Project Number	AC095
Project Title	ASPeCT: Advanced Security for Personal Communications Technologies
Deliverable Type	Intermediate
Security Class	Public

Deliverable Number	D18
Title of Deliverable	**Fraud Detection Concepts: Final Report**
Nature of the Deliverable	Report
Document reference	AC095/VOD/W22/DS/P/18/1
Contributing WPs	WP2.2, WP2.6
Contractual Date of Delivery	November 1997 (Y03M09)
Actual Date of Delivery	January1998 (Y03M11)
Editor	Phil Gosset

Abstract	This report contains further analysis of the three different approaches considered for Fraud Detection, namely Rule Based, and both Supervised and Unsupervised Neural Networks. It presents a single combined tool, BRUTUS, which is considered to use the best parts of the three approaches, and then defines a prototype which can be achieved within the project's lifetime. In addition, further analysis of displayed results against legal and practical needs is provided.

Keywords	ACTS, ASPeCT, UMTS, Fraud Detection, Rule Based, Neural Networks, Supervised, Unsupervised, BRUTUS, Legal

1 Contents

2 Executive Summary

This document contains further analysis of the three different ASPeCT Fraud Detection Systems. After describing the concepts (D06 [5]), the first implementation (D08 [6]), and an evaluation of the tools (D13 [7]), this report aims to present the details required for the trials. In addition, the preliminary results of early studies into the legal aspects of fraud detection are presented here.

Since the evaluation of the three prototypes, the work has focused on developing a single efficient tool which would utilise the best parts of the three approaches. The results of this study are presented here as the combined tool, BRUTUS.

The basic philosophy of BRUTUS is to maximise the available information. This is achieved by using the Unsupervised Neural Network to generate information about the change in behaviour of the user, which can clearly be a good indicator of fraud. However, it is only an indicator and the tool must use additional information to determine if indeed a fraud has occurred. In the same way, a B-number analysis tool is used to generate geographical information to be used as another indicator.

This information is then forwarded to a Neural Network (NN), which uses a fuzzy rule interface to detect fraudulent behaviour. Finally, this information would be collated by an intelligent monitoring tool which receives alarms from the NN, and distributes them to the relevant destination.

However, time limitations mean that it is not possible to implement a tool with the above functionality. Instead, an achievable prototype will be implemented which will allow many of the assumptions made as part of BRUTUS to be tested. This prototype will again use the Unsupervised Neural Network and B-number analysis tool to generate additional information for detecting fraudulent behaviour, but will pass this information to the Supervised Neural Network for initial analysis. This will then raise any further indications of fraud that it detects, and pass all of this information on to the Rule Based tool. Once this has processed all the data, a simple monitoring tool will store and display any raised alarms.

This prototype shall be used within the trials, the planning of which is also presented within this document.

Finally, there is a preliminary report on the legal aspects of Fraud Detection. This chapter outlines the approach adopted and also scopes the work.

3 Document Control

3.1 Document History

This is the first issue of D18.

3.2 Changes Forecast

No changes to this document are currently intended; subsequent developments are planned to be included in deliverable D19.

3.3 Change Control

In conformance with the project Quality Plan [1].

4 Document Cross References

[1] ASPeCT Quality Plan .

[2] Project Technical Annex (Year 2 Form M4DD).

[3] ACTS AC095, project ASPeCT, “Initial report on security requirements”, AC095/ATEA/W21/DS/P/02/B.

[4] ACTS AC095, project ASPeCT, “Project Trial Plan”, AC095/PFN/W12/DS/P/017/C.

[5] ACTS AC095, project ASPeCT, “Definition of Fraud Detection Concepts”, AC095/KUL/W22/DS/P/06

[6] ACTS AC095, project ASPeCT, “Fraud Management tools: First Prototype.”, AC095/DOC/RHUL/072/WP22/A

[7] ACTS AC095, project ASPeCT, “Fraud Management tools: Evaluation Report.”, AC095/SAG/W22/DS/P/13/2

5 Abbreviations and Glossary of Terms

ASPeCT	Advanced Security for Personal Communications Technologies
AU	Analysing Unit
AUA	Absolute Usage Analyser
CU	Controlling Unit
CUP	Current User Profile
DUA	Differential Usage Analyser
EIR	Equipment Identification Register
GUI	Graphical User Interface
GSM	Global System for Mobile Communications
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
MA	Master Analyser
MSC	Mobile Services Switching Centre
MSISDN	Mobile Station Integrated Services Digital Network
PABX	Private Automatic Branch Exchange
PDAL	Protocol Data Analysis Language
PDAT	Protocol Data Analysis Tool
PSTN	Public Switching Telephone Network
PVM	Parallel Virtual Machines
ROC	Receiver Operating Characteristic
RCF	Roaming Call Forward
SALR	Supervised NN Alarm
SALV	Supervised NN Alarm level
SIM	Subscriber Identity Module
SP	Service Provider
TACS	Total Access Communications System
TBZC	Toll Ticket B-number Zone Code
TMN	Telecommunications Management Network
TSDN	Toll Ticket Starting Date Normalised
TSTS	Toll Ticket Starting Time in Seconds
TT	Toll Ticket
UMTS	Universal Mobile Telecommunications System
UPR	User Profile Record
UPH	User Profile History

6 Introduction

6.1 Overview of D18

This document contains further analysis of the three different ASPeCT Fraud Detection Systems, and preliminary work on both the Fraud tool trials and the legal aspects of fraud detection.

A short overview of the following chapters is given here:

7. BRUTUS

This chapter discusses the current state of the tools, and proposes a single tool called BRUTUS which combines the three different techniques. However, the complete integrated tool is not achievable within the timescales available, so an achievable prototype is presented, which will be subjected to a trial using near-real-time data.

8. B-Number analysis tool

This chapter describes the B-Number analysis tool which is an important part of BRUTUS and will be available within the achievable prototype.

9. Trial and Demo

This chapter outlines the mechanisms, plans and requirements of the trial. It includes a workplan for the trial and describes the environment within which the trials shall be conducted.

10. Legal Aspects

This chapter presents the issues relevant to fraud detection, and scopes the remainder of Work Package 2.6.

Background to deliverable

This document comes after the initial description of the concepts (D06 [5]), the first implementation of the tools (D08 [6]), and their evaluation (D13 [7]). After these documents, a reassessment of the potential of the three approaches was required, so that the optimum configuration of the tool(s) could be determined for the trial.

In addition to this work, the preliminary work on the legal aspects of Fraud Detection has been done, and is included here.

7 BRUTUS

7.1 Introduction

Since the three different fraud detection approaches have shown their own strengths and proven their usability, an integration of all three approaches to one hybrid fraud detection system is a natural progression. This way, the tools can take advantage of useful, additional information like other user profile data as well as interim results of the other tools.

Concepts for a far reaching low-level integration of all tools to a generalised system BRUTUS have been introduced. However, a fully integrated and generalised system quite close to a product is clearly outside of the scope of ASPeCT.

Nevertheless we are convinced that a high-level integration of our different approaches is worth the effort and a main step to the ideal goal BRUTUS. In the following sections an achievable integrated prototype is introduced based on an evaluation of the current code status.

7.2 Evaluation of current code status

This section reflects the current code status and describes desired features of an achievable prototype.

Although all tools have proved to be very stable even during public demonstrations, they are still prototypes. Some hidden errors might appear upon combining the tools. A careful integration and comprehensive testing is the precondition for a stable hybrid system.

