Executive summary:

In traditional telecommunication networks, fraud is already a threat depriving telecom operators of huge amounts of income every year. With the migration from circuit-switched networks to packet-switched networks, it is expected that the related situation will be worse, due to the openness and vulnerabilities associated with IP-based infrastructure.

The SCAMSTOP project addresses the problem of fraud and service misuse in VoIP networks. It also offers a prototype implementation of a Fraud Management System (FMS) that can be deployed and used by the SME partners to deal with the scam activities.

In order to build the SCAMSTOP framework, several techniques have been designed, developed and implemented. In SCAMSTOP, the following techniques have been designed: rule-based classification; signatures; clustering based on the Nearest Neighbor Algorithm and the Balanced Iterative Reducing and Clustering using Hierarchies (BIRCH); Neural Network self-Organizing Map (NN-SOM), and Bayesian Networks. For coordinating the activities of the different detection algorithm, an event-based system was developed. The event-based system is the backend of a friendly web interface enabling the fraud expert to configure the different components and to visualize the results. The SCAMSTOP architecture was discussed in the deliverables D2.1 and D2.2, however, the software details were described in D3.1 and D3.2.

The testing activities were based on both real life and synthetized data. The real life data was delivered by the VoIP providers and included both known and unknown fraud cases. The latter refers to the call center behavior for which, the VoIP providers do not have any means to deal with. A software tool has been extended in order to generate synthenized data. Most of the detection techniques were tested against both fraud categories and in laboratory environments as well as a part of the VoIP providers' infrastructure. The obtained testing results were summarized in the deliverable D4.1.

The VoIP providers have shown interest in the framework developed by the research institutes especially that some of the algorithms detected several misconfiguration aspects related to the involved VoIP components. The VoIP providers also reported some weaknesses that require further investigation. The VoIP providers recommended to improve the Bayesian Network algorithm and the rule based system.

It is worth to mention that the data used for testing had a heavy impact on the performance of the detection algorithms. The CDRs data included in particular accounts for testing and others without external PSTN connections which made the interpretation of the obtained results a bit challenging. In future investigations, special attention will be paid to such issues and different categories of data will be used.

Project Context and Objectives:

Project context

Different definitions of fraud are reflected in the literature. However, fraud can simply be seen as any activity that leads to the obtaining of financial advantage or causing of loss by implicit or explicit deception. In traditional telecommunication networks, fraud is already a threat depriving telecom operators from huge amounts of money every year. With the migration from circuit-switched networks to IP-based networks, it is expected that the related situation will be worse. This is mainly due to the lack of strong built-in security mechanisms and the use of open standards in IP-based networks. In fact, the openness, innovative services and low cost structure of voice over IP (VoIP) services has helped VoIP providers to attract large numbers of subscribers over the past few years. These same reasons have unfortunately also attracted attackers and malicious users as well. Based on a 2011 recently published Fraud Loss Survey, the Communication Fraud Control Association (CFCA) reports that telecom fraud costs businesses more than $40 Billion every year.

Like any telecommunication operator, the VoIP providers are certainly a preferred target of fraudulent persons. Fraud can cause a loss of revenue which is by itself a huge problem in a market based on very tight margins. On the other side, news about successful fraud attacks on a VoIP provider can very easily tarnish the reputation of the provider and would cause a drop in confidence followed by a drop in stock prices and loss of subscribers.

It is worth to mention that fraud detection and intrusion detection have been traditionally completely separate research areas. Fraud detection solutions have been mainly developed by companies to protect their assets and these solutions were usually undisclosed. However, one can find few research works dealing with fraud detection and most of them are based on the use of artificial intelligence.

Intrusion detection is an area where the network is monitored for malicious activities or policy violations. The monitoring output is then reported to a management system. Intrusion detection is an area developed by the research community during the last 20 years at least. However, commercial solutions appeared a bit out of date. In addition to that, these solutions just adopted some intrusion detection simple solutions. As research is the main motivation behind intrusion detection, the related area seems to evolve faster than fraud detection.

As the convergence between telecom networks and the Internet is occurring and a lot of telecom services are being replaced by similar services which are IP-based, it is legitimate to ask ourselves whether it still makes sense to keep fraud detection and intrusion detection separate. Taking into account all the aforementioned drawbacks, the main objective of SCAMSTOP is to investigate fraud detection in the light of intrusion detection.

VoIP deployment

Understanding the business model of the VoIP providers is the first step for developing an anti-fraud system that can be successfully deployed by them. For instance, if we intend to develop per user signatures and profiles, we need first to check the VoIP providers' price plans. Just implementing features such as the number of mobile, national or

international calls during a given time interval might not help as with the current proposed flat rate options, most of these calls are free of charge and no fraud activity is expected. As an exception here, the VoIP provider might want to monitor the flat rate based service usage to check whether this service is profitable or not.

The VoIP providers do not only have residential as customers but often enterprises. An enterprise can either,
- use an online PBX service where all VoIP services are offered by the VoIP network. The customer uses closed sets of IP phones or SIP gateways (offered by the VoIP provider or one of its distributors). In this offer, the customer does not get any credentials username/password), both the IP phones and SIP gateways are automatically provisioned.
- or use its own PBX (or a different device) to place and receive calls using the VoIP network. The configuration data (server, username, and password) that the customer has to use is usually provided by the VoIP provider when the service starts

To connect the enterprise PBX to the VoIP provider network, a SIP trunk is used. A SIP trunk is a service offered by the VoIP provider including multiple voice sessions (as many as the enterprise needs) in addition to other features such as Instant Messaging (IM), presence applications, and data sharing.

Usually, the VoIP services provided to enterprises are charged on a post-paid basis. This, unfortunately, opens doors for potential fraudulent activities.

SCAMSTOP objectives
The SCAMSTOP project aims at protecting VoIP infrastructures by mitigating fraud attempts, thus protecting the VoIP providers against revenues losses and users against theft. This is being achieved by providing a complete solution for the VoIP providers to help them define an efficient fraud detection and management strategy. Based on the above description, the SCAMSTOP project pursues the following major objectives,

- Design and implement a general framework for detecting and protecting VoIP services from fraud and misuse. Within this framework, the different usage scenarios of VoIP are to be considered and the varying needs of the participating SMEs will be accommodated. This framework will present a general guidance on the deployment of fraud detection systems in VoIP environments in terms of monitoring, detection and alarming facilities.
- Specify and develop innovative and adaptive algorithms for misuse and fraud detection. This will be the core effort in SCAMSTOP. In the design of these algorithms we will not only aim at achieving a high detection rate but also target a scalable design and low processing and memory resources so as to ensure the applicability of these algorithms in large scale VoIP deployments.
- Support different means for detection that can be dynamically adapted to the user and provider specific needs as well as to the traffic patterns.
- Implementation, integration and testing of the developed tools and solutions in a provider's VoIP infrastructure

SCAMSTOP objectives for the first year

As mentioned in the Technical Annex (page 45), the SCAMSTOP project is supposed to achieve during the reporting period M1-M12, the following technical objectives:

- Investigation of fraud scope: define the terminology, describe the typology, provide some statistics
- Investigation of fraud in telecommunications: fraud classification, describe the corresponding typology, investigate fraud in PSTN and mobile networks (scenarios, tools, etc)
- Investigation of fraud problem in VoIP networks: comparison with fraud in traditional networks, provide fraud use case scenarios in VoIP, describe tools used for carrying out fraud activities
- Investigation of fraud detection in VoIP networks: description and evaluation of the existing techniques, describe the data to be collected for fraud detection and the problems facing the fraud detection in VoIP networks
- Anti-fraud architecture: identification of the different blocks of the architecture, identification of the algorithms to be used, as well as the interfaces between the different components
- Starting the development of the anti-fraud framework: a basic version of the rule-based fraud detection will be provided
- Design and development of risk assessment methodology for the SCAMSTOP Architecture

SCAMSTOP objectives for the second year
The SCAMSTOP project aimed at achieving the following objectives during the time period M13-M24,

- Explore the available components for realizing some of the needed functionalities such as SIP servers and clients, data mining frameworks, and system experts, and investigate their suitability for the project
- Explore the Call Detail Records (CDRs) fields that can be used for developing the detection algorithms
- Design and development of tools to generate fraud-based CDR
- Develop various algorithms for VoIP fraud detection. These include: Bayesian Networks, Neural Networks Self-organizing Maps (NN-SOM), Nearest Neighbour Algorithm, Balanced Iterative Reducing and Clustering using Hierarchies (BIRCH), signature based technique, and rule based technique
- Specify and develop an event-based system that will coordinate the activities of the different detection components
- Specify and develop a friendly web interface that allows the fraud expert to configure the different algorithms and visualize the results
- Prepare CDRs data for testing purposes. Here some SIP client needs to be modified to produce synthetized data. Real life data offered by the VoIP providers need also to be transformed to a format that can be used by the algorithms
- Test the different algorithms separately
- Test the entire framework
- Integrate the SCAMSTOP framework with the VoIP providers' infrastructures, test it and provide feedback to the RTD performers
- Update on the risk assessment methodology for SCAMSTOP Architecture

Project Results:

This part briefly describes the main achievements of the SCAMSTOP project.

