaluate the prototype implementation, real life traffic data (CDRs) provided by toplink GmbH has been used. The data comprises calls from a time span of two weeks containing about 3.5 million calls. Only the portion of the data with outgoing calls was used, because incoming calls are not relevant to the analysis. The outgoing calls amount to about 470,000. Table I shows the distribution of the calls for the regions national, mobile and international and are split into connected and unconnected calls.

TABLE I. NUMBER OF CDRS FOR EACH REGION

REGION	AMOUNT
CONNECTED	325,947
NATIONAL	274,205
MOBILE	42,669
INTERNATIONAL	9,073
UNCONNECTED	153,330
NATIONAL	112,476
MOBILE	24,570
INTERNATIONAL	16,284
TOTAL	479,277

In the first week, no attack attempts (fraud) were contained. This part of the data was applied to initialize the behavior profiles, building the features. In the second week, normal call traffic is contained as well as about 20,140 fraudulent calls following the typical Fritz!Box attack pattern. The second week has been used to test the detection abilities.

B. Experimental Setup

First of all, the relevant thresholds had to be determined, because this is a necessity for high-quality detection results. To accomplish this, a single run of the method, without the fraud detection, is conducted with the first week of the data and every feature value at the time of each call is recorded. The thresholds are estimated by analyzing the resulting values of the CBP for fraud and non-fraud cases and for each region (national, mobile, international). The 99%-quantiles of the number of calls from the CBP, for connected and unconnected calls as well as national, international and mobile calls each, have been recorded and used as the absolute threshold A_R for each region. The parameter G_R, representing the relative threshold, has been set to $G_R = 1$, for testing purposes.

Finally, a test run with the activated fraud detection and the previously measured thresholds is done and the detection quality is evaluated by comparing the detected cases to the known cases of fraudulent behavior.

The approach can be described with the following steps:

1. The detection method is deactivated at first
2. The profiles are initialized using the first week data set
3. Thresholds are calculated from CBP values as described before
4. The detection method is now activated
5. The second week data set is now used as input
6. The results from the detection method are compared to the known cases of fraudulent behavior

C. Results

Thresholds have been determined for successfully connected as well as unconnected call attempts, each for national, international and mobile calls. Also, the profile values have been calculated and recorded.

Unfortunately, the thresholds determined herein cannot be published for security reasons. This would especially allow fraud attackers to refine their attack patterns. On the other hand, the thresholds in this case represent the actual test data and wouldn't be representative for the situation at other telecommunication service providers. For this reason, only the results for the detection method are described.

The arithmetic mean and the standard deviation both represent valid values to generate relative thresholds, as mentioned in Section VI-B. An adjustment with the parameter G_R is only necessary in individual cases.

Under these testing conditions, the detection method achieved a false positive rate of 0.7% or 3,355 false positives (as show in Table II). Of the known attacks in the data, the detection method was able to identify all attacks, resulting in 100% detection rate or true positive rate. However, there is the possibility that not all attacks are detected because some may be unknown. An estimation of a true positive rate of about 95% would be more appropriate.

TABLE II. DETECTION RESULTS

	AMOUNT	RATE
FALSE POSITIVE	3,355	0.7%
TRUE POSITIVE	20,140	100%

Compared to the results achieved in comparable related work (see Table III), which utilizes unsupervised user profiling, with a FPR of 4% and a TPR of 75% [3] and our previous work with a FPR of 1.22% and a TPR of about 90% [9], these measurements are as good or even better.

 ISBN: 978-1-61208-357-5

TABLE III. COMPARISON OF FPR AND TPR

	TPR	FPR
THIS WORK	95%	0.7%
PREVIOUS WORK [9]	90%	1.22%
RELATED WORK [3]	75%	4%

On the other hand, no direct comparison is possible, because the detection method itself is partially different, applying a modified approach of user profiling. Additionally, the number of callees *(NumCallees)* has been found a viable criterion for administrative staff to make decisions on fraudulent or non-fraudulent behavior.

VII. CONCLUSION

The presented method successfully detects distributed fraud attacks that are conducted using multiple Fritz!Box units. The test results show that the method may also be applied to similar attack patterns in the future. It has to be stressed that the focus of this work has been on devising a universally applicable method rather than a specialized one, because the security vulnerability in the Fritz!Box has since been patched, but it is possible to use different hardware units for similar attack patterns in the future.

The method offers a low false positive rate. An experimental evaluation showed that all known cases of fraud attacks in the test data were detected.

VIII. FUTURE WORK

In future work, a further evaluation of call destination profiles will be done.