Currently, all tools are running on different machines with different UNIX versions. The software has been written according to XPG-standards to guarantee software portability. This also guarantees the reusability of code used by all tools such as the communication functions. On the way towards an integrated system all software might be ported to Sun-Solaris.

Precondition for an integration is a similar run-time performance of all different tools. Due to the fact that all tools use the same DB as well as the same number of TT-components it is not too surprising that all tools offer a similar performance of around 30 TTs per second and thus fulfil this requirement

In the following we describe some steps towards BRUTUS and to what extent they are realistic to be realised:

- All tools are using the same data base implementation which is GDBM, a simple and fast data base on UNIX. This data base fulfils the needs of user profiling, where the data records are always accessed via the IMSI as the only key. Within the first prototype the monitoring tool simply used a set of files for storing monitored users and the calls made by them. This may be retained initially for the hybrid system. For BRUTUS an advanced relational data base would be desirable for an efficient monitoring tool-set, which includes, say, presenting graphs as additional information.
- Prior to the integration each tool was embedded in a common ‘real’ environment comprising a mediation device simulator feeding the tools with toll tickets and a monitoring tool to collect suspicious IMSIs and the corresponding call data. This environment will be kept for the hybrid tool. The simple Shell- and Pearl-scripts organising the inter-process communication via pipes have shown weaknesses in fault cases (e.g. crash of any tool). More flexible routines written in C, which enable a better error handling for the communication are desirable. For BRUTUS a comprehensive fault recovery would be necessary.
- In order not to get too many dependencies between the tools during integration, we have decided to develop on different machines connected via a LAN. A single data flow through all fraud detection tools is built upon TCP/IP sockets. A tagging scheme allows the type and origin of any information passed to be distinguished. In this way the tools can be kept independent to a certain extent. They are also free to use information produced by other tools, although no tool will strictly rely on the information of any other tool. The BRUTUS goal of course would be one fraud detection system on a single machine.

- An additional reason for not combining all tools on one machine is run time performance: All tools use their own data bases for realising their specific user profiling. BRUTUS would have a unified user profiling.
- The hybrid fraud detection system will come with one common GUI to display the alarms. This GUI has mainly been finalised as part of the monitoring tool. In addition, some basic administration features are welcome enhancements. One of these features should be control bars for each contributing tool to adjust their respective alarm thresholds. This way the tools are adjustable against each other during runtime and we can easily specify to what extend each tool contributes to the common result.
  A detailed administration via one unique GUI, however, as desired for BRUTUS is clearly out of the scope of the integrated prototype developed within ASPeCT.

7.3 Common ideas and integration

When carefully analysing the three separate tools, we can see that some common ideas are present. First of all, in all three tools fraud detection is based on an intensely data-driven user-by-user profiling. Secondly, fraud is associated with changes in behaviour and, assuming that the profiling is consistently reflecting the behaviour, also with changes in profile. These changes are detected with sophisticated artificial intelligence techniques. Thirdly, the tools are to be used in an interactive way. A higher level monitoring tool manages the exchange and representation of the information and for example also sets certain tuning parameters in the fraud detection tools for customising the fraud detection sensitivity. A fourth common feature is the fast hardware environment implementation of the tools.

These common ideas motivate the integration of the separate approaches into what we would call a generalised monitoring system. A data flow chart for such a proposed system is given in Figure 7-2.

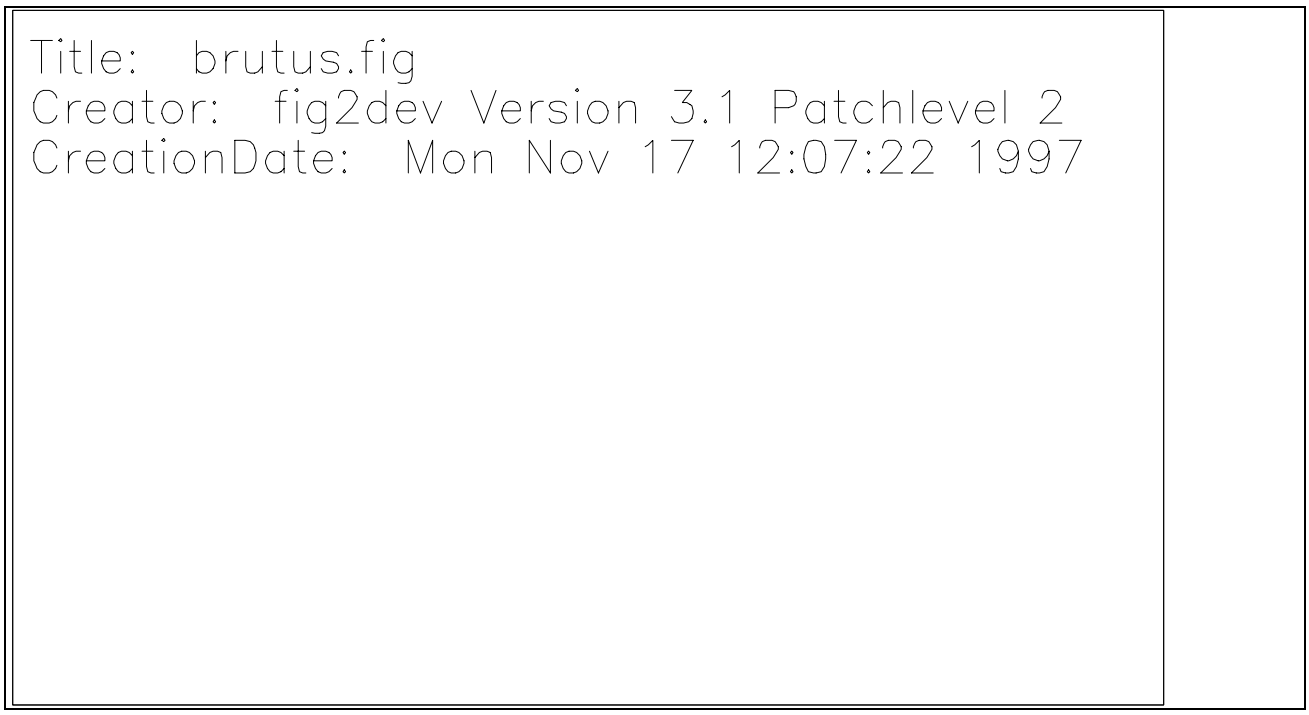

Figure 7-1- BRUTUS, Data Flow Chart

Initially, raw data from the network is pre-processed, discarding irrelevant components, and retaining useful data fields encoded in a suitable format. Secondly, the already present information on the user (i.e. the user's profile) is retrieved from the database. From the profile and the incoming data, relevant observables are derived. With these observables, we perform the following actions:

- The profile is updated and stored in the database for later re-use.

- An audit trail is maintained.
- The artificial intelligence component performs the fraud detection and generates a report on the alarm status of that user.

This report is then handled by the intelligent monitoring tool, which serves as a (graphical) interface to the human operator. Possible tasks of the monitoring tool would be:

- Filter the types of alarm that the operator wishes to handle.
- Generate operator customised data and alarm level presentation for visual inspection.
- Set tuning parameters in the detection tools.

7.4 Achievable prototype

As an achievable prototype a serial integration of the already present tools is proposed, as depicted in Figure 7-2.