Problems addressed

The classification of fraud can be achieved in different ways according to the point of view from which the related activities are observed. However, the categorization that is generally cited in the literature is the following,

- Subscription fraud: this occurs from obtaining an account or service, often with false identity details, without the intention of paying. The account is usually used for call selling or intensive self-usage.
- Superimposed fraud: a fraud activity is said to be superimposed when a fraudster illegally gets resources from legitimate users by gaining access to their phone accounts. This kind of fraud can be detected by the appearance of unknown calls on the bill of the compromised account. Scenarios describing this kind of fraud include: mobile phone cloning, breaking into a PBX system, etc.

Although the SCAMSTOP project addresses both categories, we also would like to attract the attention to a fraud scenario that can be considered as part of the subscription fraud; however, it is rarely mentioned in the literature. This scenario is the activity where the service usage does not match the subscription type. For instance, some customers can subscribe for a residential service which is usually cheaper than a business one and use it for business purposes. Another case is where the customer subscribes for the option that allows it to use its own PBX, and then use this PBX as a dialer for call center purposes. On the infrastructure side, this service abuse looks like a Denial of Service (DoS) attack, affects the VoIP provider's network and reduces its capacity. The badness of this situation depends on the capacity of the SIP trunk and how often the related operation is repeated. Another scenario that does not in any case match the subscription type is the use of the provider infrastructure to build some kind of subscriber database that can be sold to marketing companies. For instance, there are customers that look for operational mobile accounts by trying to connect to them without establishing the calls. Based on the provisioning response messages, they determine whether the targeted mobile accounts are operational or not.

Unfortunately, the VoIP provider cannot a priori be aware of the device that is installed in the customer's premises and for which purpose it is being used. In addition to that, the VoIP provider that has hundreds of thousands of customers cannot easily check the installations related to all these accounts.

Achievements

The SCAMSTOP project delivers a platform for VoIP fraud detection and management. Within this project, a bunch of components were developed and tested. These components belong to three main levels,

- Detection level: Here, several standalone modules were developed to detect fraud activities. This particularly includes a rule system and clustering algorithms

- Management level: Here, a rich management interface allowing alarms and results visualization, rules creation, and algorithms configuration was developed
- Coordination level: Here, an event-based system for correlating the activities of the detection modules

The overall architecture of the SCAMSTOP is depicted in the attached file (SCAMSTOP_architecture_High_level.jpg).

In the following paragraphs, we explain in more details each of the mentioned levels.

Detection Level

One. The rule system

The rule-based approach defines fraud patterns as rules. The rules might consist of one or more conditions. If all the conditions are met, an alarm is produced. The rules can simply be applied to the Call Data Records (CDRs). In this section, we briefly discuss the main features of the rule system. For more details, we refer to the deliverables D2.2, D3.1 and D4.1.

For creating composed rules, we undertook the following tasks:

- Definition of the features needed to be used for creating the rules (IP address, Daily Quarter, call type, time window size, etc)
- Development of a tool for checking the syntax of the rules
- Identification and storage of the rules (validation time, criteria to fetch them)
- Rules enforcement

For the alarms generation part, we undertook the following tasks:

- Definition of the alarms format and content
- Development of an interface for alarms visualization

Implementation

The rule-based system is intended to be used for detecting users' abnormal behavior. For this purpose, thresholds are used, to verify whether a certain feature (e.g the call duration) exceeds a given threshold. In our implementation, it is possible to apply the rules on a single or a set of CDRs. To apply a rule on a collection of CDRs, a mechanism, similar to "counters", was implemented. The counter functionality was designed to provide as much flexibility as possible, supporting on the fly creation and also sliding window (here the counter can be the size of the window). Through a sliding window, it is possible to define rules such as:

"If a user A makes more calls in a given time slot than a given threshold, raise an alarm".

In the beginning, existing rule-based systems as CLIPS1 and JESS2 have been studied in order to use them as a basis for the rule engine. However, we found out that these systems are very complex and cannot be easily enhanced with mechanisms such as sliding windows. Therefore, we decided to develop our own rule-based system. For simplicity reasons and for easier integration within the Event System module, Python was used as a programming language.

Rule language

In the SCAMSTOP project, a simple language to define the rules was introduced. A readable rule is typically created as a sequence of sub-rules. These sub-rules will be checked sequentially. Each time a new CDR comes, the rule is applied. A sub-rule consists of two parts: the condition and the action. The action is only performed if the condition is evaluated as true. The action contains information about either an alarm that should be generated or a counter that needs to be created or a counter value that needs to be increased. A condition can also contain binary and unary operators and sub-conditions. After the parsing, the conditions are stored in a tree data structure. The action is stored in a list data structure sequentially built on the input order. To handle the monitored CDRs, an identifier is used for each feature of the CDR data that can be built into a condition.

The counter mechanism is very important for the Rule-based System. It is used for measuring, how often an event occurred in the CDRs within a given time window. In our context, each counter has an identifier. Counters can be created and deleted. A counter is usually initially created with a "Threshold" value and additionally (if needed) the length of the counters availability (used for the sliding window). If no time for the counter availability is set, the counter will be available in the Rule-based System as long as it runs. Functions to retrieve the current counter value and increase the counter have been implemented. If a counter reaches a value above the initially set threshold, an alarm will be generated via the event system. Their necessity will be seen in the upcoming examples.

One important issue with the sliding window in counters refers to the time stamp. The rule-based system does not generate its own time stamp. All time information will be extracted from the input data of the CDRs. This behavior enables executing the rules over the CDRs in a near real-time manner.

From the Web interface to the rule system

The user defines a new ruleset through the Web interface. This can be achieved in a user friendly way, since the user does not need to specify each sub-rule and can use predefined functions. The Web interface will generate the necessary sub-rules out of the better readable input. The Web interface also saves the new rules in a database and sends the "IDs" of the rules to the event system with a special event type. The event server forwards this event to the rule system. The rule system reads the new rules from the database and applies them.

Example

The following ruleset refers to the example "If a user generates more than 10 premium calls within 1 hour, twice a week, raise an alarm."

```
'is_premium & !have_counter("$src_id premium")' , 'init_counter("$src_id
premium" 3600)'
'is_premium == 1' , 'count("$src_id premium" 1 timestamp)'
'((get_counter("$src_id premium") greater than 10) &
!have_counter("$src_id premium 2 times")) & is_premium',
'init_counter("$src_id premium 2 times" 604800)'
'get_counter("$src_id premium") greater than 10' , 'count("$src_id
premium 2 times" 1 timestamp)'
'(get_counter("$src_id premium") greater than 10) & (is_premium == 1)' ,
'del_counter("$src_id premium")'
```

'(get_counter("$src_id premium 2 times") greater than= 2) & (is_premium == 1)' , 'alarm("User $src_id make 2 or more times 10 premium calls in a week") del_counter("$src_id premium 2 times")'

Additional information can be found in,
- SCAMSTOP deliverable D2.2
- SCAMSTOP deliverable D3.1

Two. The signature based technique

Unsupervised techniques can simply be used in the case where we are not certain about which transactions in the database are fraudulent and which are legal. These techniques are in particular based on what is called "profile/signature" or "normal behavior". Here, the past behavior of the user is cumulated in order to build a profile that will be utilized to predict the user's future behavior. As this profile describes the habitual service usage pattern of the user (called "normal behavior"), any significant deviation from this profile has to be reported because it might hide some fraudulent activities. A signature can be seen as a statistical description or a set of features that captures the typical behavior of the user, namely, the total number of calls, number of calls to international/premium/mobile destinations, duration of the calls. Unfortunately, the current use of this method in telecom fraud detection does not take into account several aspects including the business plans of the VoIP providers. Moreover, the evaluation of such approaches is not an easy task with the absence of enough details. On the other side, we believe that such approach leads to problems related to the performance especially if the signature gets bigger. We also believe that using global metrics for comparison (such as the Hellinger) leads to the loss of information about individual features. This means it will be difficult to know which feature has yield to the occurred misbehavior.

When computing the signature, we also need to deal with data fluctuation in the service usage that varies from one day to another as well as the periods of inactivity in which the subscriber did not use the service. In the literature, these issues are not discussed, however they are being addressed in the context of our work. It is also worth to mention that our solution also investigates how the initialization and the update of the signatures can be achieved based on the related specification.