For example, neural networks could be applied as well, as in [15], delivering comparable results. Neural networks are not as transparent as basic statistical approaches, such as used in the presented method. Other techniques may also be applicable, for example support vector machines (SVM). On the other hand, significantly more data than in the presented case would be necessary for training. Since the training data should not contain fraud cases, the effort for generation from real life traffic data would be high. The presented method is also to be integrated into the fraud detection framework developed within this research project.

ACKNOWLEDGMENT

We would like to thank the state of Hessen, Germany for supporting this work by providing the necessary funds by the development program LOEWE. Also we would like to thank toplink GmbH from Darmstadt, Germany for cooperating with us in our project and providing essential support, data and knowledge for research and development of practical fraud detection methods. We would also like to thank Sandra Kübler for her valuable comments and general input on the subject.

REFERENCES

[1] Communications Fraud Control Association, "Global Fraud Loss Survey," October 2013. [Online]. Available: http://www.cfca.org/pdf/survey/CFCA2013GlobalFraudLossSurvey-pressrelease.pdf. [retrieved: 6, 2014].

[2] M. Taniguchi, M. Haft, J. Hollmen, and V. Tresp, "Fraud detection in communication networks using neural and probabilistic methods," in Proceedings of the 1998 IEEE International Conference on : Acoustics, Speech and Signal Processing, vol. 2, 1998, pp. 1241-1244.

[3] P. Burge and J. Shawe-Taylor, "Detecting Cellular Fraud Using Adaptive Prototypes," in Proceedings AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management, AAAI Press, 1997, pp. 9-13.

[4] C. S. Hilas and P. A. Mastorocostas, "An application of supervised and unsupervised learning approaches to telecommunications fraud detection," Knowledge-Based Systems, vol. 21, no. 7, pp. 721-726, 2008.

[5] H. Grosser, P. Britos, and R. García-Martínez, "Detecting fraud in mobile telephony using neural networks," in Proceedings of the 18th international conference on Innovations in Applied Artificial Intelligence, Bari, Italy, Springer-Verlag, 2005, pp. 613-615.

[6] heise online, "Bericht: Deutsche Telekom wertet Verbindungsdaten sämtlicher Telefonate aus | heise online," [Online]. Available: http://www.heise.de/newsticker/meldung/Bericht-Deutsche-Telekom-wertet-Verbindungsdaten-saemtlicher-Telefonate-aus-1933436.html. [retrieved 6, 2014].

[7] AVM GmbH, 06 02 2014. [Online]. Available: https://www.avm.de/de/News/artikel/2014/sicherheitshinweis_telefonmissbrauch.html. [retrieved 6, 2014].

[8] R. Eikenberg, "Hack gegen AVM-Router: Fritzbox-Lücke offengelegt, Millionen Router in Gefahr," 07 03 2014. [Online]. Available: http://www.heise.de/security/meldung/Hack-gegen-AVM-Router-Fritzbox-Luecke-offengelegt-Millionen-Router-in-Gefahr-2136784.html. [retrieved 6, 2014].

[9] A. Wiens, T. Wiens, and M. Massoth, "A new Unsupervised User Profiling Approach for Detecting Toll Fraud in VoIP Networks," in The Tenth Advanced International Conference on Telecommunications, to be published 2014.

[10] TELES AG, [Online]. Available: http://www.teles.com/en/teles.html. [retrieved 6, 2014].

[11] Y. Moreau, H. Verrelst, and J. Vandewalle, "Detection of Mobile Phone Fraud Using Supervised Neural Networks: A First Prototype," in Proceedings of the 7th International Conference on Artificial Neural Networks, Springer-Verlag, 1997, pp. 1065-1070.

[12] T. Kapourniotis, T. Dagiuklas, G. Polyzos, and P. Alefragkis, "Scam and fraud detection in VoIP Networks: Analysis and countermeasures using user profiling," in FITCE Congress (FITCE), 2011 50th, 2011, pp. 1-5.

[13] T. Fawcett and F. Provost, "Adaptive Fraud Detection," Data Mining and Knowledge Discovery, vol. 1, no. 3, pp. 291-316, 1997.

[14] "Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Bundesdatenschutzgesetz (BDSG)," [Online]. Available: http://www.bfdi.bund.de/cae/servlet/contentblob/409518/publicationFile/25234/BDSG.pdf. [retrieved 6, 2014].

[15] P. Burge, J. Shawe-Taylor, C. Cooke, Y. Moreau, B. Preneel, and C. Stoermann, "Fraud detection and management in mobile telecommunications networks," in European Conference on : Security and Detection. ECOS 97., 1997, pp. 91-96.

 ISBN: 978-1-61208-357-5