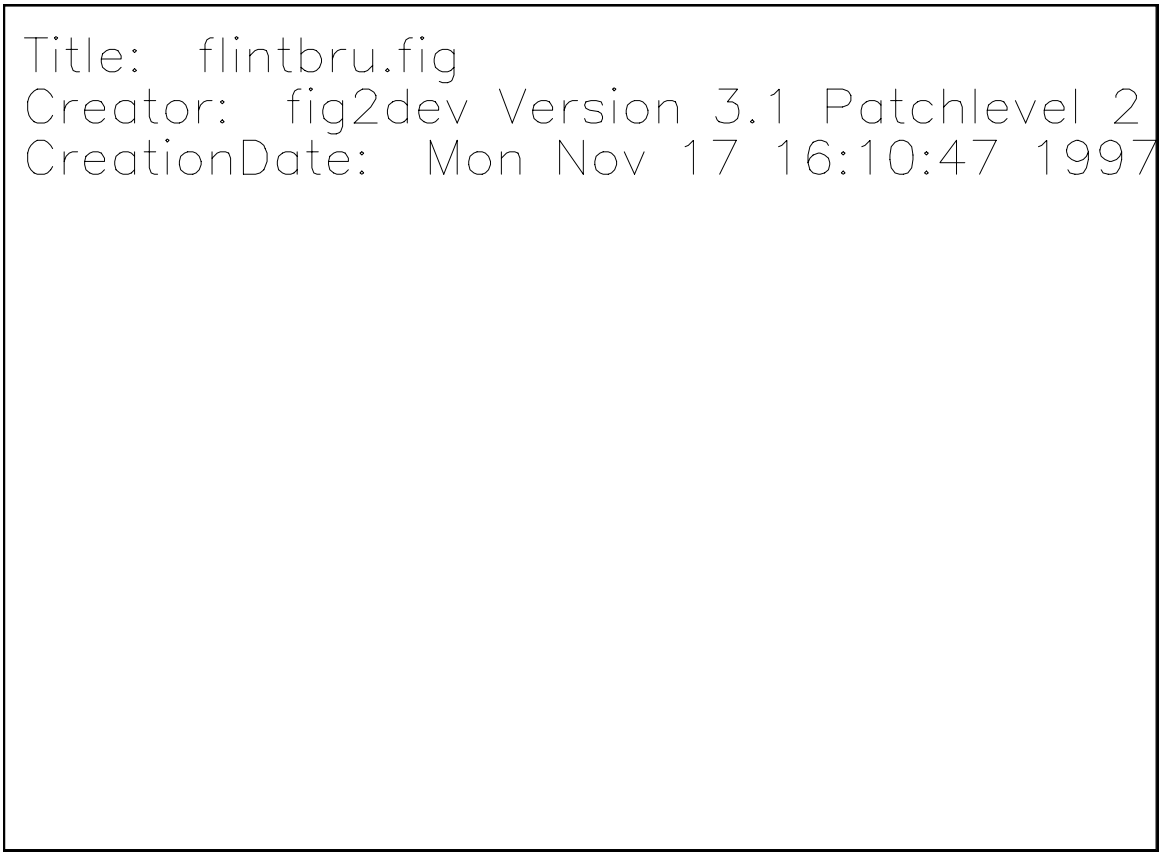

Figure 7-2 - BRUTUS, Proposed Prototype

Raw data consists of TT's entering the prototype. The preprocessing block selects data fields and puts them into a format easily manageable by software. Each 'detection module' in the subsequent chain then extracts and uses the data of its choice from the general data-stream. Then the module adds its findings/results to the data stream while leaving the original data unchanged. The next module can then select from this augmented data-stream, the relevant information that it wishes to use in its own fraud detection. This means that subsequent fraud detection modules can use the profiling and/or the results of the preceding module. In a first implementation, where the work will be distributed over different computer platforms, each detection module will keep its own database.

7.5 Ordering

The ordering of the fraud detection tools as it is depicted in Figure 7-2, is motivated by the following considerations:

- The B-number analysis is added because it is believed that adding information on the destination of the calls, will be able to boost the already reported performance of the individual tools. This module comes first because it adds information to the data-stream that every module could easily integrate by all three tools.
- The Unsupervised NN is very good for novelty detection. It has good negative predictive value, which means that it can eliminate those users very easily for which certainly nothing is happening. Therefore it could be used as a first filter to all incoming calls. Another reason for putting this module high up in the chain is that its profiling could possibly also be used as input to the Supervised NN.
- The Supervised NN can efficiently pinpoint users whose behaviour is similar to previously observed and recorded fraudulent behaviour. Its training routines can be tuned to bias the performance towards a high positive predictive value, i.e. when it puts a fraudulent label on a user, the subsequent modules and/or human operator can be confident that there really is something happening.
- The Rule Based system does very well in explaining why alarms have been raised. It could for example be extended with extra rules to inspect why previous modules had raised an alarm. In this fashion, new fraud scenarios can possibly be identified. It can also be used to define hyper rules based on alarms raised by other tools and not only on its own profiling/information.

7.6 Intermodule communication

Individual modules forward information that they receive from any other module and add tagged information of their own should it be required. The data is fully human-understandable at all times. It is structured as a sequence of tag/value elements.

- Tags are four-printable-symbol strings.
- Values are arbitrarily long printable-symbol strings.
- The size of a Tag label should be fixed.
- Blank spaces are used to separate tags and values.

The input behaviour of each tool is the following. When it reads a string, the tool scans it for the tag of the fields it wants to use and extracts the corresponding values, overlooking the tag/value pairs it does not use for its own processing. The first six elements (twelve fields) correspond to the six toll ticket fields used in the first demonstrator. The output behaviour is the following. The tool copies the string it received at its input directly to its output, and adds tag-value pairs for all the information it wants to output (for example, for use by the monitoring tool). Writing to standard output should only happen at one place in the code, so that the structure of output can be updated easily.

Example:

The output of the Toll Ticket simulator might look as follows.

```
  TMSI F23415124546303b2d224c63 TCSD 19960716 TCST 220038 TCDR 000693
TBNB

  FFFFFFFFFFFFFF30198672b641014 TBTP 01 TSDN 0016 TSTS 079238 TBZC 03

  TMSI F23415124546303b2d224c63 TCSD 19960716 TCST 221856 TCDR 000031
TBNB

  FFFFFFFFFFFFF017433333d571a4f TBTP 00 TSDN 0016 TSTS 080336 TBZC 00

  TMSI F23415124546303b2d224c63 TCSD 19960716 TCST 222015 TCDR 000367
TBNB
```

```
  FFFFFFFFFFFFF017433333d571a4f TBTP 00 TSDN 0016 TSTS 080415 TBZC 00
  TMSI F23415140807624d312f4b4c TCSD 19960716 TCST 224913 TCDR 000003
TBNB
  FFFFFFFFFFFFFFFFFFF4646250c79 TBTP 00 TSDN 0016 TSTS 082153 TBZC 00
```