Our approach is as follows,

- For each user, we build a short-term (daily basis) signature based on features such as: number of calls to premium/international/mobile destinations as well as their durations
- Reduce data fluctuation by dividing the day into four time periods: morning, afternoon, evening, and night
- Remove the inactivity related information. This information is reflected by the "null" value for instance for one of the signature features. Image the case where a user did not make any premium call in the afternoon. Keeping the "null" values will affect the calculation of the mean and does not bring any valuable information regarding fraud detection
- Integrate the short term signatures into a long term signature (on a monthly basis) using the trimmed mean and the related standard deviation.
- Before we compute the trimmed mean, we transform first our data distribution to a normal one using the logarithm or the square root function

- To check for misbehavior, we compare the long-term and short-term signatures on a feature basis using the z-score technique
- The update of the long term signature is straightforward due to the way the signature is defined.

The use of z-score for each feature of the signature directly gives the impact of this feature on the entire signature. We have also shown that the z-score and the Hellinger distance are linked to each other which give advantage to the first one as it is easier to manipulate. In addition to that, and contrary to the solutions already proposed in the literature, we use different appropriate profiles instead of a complex one as it is easier to manipulate them separately.

Initialization
New users might also be fraudsters. This means such users have to be monitored right after they start using the service. To build a reliable profile for a user, we need to observe him for some time (a week, a month, etc). However, this cannot be applied for users that just sign up for the service. A typical behavior of a subscription fraud is the excessive usage of an account or a subscription in a very short time interval which enables him to escape the detection. It turns out that the signature initialization is an important step in detecting and preventing subscription fraud. Signature initialization is a challenging task due to the very limited data about the new subscribers.

Dealing with a new subscriber in our context relies on the signature technique that we have already discussed. In the signatures, the user service usage is mainly described by the mean and the related standard deviation. In addition to that, the signature is updated on a per day basis. As a consequence, a new subscriber can be observed during two days, if no fraudulent activity is met and required an interruption of the service, this new user will be assigned a signature in the way discussed earlier. This is possible due to the fact that the mean and the standard deviation for each feature can be computed over two days but not over one day.

Observing the new subscriber for the first two days can be achieved through looking particularly whether this subscriber,

- has made at least one international call (or a premium call) with a duration greater than a predefined threshold
- or made a call to a destination from the black list.

We assume here that the VoIP provider maintains a list with phone numbers or accounts IDs for subscribers that were committing fraud. In this case, this subscriber will be labeled as suspicious and will be monitored closely during the mentioned two days.

Our approach was tested on known and unknown fraud cases as it will be discussed in the testing part. A paper related to the obtained results was submitted to the SIGCOMM 2012 conference.

Additional information can be found in,
- SCAMSTOP deliverable D2.2
- SCAMSTOP deliverable D3.2
- SCAMSTOP deliverable D4.1

Three. The BIRCH Algorithm

Clustering is used to arrange a set of n users into groups, referred to also as profiles/signatures – see previous section -, such that each group consists of users whose call patterns have similar characteristics. This essentially requires clustering the m feature vectors of the n users that represent their long-term signatures.

Before looking in more detail at how clustering was used in the SCAMSTOP project, two important points are worth mentioning. The first point concerns the fundamental purpose behind clustering the feature vectors and the second the expected result of the clustering process. Specifically, in this work, clustering is used to automatically infer knowledge about the existence, number and nature of intrinsic groups in the analyzed feature vectors. In more detail, it is expected that the feature vectors fall into a few compact and well separated clusters and that these clusters are pure in the sense that some comprises only feature vectors of regular subscribers and the others only feature vectors of fraudulent users. The implication of this result is that it is feasible to reliably distinguish between regular and fraudulent users by analyzing their Call Data Records. This makes it possible to automatically detect an end user that exhibit a fraudulent behavior.

BIRCH (Balanced Iterative Reducing and Clustering using Hierarchies) is a hierarchical clustering algorithm designed to perform hierarchical clustering over particularly large data-sets. An advantage of BIRCH is its ability to incrementally and dynamically cluster incoming, multi-dimensional metric data points in an attempt to produce the best quality clustering for a given set of resources (memory and time constraints). In most cases, BIRCH only requires a single scan of the feature vectors. The principle behind this is that in BIRCH each clustering decision is made without scanning all data points and currently existing clusters. In more detail, BIRCH exploits the observation that data space is not usually uniformly occupied and not every data point is equally important. Thereby, it makes full use of the available memory to derive the finest possible partition while minimizing I/O costs. Furthermore, BIRCH is an incremental method that does not require the whole data set in advance. In addition, BIRCH is recognized as the first clustering algorithm proposed in the database literature to handle noise (i.e., data points that are not part of the underlying pattern) in an effective way.

Since clustering finds groups of feature vectors that are not known a priori, regardless of the clustering algorithm used, the clustering results need some kind of validation. In particular, the hierarchical clustering algorithms require an a posteriori decision with respect to the partition that best satisfies or reproduces the underlying structure of the feature vectors. Put it differently, inferring valuable knowledge from the hierarchy of partitions that these algorithms produce, involves using a criterion that can determine the optimal number of clusters. Over the past years, a large number of criteria for specifying the hierarchical level on which to base inferences concerning the true differences between feature vectors have been proposed. These criteria, known as stopping rules, evaluate for a given hierarchical clustering algorithm and set of feature vectors the partition of each hierarchical level by comparing it to the partitions of every other level. Although significant effort has been devoted to stopping rules, there exist no general gold standards that are capable of revealing the optimal number of clusters over sets of data objects from diverse application fields. Hence, in the context of SCAMSTOP, three well-known and widely-used

stopping rules are employed in a complementary way: the dunn, the silhouette width and the davies-bouldin indices.

Concretely, the BIRCH algorithm was implemented and used in the context of SCAMSTOP in the following way,

- Read CDRs from the CDRs database
- Separate the read CDRs on a per user basis
- Create a signature for every user following the method discussed previously
- Find suitable features to distinguish between users. This is also based on the signatures' features discussed earlier
- Apply clustering to the signatures
- Find the best clustering structure. The best number of clusters is not known a priori. The BIRCH algorithm provides such information
- Deal with time consumption and error prone process. The stopping rules can be used here
- Use heuristics to label the clusters
- Find which clusters reflect the fraudsters

The BIRCH clustering algorithm was also tested. The algorithm arranges data points (vectors in a multidimensional space) into a tree-like hierarchy of clusters. The vectors are being grouped depending on a particular distance metric that defines the radius of a cluster and the distance between two clusters. Then, we select one appropriate level of clusters that we mark as ordinary (big clusters) or suspicious (small clusters). The small clusters contain the points that represent unusual user activity, and many of such users may be fraudsters or call centers. The big clusters represent more common patterns of user behavior.

The data used for testing was provided by VozTelecom. It consists of 4825 accounts activities over a 3 months period of time with almost 31 million CDRs. We assumed in our experiments that the users' accounts existed throughout the whole testing period, so for each of the 90 days 4825 short user signatures may be produced. Every short signature contains 20 numerical characteristics and is a point in a 20-dimensional vector space. The signatures for a given day are considered as data points and clustered through the following steps:

1. the data points are being sorted by "total number of calls" in the ascending order to avoid the skewness, because BIRCH may be sensitive to the order of the input
2. the coordinates of the points are being scaled according to their standard deviations, because the spread of different characteristics is various. The scaled coordinates have the same order of magnitude
3. the scaled points are being clustered with BIRCH, using the Euclidean distance metric, cluster radius metric, inter-cluster distance metric, the branching factors B and L, and the cluster threshold T (we refer to the deliverable D3.1 for more details)
4. small clusters are being marked as suspicious, the list of users whose activity data belong to these clusters, is being compared against the test accounts provided by the VoIP provider
5. true / false positive / negative rates are computed.

Additional information can be found in,
- SCAMSTOP deliverable D3.2
- SCAMSTOP deliverable D4.1

Four. The Nearest Neighbor Algorithm

Nearest Neighbor (also known as Collaborative Filtering or Instance-based Learning) is a useful data mining technique that allows to use past data instances, with known output values, to predict an unknown output value of a new data instance. Nearest Neighbor is very successful in situations where neither regression nor classification can be applied. First, regression can only be used for numerical outputs. Classification is a serious problem with some data where the number of classes is large and previously unknown (e.g. hundred thousand products of a company). Since the behavioral groups of users can be numerous and not determined a priori, we propose a suitable solution based on Nearest Neighbors.

The K-Nearest Neighbor algorithm is one of the oldest algorithms in machine learning. Given a set of training data and a tuple X, the KNN algorithm searches the k nearest neighbors to X based on a distance measure. Our idea was to use the KNN as a clustering module in SCAMSTOP. This kind of clustering can be considered as lazy since no general model is built until a given sample needs to be analyzed. In this sense, every subscriber has its own cluster.

This solution gets rid of the difficulties of dynamic clustering such as the operations of cluster maintenance and cluster identification in case of splits and merges. This choice reveals also to be efficient if only one or a subset of subscribers need to be analyzed.