This output is sent to the fraud detection tool. But the tool might not need all these fields. Let us say that instead of using the B-type, it prefers to use the zone code TBZC (Toll Ticket B-number Zone Code) that gives the region of the world the call was made to. And it does not use the TSDN (Toll Ticket Starting Date Normalised) and TSTS (Toll Ticket Starting Time in Seconds) fields. It further processes the information, possibly producing an alarm. At the output, it copies what it received at the input plus all the information it finds relevant (here, the information about the alarms). The output could look as follows:

```
  TMSI F23415124546303b2d224c63 TCSD 19960716 TCST 220038 TCDR 000693
TBNB
  FFFFFFFFFFFFF30198672b641014 TBTP 01 TSDN 0016 TSTS 079238 TBZC 03
SALR
  ALARM SALV 0.87
  TMSI F23415124546303b2d224c63 TCSD 19960716 TCST 221856 TCDR 000031
TBNB
  FFFFFFFFFFFFF017433333d571a4f TBTP 00 TSDN 0016 TSTS 080336 TBZC 00
SALR
  NOALR SALV 0.37
  TMSI F23415124546303b2d224c63 TCSD 19960716 TCST 222015 TCDR 000367
TBNB
  FFFFFFFFFFFFF017433333d571a4f TBTP 00 TSDN 0016 TSTS 080415 TBZC 00
SALR
  NOALR SALV 0.33
  TMSI F23415140807624d312f4b4c TCSD 19960716 TCST 224913 TCDR 000003
TBNB
  FFFFFFFFFFFFFFFFFFF4646250c79 TBTP 00 TSDN 0016 TSTS 082153 TBZC 00
SALR
  NOALR SALV 0.12
  TMSI F23415137f381c3f526f710a TCSD 19960717 TCST 074916 TCDR 000001
TBNB
  FFFFFFFFFFFFFFFFFFF4646250c79 TBTP 00 TSDN 0017 TSTS 028156 TBZC 00
SALR
  ALARM SALV 0.98
  TMSI F2341513363e667947231933 TCSD 19960717 TCST 080242 TCDR 000023
TBNB
  FFFFFFFFFFFFFF301423d5c494b49 TBTP 01 TSDN 0017 TSTS 028962 TBZC 03
SALR
  NOALR SALV 0.07
```

The added information consists of the flag SALR (Supervised NN ALaRm) and the alarm level SALV (Supervised NN Alarm LeVel).

7.7 The virtual fraud detection tool.

To distribute the workload, the separate tools will be run on different platforms. This will result in a higher speed because there is no sharing of hard-disk or processor and less stringent requirements on memory and

disk space. The integration of the tools will thus be performed by passing messages between the respective modules. We propose doing this through the use of public domain software known as Parallel Virtual Machines (PVM). The following extract describes the features of PVM.

PVM is an integrated set of software tools and libraries that emulates a general-purpose, flexible, heterogeneous concurrent computing framework on interconnected computers of varied architecture. The overall objective of the PVM system is to enable such a collection of computers to be used co-operatively for concurrent or parallel computation.

Important features of the PVM system are:

> The application's computational tasks execute on a set of machines that are selected by the user for a given run of the PVM program. Both single-CPU machines and hardware multiprocessors (including shared-memory and distributed-memory computers) may be part of the host pool. The host pool may be altered by adding and deleting machines during operation.
>
> Application programs either may view the hardware environment as an attribute-less collection of virtual processing elements or may choose to exploit the capabilities of specific machines in the host pool by positioning certain computational tasks on the most appropriate computers.
>
> The unit of parallelism in PVM is a task, often but not always a Unix process, an independent sequential thread of control that alternates between communication and computation. No process-to-processor mapping is implied or enforced by PVM; in particular, multiple tasks may execute on a single processor.
>
> Explicit message-passing model: Collections of computational tasks, each performing a part of an application's workload using data-, functional-, or hybrid decomposition, co-operate by explicitly sending and receiving messages to one another. Message size is limited only by the amount of available memory.
>
> The PVM system supports heterogeneity in terms of machines, networks, and applications. With regard to message passing, PVM permits messages containing more than one datatype to be exchanged between machines having different data representations.

The PVM system is composed of two parts. The first part is a daemon , called pvmd3 and sometimes abbreviated pvmd , that resides on all the computers making up the virtual machine. Pvmd3 is designed so any user with a valid login can install this daemon on a machine. When a user wishes to run a PVM application, he first creates a virtual machine by starting up PVM. The PVM application can then be started from a Unix prompt on any of the hosts.

The second part of the system is a library of PVM interface routines. It contains a functionally complete repertoire of primitives that are needed for cooperation between tasks of an application. This library contains user-callable routines for message passing, spawning processes, coordinating tasks, and modifying the virtual machine.

8 B-Number analysis tool

8.1 Introduction

In D13 it was shown how B-number analysis can assist in the detection of fraud. The most common and expensive type of fraud, that of Subscription Fraud, will normally involve a subscriber using a false identity to purchase as many phones as he can in order to sell them, or the air time, to people wishing to make cheap international calls. Most fraudulent call destinations are to the Indian or African sub continent.

It is the purpose of this chapter to discuss the development of a B-number analysis tool that monitors the destinations of calls on a per subscriber basis. It will be possible to weight the destinations of calls differently so that well known destinations for fraudulent calls can be given special attention.

8.2 Proposed solution

The B-number analysis tool has been developed as a separate tool to the Supervised Learning Neural Network tool, the Rule Based tool and the Unsupervised Neural Network tool. This has been done so that there is the potential for the B-number analysis and the Unsupervised tool to run in parallel with each other as their operations are mutually exclusive. This is not planned for the trial integration however, whose architecture can be seen in Figure 7-2.

For the trial implementation, the B-number analysis will be the first module that receives the toll tickets in the 'Nice_tt' format from the simulation of the billing mediation device. The output from the module will be reformatted toll tickets that include tagging information to identify the source and nature of different fields. The B-number analysis will append alarm information pertaining to the results of its analysis in the form of a BALM field appended as the 7th TT entry.

The B-number analysis tool will maintain its own database containing the short and long term international call behaviour profiles, for each subscriber, indexed by the IMSI. Again the database software for the trial will be the GNU data base management facility.

8.2.1 Adding Tags to Toll Ticket fields.

The B-number analysis tool receives Toll Tickets in the cut down form of six fields that have been developed for ease of viewing and manipulation. The six fields passed to the B-number analysis are the IMSI, Charging Start Date, Charging Start Time, Chargeable Duration, B-number and B-type of the call. The first task of the B-number analysis tool is to reformat these fields adding the tags that were agreed to identify each field.

The tag identifiers are TMSI for IMSI, TCSD for charge start date, TCST for charge start time, TCDR for chargeable duration, TBNB for the B-number and TBTP for the B-type of number. To the end of this is appended the current alarm value for the subscriber in the BALM field. The B signifies to subsequent processes, receiving the modified Toll Tickets, that the field was generated by the B-number analysis tool.

8.2.2 Dividing the world into fraud risk categories.

The first task was to list all the countries of the world and to group together countries belonging to the same geographical area or countries which we expect to have strong economic bonds. Indeed, it is assumed that people tend to have more contacts with people of neighbouring countries or, for business reasons, with their economic partners. This leads to the implementation of 10 different classes corresponding roughly to the following regions : North-America, Africa, South-America, Australia, Asia, Russia, East Block, European Community, Middle East and Central Asia.

During runtime, for each Toll Ticket related to an international call, the country code is extracted. As the country code is kept unsanitised, extracting it boils down to truncating the leading 'F' characters, included during pre-processing to pad out the TT-NON-CHARGED-PARTY field, and extracting two, three or four characters depending on the country code considered. Indeed, to make a correct classification, we sometimes have to distinguish between dialling codes such as 00-353, which belongs to Ireland and should be assigned to

the European Community class, and 00-355 which belongs to Albania and should be assigned to the East-Block class.