The idea is the following: for each subscriber, we monitor the K users having the closest behavior during a given time window in terms of a number of defined features. These users are called the neighbors of the subscriber in question. We update the list of neighbors after each analyzing window using a bumping algorithm. In fact new neighbors appear and old neighbors may become irrelevant. For each neighbor we track two variables: the frequency (how many times it has been chosen in the top-K neighbors) and the recency (when was the 17 last time it has been seen). The updating is done periodically during all the training period. The bumping algorithm works as follows:

```
Input:
- L1: list of old neighbors with their frequencies and recencies
- L2 : list of new neighbors
Body:
  For each neighbor in L2:
        If neighbor exists in L1:
                Update the frequency and the recency of the neighbor
  For each neighbor in L2:
        If neighbor doesn't exist in L1:
                Draw a random number in [0,1]
                  If random number greater than Threshold (We choose 0.7
in our case):
                        Choose a candidate from the L1
                        "The candidate should have low frequency
                        and should not be seen recently"
                        Replace the candidate by the new neighbor
Output:
- L3: List of updated neighbors with their frequencies and recencies
```

For the time periods where some subscribers are absent and do not issue any call activities, the lists of neighbors for these subscribers are not

updated. In this way, we compensate the effect of some contexts where a lot of subscribers go idle and it is difficult to know the real neighbors (example, weekends or holidays for professional accounts).

In the testing period, we ask the question "is there a sudden change in the neighbors of a given subscriber?". To answer this question we need to compare the neighbors discovered during the testing period with the updated history of the subscriber. This comparison is quantified using a score (s). The latter is increased for each training neighbor that is found in the testing neighbors, and it is decreased for each training neighbor that is not found in the testing neighbors. The amount of increase or decrease depends on the frequency and the recency of the neighbor in question. In result, subscribers with large negative values are revealed by our algorithm as suspected. It means that some neighbors that have been seen frequently and recently in the past are not seen any more in the testing period.

As for the list of features used for the computation of the KNN, one can mention: number of calls issued during the analyzed window, average call duration for successful calls, ratio of call success, ratio of calls towards international destinations and information entropy of the different source IPs of the caller.

For the implementation, we have used the Instance Based learner IBK from the WEKA library. IBK is a classifier based on the KNN algorithm. In our case, we use it only to calculate the Nearest Neighbors since our problem is not about classification. The used search algorithm is linear (the brute force search) and the used distance is Euclidean.

Additional information can be found in,
- SCAMSTOP deliverable D3.2
- SCAMSTOP deliverable D4.1

Five. The Neural Network Self-Organizing Map (NN-SOM)

The idea behind using NN-SOM as a fraud detection module in SCAMSTOP was based on the assumption that the behavior of an individual subscriber cannot suddenly change. Thus if historical behavior patterns were used during the training of the neural network and the current behavior pattern is given as input, then the current pattern should be classified as a known pattern. If this will not happen then we should consider the subscriber behavior as a possible fraud. In this sense, every subscriber has to have its own neural network.

On the other hand, special temporal situations may happen, like an emergency situation such as an earthquake or a national holiday on which it is usual for subscribers to change their calling patterns. In such situations a change in "normal" behavior should not be considered a fraud. To overcome this problem, we partition the subscribers into groups and for each group another NN-SOM network is created using the aggregated records of all users in a group as training data. Similar to the K Nearest Neighbor (KNN) algorithm, we do not have to create perfect partitions of the subscribers. The subscriber can participate to one or more groups that were having the closest behavior during a given time window. This can be accomplished by comparing the output of the individual NN-SOM of the subscriber with input from the same period of the other group participants or use the clustering of the subscribers of the KNN algorithm. When we observe a possible fraud detection on an individual subscriber the input record of the subscriber is also fed as

input to the NN-SOM of the group and the other individual NN-SOM of the subscribers belonging to group are activated and are fed the corresponding users data. If the group behavior has also changed this is an indication that we may not have a fraud situation. If the other members of the group have not changed their behavior then the fraud indication is stronger.

The implementation of the algorithm is based on the Encog Neural Network Framework (see http://www.heatonresearch.com/encog online). For each subscriber, a lightweight NN-SOM is created having 9 input neurons and 50 output neurons. The input record represents aggregated values of call data for each subscriber for a predefined period of time (e.g. 60 min). More specifically the input record comprises in particular the following fields: quarter of the day, working day or not, number of calls, average duration of calls, percentage of international calls and percentage of premium calls.

A high level pseudo code for the training phase is as follows,

```
Input:
          L1: List of CDR
          S: List of Subscribers
          T: Training Period
          Tp: Time partition step
Body:
          For each s in S
              For each Tp in T
                    Extract input record( s , Tp ) from L1
                    Update NN-SOM (s)
              Persist NN-SOM(s) in Database
Output:
           Forall s in S exists NN-SOM(s) in Database
```

A high level pseudo code for the fraud detection phase is presented below,

```
Input:
          L1: List of CDR of subscriber s
          Tp: last Time partition step
Body:
          Extract input record( s , Tp ) from L1
          Fetch NN-SOM(s) from Database
          Feed input record( s , Tp ) in NN-SOM(s)
          If (Fraud_detected) by NN-SOM(s)
               Fetch NN-SOM(group(s)) from Database
               Feed input record( s , Tp ) in NN-SOM(group(s))
               Foreach s' in group(s)
                    Fetch NN-SOM(s') from Database
                    Fetch L2: List of CDR of subscriber s' for Tp
                    Extract input record( s' , Tp ) from L2
                    Feed input record( s' , Tp ) in NN-SOM(s')
                    Get possible fraud percentage from NN-SOM(s')
               Generate ballot for group special situation
               Decide if special situation exist
               if (no special situation)
                        Generate fraud alarm
               else //We have a special situation in all group members
```

```
                    Update NN-SOM (s)
                    Persist NN-SOM(s) in Database
          else
               Update NN-SOM (s)
               Persist NN-SOM(s) in Database
Output:
           1. An updated NN-SOM(s)
           2. An optional fraud alarm
```

The NN-SOM was tested using data provided by VozTelecom. In a modern server with sufficient memory, the initial training phase for the neural network for each subscriber required 0.44-1.04 sec, with an average training time of 0.6 sec. The initial training phase is required only once, although incremental training of the neural networks is constantly required in order to keep the neural networks

Additional information can be found in,
- SCAMSTOP deliverable D3.2
- SCAMSTOP deliverable D4.1

Six. The Probabilistic approach

The probabilistic approach generates the user profile through the elaboration of the CDRs. This user profile includes for every type of user his origin, the destination and the average Duration. After the training time, the system can put a flag on the user with his profile. All the user profiles populate a user profile database, which keeps all the user profiles for legitimate and non-legitimate users. The non-legitimate users have specific characteristics that deviate from the legitimate (e.g. calling number selection towards unusual destination, calling duration deviates from the average call duration).

Both user types are stored in to the user profile database. The user profile database communicates with the Policy Controller. The policy controller monitors the user profile database, and makes decisions, based on user profiles. If a user belongs to a certain profile and a number of his calls deviate from that, then the Policy controller decides to communicate with the active or passive components of the system. The Policy Controller may include both passive and active components.

In this approach, we calculate all the conditional probabilities between our different variables and store them in a table. Such condition probabilities include the calculation of probability of odd destination country (i.e. Africa) given that the time is Morning, the Calling Number is Fixed and the call duration exceeds a threshold. The aim of this Probabilistic Approach is to generate alarms for the following scenarios,

- Scenario 1: Increased number of calls to a certain African country that have short duration and spread throughout the day.
- Scenario 2: Increased number of calls to a non-European destination that have long duration and are made during the morning.

Input: Read from the CDR the following information
- Source specific number (SN)
- Source area code (or mobile company code) (SA)
- Destination specific number (DN)
- Destination country code (DC)

- Destination area code (or mobile company code) (DA)
- Time of day classification: (CT)
 Night (00:01-08:00)
 Morning (08:01-16:00)
 Evening (16:01-12:00)
- Weekday/Weekend classification (CD)
- Duration classification (DU)
 Short (0-90 sec)
 Medium (90-240 sec)
  Long (240 or more sec)
- Call type (TY):
 Local, Long-distance, Mobile or Other

Confidence Interval:
Generate the following condition probabilities
P(DC, CD, CT, DU, TY)=P(DC)P(DU/DC)P(CD/DU)P(TY/DU)P(CT/TY)
DC: Destination Country, CD: Call Day, CT: Call Type, DU: Duration, TY: Call Time
Input CDR under tests
Output

Number of False Alarms, Number of True Alarms
The Probabilistic algorithm was tested using one-month data provided by the Greek VoIP Provider ViVA where all the above data were provided without any anonymization process. These data were used in order to generate synthetic fraudulent CDR data using the SIPp tool.