8.2.3 B-number Profiling

As a Toll Ticket arrives for a user, the tool first determines if the call made concerns an international destination, and applies the international analysis if necessary. Each time an international call is made the Toll Ticket is assigned to one of the classes it belongs to and a vector of counters keeps track of the number of times each class has been excited by an incoming Toll Ticket. By considering two different time-spans over the toll tickets, we generate two profile records for each user. The profile representing the shorter Toll Ticket span represents the user's most recent activity and is called **`CUP_int`** while the longer span represents the user's history of usage and is called **`UPH_int`** The two profiles are maintained as probability distributions using two different decay factors a and b , both between 0 and 1. When a new Toll Ticket arrives, the user's **`CUP_int`** is updated. Each element of the **`CUP_int`** is multiplied by the factor a and the class to which the incoming Toll Ticket belongs is incremented by a factor $1-a$.

The update rules for CUP_int are thus:

$$CUP\_\text{int}_{i\,new} = CUP\_\text{int}_{i_{old}} * a \quad \text{for } i \neq k$$

$$CUP\_\text{int}_{k_{new}} = CUP\_\text{int}_{k_{old}} * a + (1-a) \quad \text{for } i = k$$

with *k* being the number of the class to which the Toll Ticket belongs and *i* referring to the index of each class.

By assigning a 1 to the class which the Toll Ticket belongs to, the first time an international call is made, and using this updating technique, the profile is maintained as a probability distribution function. After updating the **`CUP_int`** both profiles are presented to the fraud engine that will determine the alarm level. It is necessary to allow both profiles to develop adequately for each user before considering the alarm level as evidence that anomalous behaviour is occurring. Following presentation to the fraud engine, the **`UPH_int`** is updated by incorporating information from the **`CUP_int`** to it and by using a decay factor of b .

The update rule used for the UPH_int is:

$$UPH\_\text{int}_{i_{new}} = UPH\_\text{int}_{i_{old}} * b + (1-b) * CUP\_\text{int}_{i},$$

where *i* refers to the index of each class.

The exact value of the two decay factors a and b is critical to the success or failure of the system and has still to be determined by experiment. So as not to increase unnecessarily the overhead on the system, we use the same a and b factors as the one used in the A-number analysis.

8.3 Results

The fraud engine takes the B-number profile record consisting of the **`CUP_int`** and **`UPH_int`** as an input and calculates a *modified* Hellinger distance over all the entries of the profile record. Indeed, we weight each entry in the Hellinger distance by a factor depending on how frequently this class is called over all the users. In this way we can attach more importance to changes occurring to classes that a genuine subscriber rarely calls while minimising the influence of changes to classes that are very often called. We determine the weights by first calculating the number of calls to each class over all the Toll Tickets. This gives us the histogram as shown below where the scale used is logarithmic :

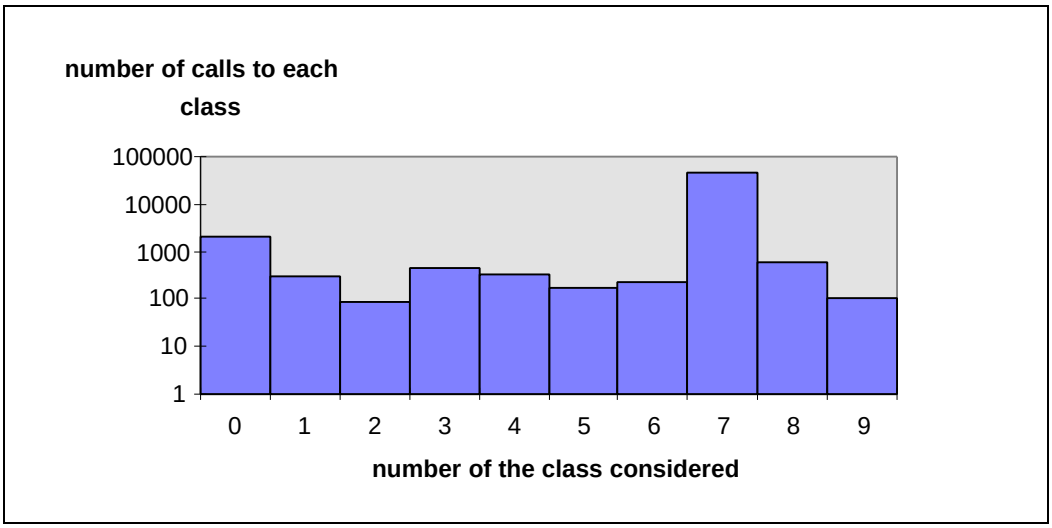

Figure 8-1 - Number of calls made to each class over the sequence of international Toll Tickets.

It can be seen from this figure that the majority of calls are made to the European Community class which corresponds to class number seven, while the other classes seem to have a more or less equal probability of being called. We decide thereupon to assign a weight of 0.5 to the European Community class, and to assign each other class a weight given by :

$w_i = 1 - \frac{n_i}{\sum_{j \neq k} n_j}$, where n_i is the number of calls to class i, and k is the index of the European Community class. The factor 0.5 for the European Community was chosen arbitrarily. It has to be high enough to allow changes in this class to raise an alarm and low enough so as not to raise an alarm too often.

8.4 Conclusion

In this chapter we have explained the solution and implementation of a B-number analysis tool. International calls amount to approximately 10% of the total call distribution and we thus require ten times the quantity of data to test our tool to the same extent as the A-number analysis. Data is still being accumulated as a result of the user selection process and will be available for the project trials. We thus expect to be able to comment further on the performance of the B-number analysis in the final project report.

We note that it would also be desirable to perform a national B-number analysis. This should enable us to target drug rings and prostitution rackets that tend to use fraudulent mobiles for their criminal activity. It would also be possible to take this a stage further and consider geographical information and weight calls that are destined for cell sites with a reputation for attracting fraudulent activity.

9 Trials and demonstrations

9.1 Demonstration and trial requirements

The demonstrations and trial for the fraud detection tools provide the basis for WP2.2 contribution to the main objective of this project, concerning the feasibility and acceptability of new and advanced security features in existing and future personal communication networks.

In the context of fraud detection especially, new techniques for detecting fraudulent behaviour were developed, including both rule-based and neural network implementations, in line with the approach currently being taken by many of the larger financial organisations world-wide.

The technical feasibility of the developed mechanisms is displayed through the demonstrations. Following this, the acceptability of the security features by users and network operators will be measured during the trial. The trial also provides the means to measure the tools' performance in a near-real-time network environment. The outcome and the collected results will form part of the final project report, where the opportunities for further development will be assessed.

9.1.1 Demonstration requirements

The aim of the demonstration is to show the validity of the fraud detection concepts in a mobile network scenario. To provide a thorough test of the practicality and utility of the fraud detection methods proposed, a series of requirements must be met.

First of all, genuine network data need to be used. Suitable UMTS network data are not available because - apart from the fact that the number of users in UMTS trials is quite small - only simulated fraud could occur there. Therefore, the fraud detection concepts could not be validated. Only in operational commercial networks, serving a large user population, is there a substantial probability that fraud attempts will occur. Thus, the network operators need to supply real usage data, representative of the operation of their network, not subjected to any ordering or filtering, to be used for the evaluation process.

Also, taking into account the data protection laws, the user data need to be converted in a way that prevents any user identification, before their processing by the fraud detection tools. This is the sanitisation procedure, by which all fields with references to users' identities in the subscriber data are encrypted.

Finally, the outcome needs to be evaluated by the network operators, so that the validity of the results can be measured and any issues arising in this context identified. In this view, the co-operation of the identified subscribers' service providers might become necessary in some cases, while still taking into account user privacy considerations.

9.1.2 Trial requirements

The trial aims to show the proper functioning of the integrated hybrid fraud detection tool in a real network. To achieve this, the following additional requirements must be met:

- the tool should be connected to a mediation device, where the toll tickets are collected, to provide fraud detection as close to real-time as possible;
- the presentational aspects of the fraud detection tool should be considered (e.g. user interface, quality of service).