Additional information can be found in,
- SCAMSTOP deliverable D3.2
- SCAMSTOP deliverable D4.1

Management Level

The aim of the SCAMSTOP management framework is to help the VoIP provider to administrate the SCAMSTOP platform. Through a friendly user interface, the administrator can,
- Visualize the results of the detection
- Visualize the alarms generated
- Search for a given user and visualize his activities
- Filter activities
- Create and apply rules
- Configure and schedule the detection

In the context of SCAMSTOP, a Web interface based on Django (see http://www.djangoproject.com/ online) which is a high level Python Web framework that encourages rapid development and clean, pragmatic design was developed. In this section, we will just list the functionalities that this interface supports. For the details, we refer to the attached guide (Guide for the management interface.pdf).

The management interface allows to list all the users or to look for a certain user if we have his identifier. The identifiers we are currently using are the ones provided by the VoIP partners. Once, a user is selected, different frames showing the user's activities are available.

As we intended a friendly fraud management interface, we decided to incorporate charts to it.

This makes the results interpretation easier especially that the signatures include different features whose values might be difficult to analyze and to explain without the support of graphs. Pie charts and histograms are used to describe the evolution of the user activities during the signature period of time. The charts we incorporated are based on the library (see http://www.highcharts.com/demo/ online).

IP addresses information can support the fraud detection operation. For a user who has a subscription with a given Internet provider, the IP addresses assigned to him should present some kind of correlation. As a consequence, looking for the IP addresses (and their frequency) used during the signature period of time is important as this can allow to find out some potential fraud indicators.

Additional information can be found in,
- SCAMSTOP deliverable D3.2
- SCAMSTOP deliverable D4.1
- Guide for the management interface (attached)

Coordination Level
The SCAMSTOP framework has a modular architecture where each module represents a fraud detection algorithm. This framework is designed in a way permitting incorporation of additional detection, correlation, analysis, and notification tools.

A legitimate question that might be raised is: how should these techniques be integrated together to provide a better detection rate. To answer to this question, we need to notice that launching the detection algorithms in parallel or in a sequence (one after the other) does not really make sense as there are algorithms that need to be scheduled over sufficiently large time intervals to be able to operate. The signature-based technique is a particular case of such algorithms. In contrast to this, a rule-based technique can be launched on demand. Indeed, the rule engine can be configured to apply a given rule on any new call (or CDR) that comes during the night to some suspected destinations. In addition to that, an alarm can be sent (in urgent cases) by email or by another means to the fraud management expert.

For these reasons, we decided to implement the SCAMSTOP framework in an event-based manner. This means the different components communicate by generating and receiving notifications. An event reflects the occurrence of an item of interest to some of the system components, for instance the arrival of a new CDR or the creation of a new rule. The event-based architecture is well suited for large scale distributed applications and provides easy integration of autonomous and heterogeneous components into a complex system.

The Event System builds a simple Star-topology with "a server" in the middle surrounded by clients (see SCAMSTOP_architecture_High_level.jpg). Each client talks only to the server. Clients can talk to each other, however, this is possible only through the server.

Our event system is based on XMPP. The latter refers to "Extensible Messaging and Presence Protocol", which is an open technology for real-time communication, powering a bunch of applications including instant messaging, presence, and voice and video calls. XMPP is open, standard, secure, extensible and flexible. In addition, XMPP is XML based and being

used by various companies in particular: Jabber, Google, Apple, Facebook, and Skype.

The Extensible Messaging and Presence Protocol provides the following features,

- XMPP Message: Request/Response (e.g. Server Push), Point-to-Point, Broadcast (e.g. Publish/Subscribe)
- Many extensions: XMPP over HTTP (XEP-0124), Service Discovery (XEP-0030), User Location (XEP-0080), Jingle (XEP-0166) .
- Many implementations:
 Server: jabber, ejabberd, apache vysper, openfire etc.
 Client: Jetsi, Empathy, iChat, JWChat etc.
 Libraries: Python (pyxmpp, xmppy), C++ (txmpp), Java (Smack), PHP (Jaxl)

In our implementation of the event system, we used the following libraries,
Client library:
- Python: xmpppy (see http://xmpppy.sourceforge.net/ online). This client is integrated to the web interface to inform the XMPP server that a new rule was created
- C: txmpp (see https://github.com/silas/txmpp online) . This client is integrated for instance to the CDRs database to inform the event system that a new CDR came in. It is also integrated to the Rule Engine to subscribe to the event system for notification about events such as "a new rule was created"

Server:
- jabberd2 (see http://codex.xiaoka.com/wiki/jabberd2:start online)

To inform the rule system about a new CDR or a new rule, the usual XMPP chat-frame was modified, such that every XMPP-frame sent contains a XMPP-type field containing one of the following:
- "rule_id"
- "cdr_id"
The Body of the frame will contain the individual id, either of the new rule or the new CDR. The rule system (initiated by its listening client) executes the following steps:
1. Evaluate the type field of the incoming XMPP message
2. a) If type is related to a new rule: apply the new rule to all CDR entries in the database or
b) If type is related to a new CDR: apply all "active" marked rules in the database to the CDRs

In order to avoid message communication overhead for every single new CDR, a single cdr_id is only sent to identify the last cdr_id of a collection of new CDRs. This means, if we inject a collection (imagine 38 million CDRs) of new CDRs at a point of time in the database, the XMPP client will not send 38 million single XMPP messages. After injecting the CDRs only one message is send, identifying the last CDR. The rule system that stores (and therefore knows) the cdr_id before the last injected one will start applying the active rules only to the new CDRs until the last received cdr_id (no computation overhead) in an increasing sequential CDR order. For this scheme it is necessary to auto-increment all the database cdr_ids.

Beyond this functionality, receiving XMPP messages and taking them as starting points for any execution makes it necessary to use a scheduler.

Imagine a realistic scenario with an execution time of 30 minutes (to apply a rule to all CDRs) where 4 new incoming rules shall be applied to the CDRs. Therefor a scheduler similar to the concept of a monitor from operating systems was implemented. The execution is handled as a job. Only one job is allowed to run at a time to have a consistent database. If 4 new rules are sent via the XMPP client, the required jobs to apply the rules are added to a queue for later execution. If a job has finished, the next job from the queue is executed.

Additional information can be found in,
- SCAMSTOP deliverable D3.2
- SCAMSTOP deliverable D4.1

Testing activities

One. Data used for testing

Real life data
For testing the different modules, both real and synthetized CDRs data were used. The real data reflects three months of CDRs (provided by VozTelecom) starting from the 1st of January 2011 to the end of March 2011. The data belongs to 4825 subscribers who generated almost 31 million of CDRs during these 3 months. The CDRs were provided within a tsv file which required the development of a parser module, using parallel processes, to parse the information in the file and store it in some SQL based "calls" tables within a reasonable period of time. After changing the CDRs data to a format we can use, we started analyzing it. The VoIP provider also offered a small set (17 cases) of compromised accounts with the corresponding activities. The major part of the fraudulent activities reflected suspected persons that (1) when using the VoIP service they exceeded a virtual threshold, (2) or called some unusual destinations.

The data was first analyzed and some preliminary discussions with the VoIP provider were triggered. The discussions were mainly to understand some aspects in the data that are related to the rate of successful calls and the rate of calls coming with the state (487: Request Terminated). Some details were provided in the deliverable D4.1.

What is also interesting is the fact that when analyzing the related activities, we noticed that 70% of the scam activities took place between 6:00 and 18:00, so during the day (morning and afternoon). This fact is "strange" due to the fact that usually fraudsters act during evenings and nights to escape detection when carrying out their activities. We also noticed that 57% of the fraudulent calls were made in the afternoon.

Synthetized data
In order to test the robustness of some of the antifraud algorithms, a tool has been used in order to generate synthesized CDR data. This tool uses as a basis SIPp tool that generates SIP calls. The tool has been extended in a way so that a profile can be loaded in order to generate calls and CDR from several users. In SCAMSTOP, these profile characteristics have been retrieved by analyzing CDRs from the VoIP providers. These characteristics are the following:
- PDF of Inter-arrival Time: Poisson, Pareto, Weibull, Gaussian distributions have been considered. By analyzing CDRs, it has been found that mean interarrival time during rush hours is shorter (08:00-16:00) than that of the rest of the day (00:01-07:59 & 16:01-12:00).

- Service Time follows exponential distribution.
- Probability Type of Outgoing Call: Outgoing Calls fall in the following categories: Local, National, Mobile, International (within European Union, USA, Other) Calls. Probability mass of function of outgoing calls towards specific destination (e.g. Asia) is smaller as compared to that of a Local/National Call.

By modifying either one of the following parameters, a fraud scenario can be defined:

- Increasing the number of calls within a certain period (either rush hour or rest of the day); interarrival time is decreased
- Probability of outgoing call towards a specific destination (e.g. USA, Asia) is increased.

Some screenshots of the extensions made to the SIPp tool were inserted in the deliverable D4.1. We also refer to the attached file (Screenshots of the extensions made to SIPp.pdf).

Two. Use case: How did we test the effectiveness of the signature based technique?
To check the efficiency of the developed algorithm, we used two samples to which we matched the results of the detection.

Known fraudulent cases
These are the 17 cases mentioned earlier and which the VoIP provider (VozTelecom) has offered.

Unknown fraudulent cases
Call centers activities can also be considered as a kind of fraud in case these activities do not
respect the subscription agreement. Unfortunately, VoIP providers do not have any mechanism to deal with such issue. This has pushed us to investigate how the unsupervised
techniques could be utilized to detect the related activities.

The first step in this direction was to define some heuristics to classify the provided data to potential call centers and non call centers. The heuristics we have used are related to the total number of calls and the success rate. One could also think about using other filtering criteria such as the number of calls made during nights and weekends. These numbers should be very small as call centers are also enterprises that are often not active during the mentioned periods of times. In fact, this is not always true as the VoIP providers might have business with other countries in other continents which requires from us to take into account the time offset between these countries. To summarize, the heuristics we used for classification are the following,

- The total number of calls made from a given account is greater than 100 per day and it happened at least 3 times during the 3 months
- The calls success rate is less than 60%

These criteria allowed us to generate a list of 119 potential call centers which represent 2.46% of the total numbers of accounts used in the tests. This sounds reasonable because the scam related data usually occupy a small portion of the entire data. This list was also reviewed by

the VoIP provider who confirmed the realisticness of the filtering criteria as well as the subscription accounts figuring on this list.

Performance and effectiveness

A general question that is frequently asked about unsupervised classifications techniques is how to assess the reasonableness of the obtained results and by which standards. One method to do this is to create a list of potential suspicious accounts and ask the VoIP provider to assess each of these accounts in terms of its functionality and the criteria used for filtering. For instance, some accounts are used by the VoIP provider to test the status of the network components, so one should expect a huge amount of calls generated by these accounts with a weak rate of call success as the provider is often interested in whether these components react or not, so no need to establish the calls. This behavior (huge number of call with weak success rate) is a typical call center behavior and the accounts for testing cannot be separated for the potential call centers without the help of the provider.

Unfortunately this method requires time and resources especially if the created list is long. In our work, we used this method as a first assessment and the results are presented in the previous section. Another method is to compare the signature based technique to other unsupervised or supervised methods. In this project, we also compared our work to the Neural Network Self Organizing Map (NN-SOM) technique discussed earlier.

The testing activities related to NN-SOM are based on a modified software provided by T.E.I. of Mesolonghi. This software is, in its turn, based on the Encog Neural Network Framework.

When applying NN-SOM to the unknown fraud cases, we noticed that 94 cases out of 119 were detected which means a detection rate of 79%. One can see that the signature based technique is performing better in detecting potential call centers accounts as the detection rate is 95% if we compare it with the 79% which is the rate obtained by NN-SOM. However, if we investigate deeper the results of both techniques, we find that 89 potential call center accounts (from 119) belong to both lists. In spite of the difference between the detection rates, one can note that almost 75% of the 119 potential call centers accounts were detected by both techniques. This rate is more than reasonable in the context of unsupervised techniques.

Three. Example of real life testbed: Integration with VozTelecom's infrastructure

The main objective of the testbed deployed in Voztelecom is to feed the SCAMSTOP framework modules with real life generated CDRs. This testbed is also be used to give feedback to the research partners about the usability of the framework and possible improvements that might need to be done to achieve a good integration with Voztelecom's platform.

To understand where has the SCAMSTOP framework been placed in Voztelecom's platform, we first have to know how Vozelecom does the accounting to their users. The diagram depicted in the attached file (Integration of the SCAMSTOP framework with VozTelecom platform.pdf) shows the elements that take part in that process of the CDRs generation:
- SIP Proxy: This is the core element in Voztelecom's platform. It routes all user's SIP signaling. The proxy sends a RADIUS accounting request to a RADIUS server for each one of the following SIP Messages:

Start: 200 and ACK
Stop: BYE
Failed: Error cause

- RADIUS server: This component stores proxies's accounting requests in plain text files. A new file is generated each day. Notice that in this file the duration of a call is not directly known, as for a single call we have 3 records (2 Starts and 1 Stop).
- CDR Parser: This is a program that reads the RADIUS text files and parses them to load all the records in a DB.
- CDR treat DB: This is a temporary DB where all accounting records for a call are merged in a single CDR. That CDR contains the duration of the call and might be treated to format the CDR with some custom parameters.
- CDR DB: This is the final DB where CDRs are stored.

To feed the SCAMSTOP DB with new CDRs there was the option to create a script that periodically dumped new CDRs from the "CDR DB" to text files, which could then be manually loaded using Wharf, but a more automatic procedure was chosen.

As Wharf commands have to be run manually and it's not possible to automate the whole detection process, a first approach to the real-life integration, is to create a process in the "CDR treat DB" so that when it has handled all the information to get one final CDR it feeds both the "CDR DB" and the "SCAMSTOP DB" with the needed information and the appropriate format.

The SCAMSTOP database and all the framework modules (detection modules, events, web server) have been installed in a dedicated server in Voztelecom's internal network.

The results obtained from applying the real-life traffic to 3 modules of the SCAMSTOP framework are described in the deliverable D4.1. The three chosen modules are the rule-based technique, the signature-based technique and the probabilistic approach. The results obtained from the modules correspond to a 2-month period data. The tests were performed for two different types of Voztelecom product users:
- Oigaa Office: Group of very homogeneous users, with few simultaneous calls, similar call patterns, and pre-provisioned devices with closed configurations (Hosted PBX service). For this group of users Voztelecom has not had many fraud attacks since it was launched.

- Oigaa Direct: Very heterogeneous users with different call patters, different simultaneous calls and with devices configured directly by clients (SIP trunking service). This group of users is the one that has suffered most of the attacks, mostly because of client's SIP agent misconfiguration.

The testing results are also included in the deliverable D4.1.

Additional information can be found in,
- SCAMSTOP deliverable D4.1

Potential Impact:

Strategic impact
The SCAMSTOP project resulted in the specification and the implementation of a Fraud Management Solution (FMS) for VoIP networks. The SCAMSTOP framework supports the following features:

- A rich management interface allowing alarms and results visualization, rules creation, and algorithms configuration
- Several detections techniques and algorithms
- An event-based system for correlating the activities of the detection modules

The SCAMSTOP project brought together a mixture of European SMEs including VoIP service providers, VoIP security solution providers, revenue assurance experts as well as reputable research organizations. First of all, the project contributes to the extension of the European knowledge in VoIP security. Second, SCAMSTOP enhances the portfolio of the fraud detection and revenue assurance solutions providers. Third, the outcome of the project benefits the involved SMEs in securing their infrastructures as well as protecting their revenues from fraudulent activities, which will lead to a sustained development of the European VoIP business. The combination of the development and validation of several classification techniques with a rich fraud management interface and an event based system for correlating the activities of the different detection algorithms resulted in a better understanding, so a better fight against scam activities.

The expected impact of this project can be summarized in the following points,
- The project brought together some of the stakeholder groups from industry and research institutions interested in the fraud problem at VoIP networks.
- The project also developed a strong and active networking with industry and research entities beyond the project consortium. This was achieved in the context of the dissemination activities
- The project supports the initiative of the EC where the SMEs get benefit from the R&D activities handled by research partners
- The SCAMSTOP project establishes a trust relationship between the VoIP providers and their customers as it protects the customers' accounts to be misused by fraudsters
- The development that was undertaken within SCAMSTOP will be directly usable by the VoIP providers (for instance VozTelecom and Telio)
- The concepts and mechanisms developed in SCAMSTOP will either be integrated in the products and services of the involved SME (PDMFC), or be used as a basis for a further solution that will be developed by this SME
- This project makes available several innovative techniques applicable to VoIP fraud detection
- The SCAMSTOP project also evaluates some of the traditionally used fraud detection methods
- SCAMSTOP provides risk analysis methodology of the VoIP providers' networks using ISO

Economic and social impact
One of the major promises of the VoIP technologies in general and SIP in particular is that it will support a wide range of communication services such as telephony, messaging, video conferencing and many more at a lower

cost than today's PSTN services. In such an environment of mass deployment large manufacturers will have better chances of providing low cost VoIP components such as IP-Phones, gateways and media servers. For SMEs to succeed in this market they will need to provide customized solutions based on cutting edge technologies. Regarding security, VoIP service providers will require customized solutions that are adaptable to their exact needs and business models, policies and supported services. With the results of SCAMSTOP, the involved SMEs received knowledge and tools that enable them to provide / deploy such customized security solutions allowing them to extend and enhance their service offers. To be more concrete, SCAMSTOP will contribute to a substantial increase in the revenue. With the extension of its service assurance product (RAID), PDMFC expects a substantial increase of the attractiveness of its product that would allow a higher price and more sales. Based on rough discussions with potential customers this increase is currently estimated at 20%. Based on a 2011 recently published Fraud Loss Survey, the Communication Fraud Control Association (CFCA) reports that telecom fraud costs businesses more than $40 Billion every year. By deploying SCAMSTOP, Telio estimates that 40% of the lost revenue might be regained. This would increase its profitability by a value ranging between 2% and 6%. By integrating anti-fraud mechanisms in its application platform VozTelecom aims at increasing the trust of its customers in its products and hence help it to increase its sales and acquire more customers. Based on discussions with current customers as well as sales activities it is estimated that the revenue could be increased by 10%.