9.2 Description of demonstration and trial

9.2.1 Description of demonstration

The first demonstration, where the three original tools were tested, showed the validity of the basic fraud detection concepts and compared them. The results were analysed with respect to the identified requirements, to the defined functionality and to the aimed quality of service. The outcome of this analysis was fed back to the demonstrators to enhance their functionality. Each method's strengths and weaknesses were thus perceived.

Also, it was made clearer that the interconnection of the tools to form one enhanced hybrid system could combine all components' strong points.

The second demonstration will display the functionality of this hybrid tool.

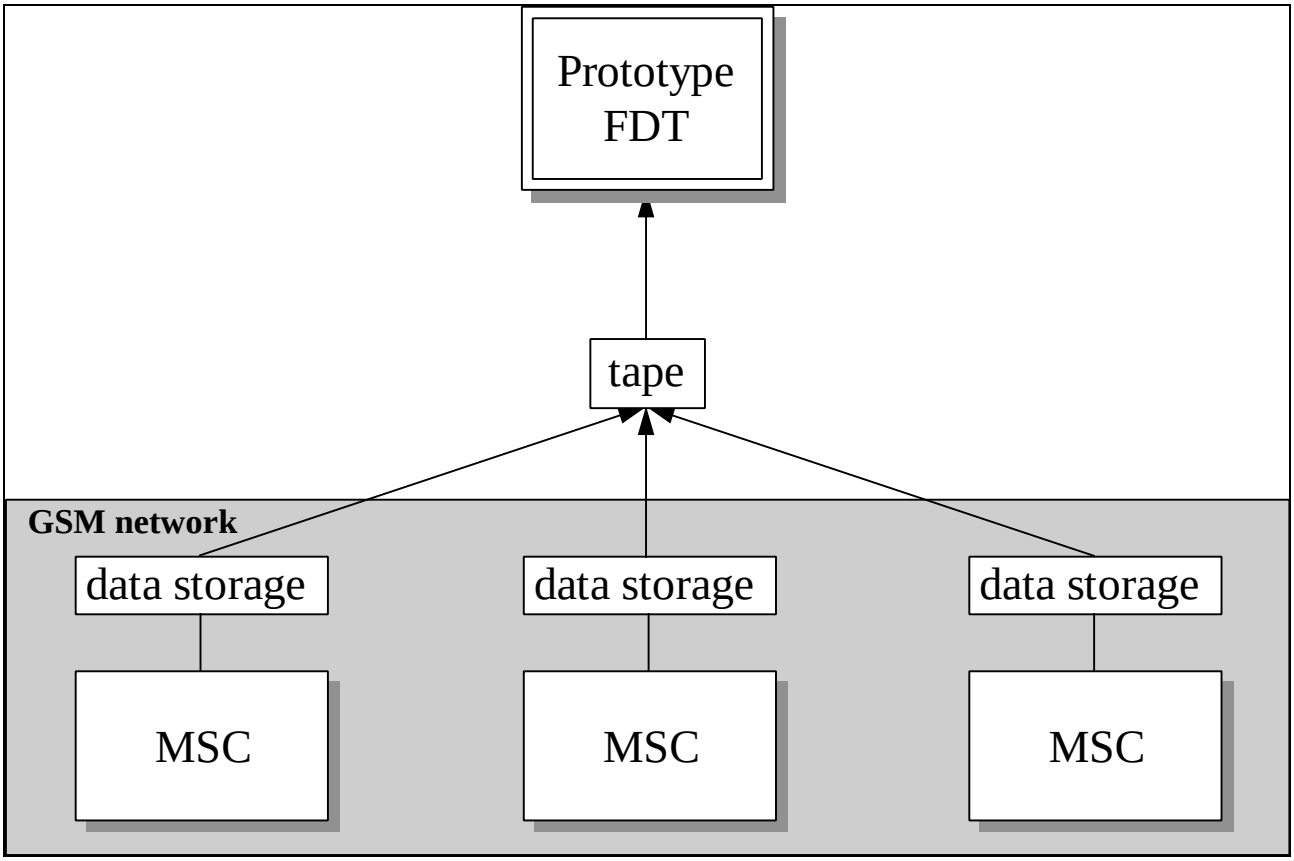

Figure 9-1 - Demonstration Architecture

Figure 9-1 shows the structure of the demonstration. The fraud detection tool is used off-line.

The GSM network data is provided by the operators on tape from different switching units of the network.

The outcome of the analysis will give a first indication of their performance and of the percentage of frauds that can be identified.

Finally, the user interface will be in the form of screen displays and automated reporting facilities provided by the artificial intelligence systems. The legal team, responsible for the presentation of fraud detection, will direct and ensure that the indicators are complete and coherent, providing detailed instructions.

9.2.2 Description of trial

The aim of the trial is to show the validity of the fraud detection concepts in real environments.