By deploying such fraud management systems, it is also expected that a trustworthy relationship between the VoIP providers and their customers will be established. The detection algorithms can deal with both subscription and superimposed fraud categories. This will prevent and also reduce the time where a legitimate account is compromised by a fraudster and the owner of the account has to pay for calls that he did not make.

Dissemination activities
For SCAMSTOP dissemination, we have dealt with the following,

Public deliverables
Some public deliverables were uploaded on the SCAMSTOP Web portal (see http://www.sme-SCAMSTOP.eu/ online).

Fair events
We attended the Telecoms Fraud and Risk Management conference, 05 - 08 December, 2011, Sheraton Park Lane, Piccadilly, London. In such conferences, one can meet operators, VoIP providers and enterprises that can be interested in the SCAMSTOP Fraud Management Framework. In addition to that, SCAMSTOP flyers were distributed in this conference.

Industry talks
- -Yacine Rebahi. Key speaker at The 4th Annual Telecoms Fraud and Fraud Risk Prevention, December 2010, Malaysia
- Yacine Rebahi. Key speaker at the Telecoms Fraud and risk management, December 2011, UK

Industry contacts

The following contacts were made to promote the work achieved within SCAMSTOP,

1. Technological Educational Institute of Serres, Terma Magnisias, Serres, Greece university. Mr Costas Hilas has a strong and long experience in data mining and fraud detection. He was contacted to exchange ideas and seek for future collaboration

2. Orange-labs, France. The department dealing with R&D in the security area was contacted to promote SCAMSTOP and look for future collaboration

3. CGI. CGI does have a large focus in telecommunications as well, and the SAS Fraud Framework does have a telecommunications component. Their fraud practice is mostly financial focused, but they are looking to grow into the telecom area. A first contact was made to look for potential collaboration
4. T-online. Deutsche Telekom is the biggest operator in Germany. They currently run a fraud management project in Bonn. A first contact was made to look for potential collaboration
5. Hugin. HUGIN is a company from Denmark currently focusing on fraud detection in the insurance industry. Their solution is based on Bayesian Networks. A first contact was made as they are interested in exploring new areas in particular the telecom one
6. Trifense. Trifense is a german company with a strong expertise in the area of machine learning (supervised and unsupervised) with particular focus on efficient sequential data analysis applied to network security problems. They are interested in the project for future potential collaboration
7. Xintec. Xintec is a fraud management company located in Luxemburg (see http://www.xintec.com/ online). They are interested in the project results for potential collaboration
8. Kabel Deutschland. Kabel Deutschland is a big german cable operator. They have already a solution for fraud detection and revenue assurance, however, they are also interested in the results of the SCAMSTOP project for potential extensions.
9. Trading-bull. Trading bull is a small VoIP provider located in UK, currently suffering from fraud activities that are harming their business. They have contacted Fraunhofer Fokus because they see in the SCAMSTOP results a potential solution for stopping the fraudsters' activities
10. ViVa (see http://www.viva.gr online): A Greek VoIP provider that provided CDRs used to create synthetic CDRs from the SIPp tool

Publications

The following papers have been published/presented,

- Y. Rebahi, R. Ruppelt, M. Nassar, O. Festor, "SCAMSTOP: A Platform for Mitigating Fraud in VoIP Environments", Book Chapter to appear in the "Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications", Publisher: IGI Global
- Y. Rebahi, M. Nassar, T. Magedanz, O. Festor, "A Survey on Fraud and Services Misuse in Voice Over IP (VoIP) Networks", In the Information Security Technical Report (ISTR) journal, Vol. 16, No. 1. (February 2011), pp. 12-19. doi:10.1016/j.istr.2010.10.012 Key: citeulike:9776454
- T. Kapourniotis, G. Polyzos, T. Dagiuklas, P. Alegragkis, "Scam and Fraud Detection in VoIP Networks: Analysis and Countermeasures using User Profiling", 50th FITCE Congress, Palermo, Italy, August 2011
- Y. Rebahi, "SCAMSTOP FMS: A Fraud Management System for VoIP Networks", Flyer describing some parts of the SCAMSTOP project and distributed at the Telecoms Fraud and risk management conference, December 2011, UK

The following paper was submitted to SIGCOMM 2012:
- Y. Rebahi, T. Q. Tran, "A Signature based Technique for Fraud Detection in VoIP Networks".

The following paper was submitted to IEEE GLOBECOM 2012:
- P. Galiotos, T. Dagiuklas, T. Kapourniotis, "Non conforming behavior detection in VoIP Based Networks"

Results Exploitation

VozTelecom
VozTelecom offers VoIP solutions to different markets:
- End user market: Addressing mainly Spanish business and residential market with VozTelecom brand and two different products, Oigaa (a hosted IP PBX for the SME market) and Oigaa Direct (a SIP trunk to be configured in existing PBX/ SIP Devices).
- Wholesale market: VozTelecom offers to small and medium service providers a complete VoIP solution, that integrates all the necessary items a service provider needs to deliver and advanced VoIP service to its end users: From the pre-defined end user products to the provisioning, logistics and service management solutions. VozTelecom addresses this market with the VozIP.com solution. VozIP.com solution is marketed in two different ways: As an ASP solution (the service provider rents "capacity" in VozTelecom central platform) or in a license mode, where the customer buys all the equipment and software necessary to run a 100% standalone VoIP platform based on VozTelecom's VozIP.com solution.

Direct Marketable Results Expected from SCAMSTOP Project
The main business results VozTelecom will get from the SCAMSTOP project are,

VoIP security knowledge: As a player in VoIP market, it is key for VozTelecom to have a team specialized with a high level of VoIP security knowledge. This will help VozTelecom in finding the main issues that have to be addressed in order to offer a secure service to its own end users, and provide a reliable solution to its wholesale customers. This knowledge will be materialized with a network reference model, a set of rules and patterns that will help to create a standardized reference model that will be very useful to be shared with the wholesale partners.

Increase Oigaa and Oigaa direct features: With the inclusion of the anti-fraud system in VozTelecom's core platform the number of fraud cases, as well as their impact, will be reduced. That will not only have effect on the money that both the end-user and VozTelecom will save thanks to decreasing the number of frauds, but also to the security perception of the service.

Increase VozTelecom ASP features: VozTelecom will add a module in its current ASP solution offer to use an anti-fraud system. Thanks to this new module, VozTelecom will be able to increase ASP solution features: This will increase VozTelecom ASP Solution differentiation adding a key element -an anti-fraud solution- for a service provider. It is important to mention that none of the current VozTelecom competitors have any kind of SIP anti-fraud related module included in their current offer.

As an additional module in VozIP.com solution: When VozTelecom sells the entire platform to a service provider, the service provider is able to choose between different modules to be installed, from billing services to web based provisioning or stock control. Thanks to SCAMSTOP project, VozTelecom will add an additional module to its current offer.

Direct Revenues Expected from Project Results
VoIP anti-fraud knowledge: This knowledge is not expected to provide VozTelecom with any specific additional amount of new customers (end users or wholesale), but will help VozTelecom to provide a better

service, and in fact will, in an indirect way, increase VozTelecom business opportunities.

Increase Oigaa and Oigaa direct features: A VoIP platform that includes an anti-fraud system may be an important point for those customers who see VoIP as an insecure technology. That is a plus for undecided users that think about transitioning to VoIP. But the main priority for VozTelecom in including is to reduce the number of attacks received by current users.

Increase VozTelecom ASP features: Right now, service providers are buying SIP platforms without any special anti-fraud module: This means that SIP related anti-fraud measures are an important issue but do not prevent a service provider from launching or selling a VoIP service. Based on this assumption, as a marketing strategy, VozTelecom will not increase its current ASP solution price based on the addition of the anti-fraud related module, but on the other side these modules will increase VozTelecom selling exit, by approx. a 10%: For each 10 ASP solution sold to a service provider, 1 of them will be sold thanks to the anti-fraud module inclusion.