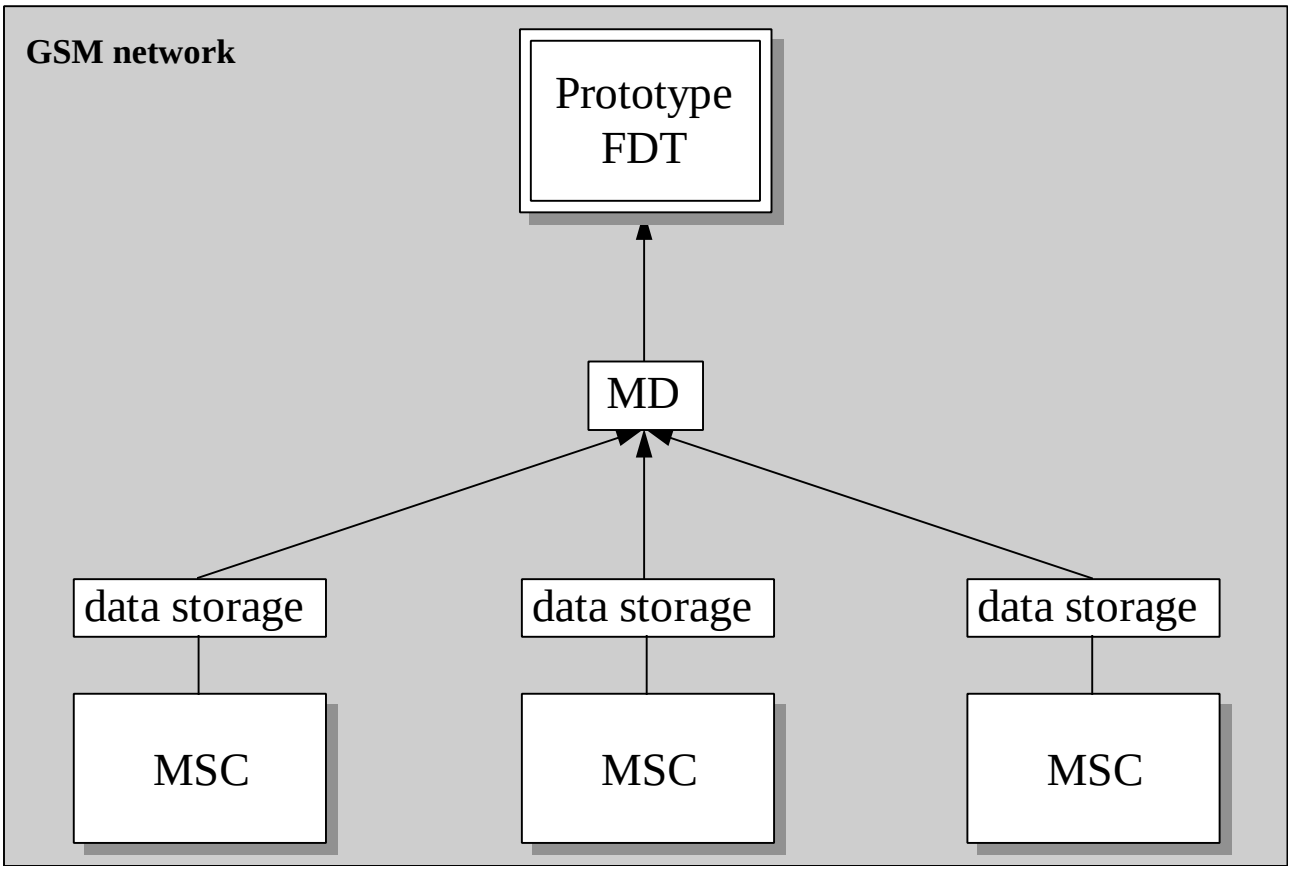

Figure 9-2 - Trial Architecture

Figure 9-2 shows a possible structure of the trial. The actual configuration will be defined in later stages of the project. The fraud detection components of the integrated tool are enhanced prototypes that realise the basic functionality as well as part of the enhanced functionality developed during the second design phase. Again, GSM network data will be used to ensure that the data arise from a network with a large user population and therefore with a substantial probability that real frauds may occur.

In the trial, the fraud detection tool may be connected to a real network through a mediation device. At regular intervals, the data will be transmitted to the fraud detection tool. In this case, the fraud detection tools would be used on-line as part of the GSM system. The results of the analysis would be directly evaluated by the network operator.

9.3 Trial workplan

Description of the combined tool will be included in deliverable D19.

A trial of the combined tool will take place in the second half of 1998.

The results of the trial will be evaluated, and conclusions and recommendations will be included in the final report of the project.

10 Legal Aspects

This Chapter introduces the legal aspects of Fraud Detection. It discusses the main issues which are relevant to this topic, and scopes the work that is to be done in Work Package 2.6.

10.1 Scope of our study: legal aspects of ASPeCT

This study will specifically focus on identifying and analysing the legal provisions at European Union and domestic level which are relevant to fraud in the field of mobile telecommunications. If there are no relevant European Union legal instruments it will establish which Member States have and which do not have legislation which may be relevant to the field of telecommunications fraud. Finally, the study will examine whether there are relevant legislative proposals in certain Member States.

The study will then focus on legislation which may make the detection of fraud more difficult. Ironically, this may include laws safeguarding the right to privacy in one's communications[1] and legislation on personal data protection.

Each type of fraud will have to be matched with a legal provision. This will necessitate adopting precise definitions of the different types of fraud. It will also be considered whether certain types of fraud fall outside all the relevant existing legislation in a Member State thus giving rise to legal loopholes. The study will determine which Member States have stricter regimes than others concerning fraud prevention.

The study will establish what are the possible legal remedies for parties that have been prejudiced by fraud. They may include remedies in contract law e.g. termination of the contract, criminal prosecutions and sanctions and compensation for economic loss suffered.

As trans-border fraud will constitute a very real risk in the area of mobile telecommunications the study will cover the issues of the applicable law and competent jurisdiction. This will involve analysing the fields of conflicts of laws and Private International Law.

The aim of Private International Law is to “localise” a legal relationship which touches upon more than one State within a specific national legal order. The law of this State will then be declared applicable to the case. Private International Law generally chooses the applicable law by applying conflict of law rules.

As a first step, the study will analyse the provisions of the San Sebastian Convention (which is the latest version of the Brussels Convention[2]) to determine if any of its provisions are relevant to the study. The provisions of the Lugano Convention will also be examined. Like the Brussels Convention (upon which it is based), the Lugano Convention promotes the free movement of judgements between the contracting states (so long as the Brussels Convention is not applicable).The structure of the Lugano Convention resembles that of the Brussels Convention. However, the Lugano Convention does not guarantee uniform interpretation in the way that the Brussels Convention does as the European Court of Justice does not have jurisdiction to interpret the Lugano Convention.

---

[1] A good example is Article 5 of the Common Position (EC) no 57/96 adopted by the Council on 12 September 1996 with a view to adopting a Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks. It bears the heading "Confidentiality of the communications" and provides as follows:

"*Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized".*

This provision is influenced by Article 8 of the ECHR.

[2] The full title of the convention is the "Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters". It was concluded on 27 September 1968 between the original six Member States of the EEC. The purpose of the Brussels Convention is threefold: it regulates the jurisdiction of the Courts of the Member States, introduces a simplified procedure for the recognition and enforcement of judgments and arranges for the recognition of authentic documents from other Member States.

The study will also focus on the evidential value of fraud data in legal procedures. The admissibility of evidence in the form of electronic data is far from clear. This relates to the phenomenon of "dematerialisation" of paper documents.

10.2 The legal issues

The legal issues which arise in the context of the ASPeCT project can be classified in two groups:

1. the ones arising during the fraud detection process, mainly problems related to telecommunications privacy and personal data protection;
2. once fraud data have been detected, the legal value of these data is at stake; we might face problems related to the existing legal qualifications of fraud and possible legal remedies.

10.2.1 Fraud detection process

10.2.1.1.1.1 Telecom privacy

A network operator who wants to install fraud detection systems might face problems arising from the existing international and national rules protecting the privacy rights of the individuals.

It is recognised at the international level that *everyone has the right to respect for his private and family life, his home and his correspondence,* as it is stated in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[3].

However, this article of the European Convention of Human Rights (ECHR) allows certain exceptions to this rule when the following conditions are fulfilled:

1. any interference with this right should be in accordance with the law.

   This means that the network operator can only take fraud prevention measures which interfere in one way or another with the privacy rights of the mobile telephone users if this interference is regulated by a law.
2. the interference should be necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder of crime, for the protection of heath or morals or for the protection of rights and freedoms of others.

The European Court of Human Rights has clarified somewhat the scope of these conditions in the framework of the *Malone case*[4], in which the applicant alleged violation of article 8 of the ECHM under two heads: 1. Interception of his postal and telephone communications by or on behalf of the police; 2. "Metering" of his telephone by or behalf of the police.

Regarding the first condition, the Court made it clear that the expression "in accordance with the law" should be interpreted in the light of the general principles as stated in the *Sunday Times* judgement of 26 April 1979[5] to apply to the comparable expression "prescribed by law":

1. The word "law" is to be interpreted as covering not only written law but also unwritten law;
2. The interference in question must have a basis in domestic law.

Both expressions were however also taken to include requirements over and above compliance with domestic law. Two of these requirements are the following:

1. the law must be adequately accessible;
2. a norm can not be regarded as law unless it is formulated with sufficient precision to enable the citizen to regulate his conduct[6].

---

[3] This Convention was signed in Rome on the 4th of November 1950, in the framework of the Council of Europe.

[4] Malone judgement of 2 August 1984, Publ. Court, Series A, vol. 82, page 30 and following.

[5] Series A, no. 30.

The Court also reiterated its opinion that the phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention.

It appears at first sight that the second condition imposed by article 8.2 of the ECHR will be less difficult to satisfy since it is clear that the measures which a network operator might wish to put into practice to prevent fraud are motivated by the need for preventing a disorder or crime: fraud.