As an additional module in VozIP.com solution: Right now there is no specific SIP related anti-fraud module in the market, so it makes it quite difficult to define a price for this module. The costs associated with setting up a complete VoIP solution in a service provider are quite high: The costs are not only related to the technical platform, the biggest costs are related with the marketing and commercial area. This means that the module cost will be considered not as a standalone price, but as just a part of a whole new product launch costs. This will make the customer less conscious about the module price, as long as the whole new product creation costs are affordable and provides the customer with a reasonable investment return. VozTelecom is sure that this will be a key element in its current VozIP.com solution, and will be sold to approx. 90% of the current and future VozIP.com customers.

Communication Strategy
Apart from the efforts that will be made inside the SCAMSTOP project to promote the project results, VozTelecom will do an additional effort to make public the SCAMSTOP project results.

This commercial strategy will be done in several ways:
- Adding the SIP anti-fraud module info to VozTelecom current commercial offer.
- Explaining SIP fraud related issues in the conferences where VozTelecom is invited as a relevant market player.
- Explaining SIP fraud related issues in the technical articles VozTelecom publishes in specialized reviews.

Competitors
There are of course, competitors for a VoIP security solutions, mainly session border controllers that some medium or big service providers launching VoIP solutions can add to increase security. SCAMSTOP will not directly compete with this kind of solutions because it is focused to medium-low sized service providers. In this kind of customers the relationship between security investment / number of lines is more complicated. In this kind of customers, a whole solution including hosted VoIP service with security would fit better than a complete hardware based VoIP solution. There is right now no competitor in Spain offering a

hosted VoIP solution, so we should look at the European market to find competitors to a complete hosted VoIP solution.

Roadmap
The implementation steps of the SCAMSTOP architecture in Voztelecom's products and platforms are expected to be as described below:

Phase 1 - Lab testing
- Early 2011
- The SCAMSTOP architecture will be tested in a well-known lab environment.
- This phase started to be executed at the time it was planned but it was also carried on while the next phase took place.

Phase 2 - First real-life testing
- Mid 2011
- The SCAMSTOP architecture will be evaluated for the first time with real-life traffic.
- In this phase the architecture and modules have been tested and the result was satisfying. Taking into account that the architecture is still a prototype it presents a great potential.
Phase 3 - Implement in minor ASPs and VozTelecom products
- Mid 2012
- The SCAMSTOP architecture will be installed in VozTelecom's platform and will be in use for minor ASPs and for less-critical VozTelecom products.
Phase 4 – Fully integration of the SCAMSTOP architecture
- Late 2012
- The SCAMSTOP architecture will be fully integrated in VozTelecom's platform to extend the anti-fraud capabilities to all products and ASPs.
- The full adoption of the SCAMSTOP architecture should not be delayed much from the previous phase, as once the SCAMSTOP architecture is integrated in VozTelecom's platform it's very simple to feed the framework with the rest of CDRs.

Telio

Product description
Telio was one of the early providers located in Norway, and they pride themselves of having the skills and innovation to be the best in the market, not only in Norway but on world basis as well. This is proven with the ties and resources they have by attaining VoIP pioneers as advisors. With this successful track record in mind, Telio has the opportunity to develop unique solutions and create new ideas, and this is where the SCAMSTOP project comes into play. With the collaboration of all the SCAMSTOP partners and collected intellect, we have the chance to be on the forefront in the VoIP industry, not only technology-wise, but also security-wise.

The SCAMSTOP project has delivered a solution for the participating SMEs to detect and prevent fraudulent VoIP calls. Telio is forking into two directions; landline replacement and mobile VoIP, hence all references to SCAMSTOP and Telio will include this consideration.

As VoIP is continuously evolving, and high speed Internet connections are becoming ubiquitous, we can already observe consumers' migration towards mobile Voice and Video over IP. How Telio is preparing the preventative

fraud measures is described in the section "SCAMSTOP and the Telio platform".

Other competitors
The top contenders are Telio and Telenor. NextGentel is number three.

Implications or risk factors
As with all intrusion prevention and detection systems, there is a chance of false negatives and false positives. In this context, a false negative is a fraudulent attack, which is not detected, and a false positive is an authentic call passed as a fraudulent one. While the false negative is annoying, and can quickly become very expensive for the provider, there should already be other measures in place, which would stop most of these attempts. A false positive is perhaps more troublesome for the provider – especially if it passes unnoticed. They cause discontent among the users, and, if they happen often enough, cause major service disruptions. For these reasons, in the SCAMSTOP project, we do not have automatic reaction in case a certain activity is suspected (for instance, dropping an ongoing call). In fact, when a potential misbehavior is detected, and alarm is sent requesting deeper investigation.

Roadmap
Below phase iteration aims to illustrate the future phases where Telio believes SCAMSTOP will have its major impact. While voice and video will always be the primary services, Telio is constantly exploring new ways of communicating, emphasizing the importance of SCAMSTOP being a flexible framework.

Phase 1 – First half of 2011 – Lab testing
- Evaluating the SCAMSTOP architecture in a lab environment.
Phase 2 – Second half of 2011 – Trial implement
- Evaluate the SCAMSTOP architecture in a life environment.
Phase 3 – After-project – Integration in existing Telio platform
- Deploy the SCAMSTOP architecture by integrating it into Telio's overall value-chain.

SCAMSTOP and the Telio Platform
The technology and knowledge of the SCAMSTOP project will help Telio to effectively manage the fraud threat. This will provide us with an important advantage over competing VoIP providers. As the discussion above has shown, voice and video on the net is on a steady move from early adopters towards the mainstream. Unreliable fraud detection and prevention systems can seriously threaten this move by turning the new technology into a nuisance, stressing the importance of transparency and reliability of the architecture. As the end user does not care about economical fraud against their provider, the system needs to be ubiquitous, and provide the user with a service level indistinguishable from what they already had. The tech savy and early adopters may forgive the odd false positive – for a main stream user, a call incorrectly classified as fraudulent, and therefore dropped, is a reason to complain.

The move from fixed VoIP to video and mobile VoIP and FMC will increase the likelihood of attempted fraud, due to the more chaotic and unknown network scenarios.

While the SCAMSTOP project was going on, there was also a project within Telio to rework the chain for generation of CDRs. This new platform

neatly coincides with SCAMSTOP since the results of the project can be more easily integrated with Telio's call accounting and billing platform. SCAMSTOP will thus be part of this new platform and will be subsequently rolled out in all markets.

PDMFC
Revenue Assurance Integrity Driller
PDMFC has a large experience in developing carrier grade solutions to worldwide leading operators, especially in the area of Revenue Assurance, where it has deployed in production, in partnership with WeDo Technologies, more than 30 licenses of its Revenue Assurance Integrity Driller (RAID) software.

PDMFC expects to fully exploit the results of the project by incorporating all new developments into its most promising product, namely, the revenue assurance integrity driller. We expect our current product line to greatly benefit from the solid mathematical foundations in which the development will take place and the extensive testing and evaluation that will be followed. Since through the partnership with WeDo Technologies, PDMFC has direct connection to almost all leading mobile operators in the world and expects to showcase the versions of their products enhanced with SCAMSTOP technology in trade shows and industry gatherings. This new anti-fraud additions will lead to either product upgrade by their customers, new purchases from current and future customers and additional services (support contract extensions).

Currently WeDo is testing anti-fraud solutions in over twenty different mobile carriers and it is expected to obtain positive results during the first semester of 2012 and deploy a full-scale solution in the second semester of 2012.

Consultancy Services
PDMFC plans also to provide consultancy services to a number of telecom companies (e.g., PT (the Portuguese PPT), Optimus, VODAFONE) as well as to several government agencies (e.g. Ministry of Defense, Ministry of Justice, Ministry of Education, etc.) in Portugal. All these agencies have a large and complex VoIP infrastructure deployed (partially with the technical help from PDMFC). These services include authentication infrastructures (e.g., PKI and strong authentication), infrastructure & perimeter security (e.g., SOHO security and intrusion detection) vulnerability assessment (e.g., penetration and stress testing) digital data and communications protection (e.g., fixed / mobile data security and document signing) information security certification and legal compliance (e.g., ISO27001, digital signature law), secure applications (e.g., e-voting and monitoring/tracking) secure system design and implementation and software development.

Cross industry fraud detection
PDMFC is currently active in several industries in which fraud is a major issue. Those include Banking, Insurance, Telecommunications, Retail. and Online Gaming.

PDMFC is actively testing some of the algorithms developed in SCAMSTOP in multiple scopes. The short term goal is to create a propriety repository of tuples {algorithm, fraud detection result} which will allow to position PDMFC as strategic consultant to multiple industries in the area of fraud prevention and detection.

Preliminary results have already been achieved in the area of telecommunications (both VoIP an non-VoIP) and in the area of banking.

One of the main medium term investments is in the area of massive online gaming where fraud detection is a major problem to tackle. PDMFC is now in the process of trying several variants of the algorithms developed in SCAMSTOP (meaning they are using the underlying concepts but applied in completely different datasets).

List of Websites:

http://www.sme-SCAMSTOP.eu/