However, it should be also taken into account that the European Court of Human Rights specified, in the above-mentioned *Malone* case, that an interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse.

It will be necessary to analyse the national rules existing in each Member States regulating telecommunications in order to see if exceptions for the network operator are foreseen, to analyse the nature of the law in question and the extension of eventual exceptions.

Our intention is to include a comprehensive table illustrating the rules of all the Member States concerning this issue in our final report.

10.2.1.1.1.2 Personal data protection

The issue of personal data protection is extremely important in the context of the ASPeCT project as it is clear that anybody wishing to detect fraud will need to have enough data. These data will refer to the clients, the users of mobile phones, and to their profile as telephone user; in other words, these data will be "personal data" in the sense of the European and national data protection legislation as it will refer to an identified or identifiable person.

The European and national data protection legislation protects individuals against the processing of their personal data by making this processing subject to certain conditions, imposing obligations on the controllers of the data and guaranteeing extensive rights to the data subjects, in this case, the users of the mobile phones.

Processing of personal data carried out in the context of the ASPeCT project in order to detect fraud will have to satisfy the conditions imposed by the European and national data protection legislation as to the legality of the processing operations, the adequacy and quality of the data, the principles which the data controller should respect and the obligations which he should comply with and the rights which the data subjects are entitled to.

The existing European instruments in the telecommunications field, such as the European Commission's mobile Green Paper[7], are characterised by viewing data protection as a possible obstacle to the free working of telecommunications networks.

This point of view is however not correct as data protection rules do not impede the development of modern telecommunications but they just impose certain obligations which should be respected in order to guarantee the rights of the users of the new telecommunications technologies.

It should not be forgotten that new telecommunication technologies represent a greater danger for the protection of personal data. This is due to the fact that new telecommunication technologies make use of sophisticated data processing and transmission systems which make the processing and exchange of data easier and quicker.

At European level, two legal instruments should be taken into account:

1. The European data protection directive 95/46/EC of 24 October 1995 for the protection of the individuals with regard to the processing of personal data and the free movement of such data [8].
2. The European privacy and telecommunications draft directive.

---

[6] Sunday Times judgement, p. 31, § 49; Silver and other judgement, p. 33, §§ 87 and 88.

[7] Towards the Personal Communications Environment: Green Paper on a Common Approach in the Field of Mobile and Personal Communications in the European Union (27 April 1994), COM 94/145/Final.

[8] Directive 95/46/EC, OJ L 281, 23.11.95., p.31; from now on "the directive"

1. **The European data protection directive**

The European data protection directive, which was adopted in 1995 after five long years of negotiation, aims at achieving a harmonised data protection framework at European level, minimising the differences presently existing between the legislation of the fifteen Member States. The Member States have three years (ending 24 of October 1998) within which to implement the European directive in their legal systems.

The data protection directive is based on two fundamental principles:

1. Free movement of data within the European Union: Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data;
2. A high level of protection should be guaranteed by the Member States.

The European directive establishes a number of general principles, which may have important consequences in the context of the ASPeCT project. Among others:

- Legitimate processing: Article 7 of the directive enumerates the cases in which the processing of personal data will be considered legitimate by the Member States. For instance: when the data subject has given his consent to the specific processing operations; when the processing is necessary for the performance of a contract to which the data subject is party; when the processing is necessary for compliance with a legal obligation to which the controller is subject, etc.

  Only in these cases can processing of personal data be allowed by the Member States.

  This means in the context of ASPeCT that one has to make sure that the processing activities which take place in order to detect fraud fulfil the requirements of one or more of the letters of article 7 of the directive. If this appears not to be the case, additional measures will have to be taken to make sure that the requirements of article 7 of the directive are fulfilled, like, for instance, asking for the consent of the data subjects (the mobile phone users).

- Finality principle: article 6.1 b) of the directive states that data should always be collected and processed for a specified purpose, they can not just be collected and processed at random. Further processing for other legitimate purposes is allowed if this second purpose is not incompatible with the specified purposes.

  In other words, personal data that the phone companies collect from the clients for billing purposes can in principle only be used for this purpose or, eventually, for other purposes considered compatible with this one. It should therefore be assessed if fraud detection purposes can be considered as compatible purposes. Moreover, as we will see later on, the clients (data subjects) should be informed of these secondary purposes.

- Adequacy and quality of data: The first paragraph of article 6 of the directive refers to data adequacy and quality principles providing that personal data should be:

  - adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

  - accurate and, where necessary, kept up to date;

  - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which data were collected or for which they were further processed.

  This principle is clearly related to the above-mentioned finality principle. It will be necessary to take adequate measures to act in accordance with these provisions of the directive.

- Special protection of sensitive data: The directive grants greater protection to special categories of data enumerated in article 8: data revealing racial or ethnic origin, political opinions, religious or philosophical

beliefs, trade-union membership, health or sex life. These data can only be processed in exceptional circumstances.

In principle, none of these data appear to be susceptible to being processed by a network operator or service provider; it can therefore be assumed that article 8 will not bring about any difficulties for phone companies willing to put into practice fraud detection systems.

- Rights of the data subjects: Article 10 to 14 of the directive deal with the rights of the data subject, in particular the right to be informed, to have access to the data and to object to the processing of data. It is for the controller (the one determining the purposes and means of the processing) to guarantee the exercise of these rights.

  It will have to be analysed what consequences these rights will have in the context of fraud detection systems; it is anyway clear that the data subjects (the users of mobile phones) should be informed of the collecting and processing of their data for the purposes of fraud detection.

- Obligations of the controller: the directive imposes specific obligations and responsibilities on the controller:

  1. with regard to the rights of the data subjects, which should be guaranteed by him;
  2. with regard to the adequacy of the data, security of the processing and liability towards any person who has suffered damages;
  3. with regard to the notification to the supervisory authorities.

  It will be necessary to provide the phone companies willing to put into practice fraud detection systems with a list including all the obligations they should fulfil in order to respect the obligations imposed on them by the directive.

- Trans-border flows of data: Given the international dimension of mobile telecommunications, it will be essential to take into account the provisions of the data protection directive regulating trans-border flows of personal data. The directive aims at guaranteeing the free movement of personal data within the European Union but imposes serious limitations when personal data have to be transmitted to third countries.

2. **The European privacy and telecommunications draft directive**

The Council of the European Union adopted on the 12th September of 1996 a common position regarding a directive concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks[9]. This draft directive is presently being discussed at the European Parliament and will be, once approved, of vital importance in the context of the ASPeCT project.

The aim of this proposal is to apply for the specific purposes of telecommunications networks the general data protection principles laid down in Directive 95/46/EC. It is designed, in a constantly changing field, to prevent Member States' legislation from developing along different lines in ways which may jeopardise the single market in telecommunications services and terminal equipment, while ensuring a high level of protection for the rights of individuals, in particular, their right to privacy.

This directive emphasises the increasing risk associated with automated storage and processing of data relating to subscribers and users[10].

---

[9] Common position (EC) No. 57/96 adopted by the Council on 12 September 1996 with the view to adopting Directive 96/…/EC of the European Parliament and of the Council, of … , concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks (96/C 315/06), OJ C 315, 24.10.96, p. 30.

[10] See recital n. 6 of the preamble to this directive.

The privacy and telecommunications draft directive contains specific provisions dealing with security and confidentiality of the communications, processing of traffic and billing data, itemised billing, presentation and restriction of calling and connected line identification, automatic call forwarding, directories of subscribers, unsolicited calls, technical features and standardisation.

In particular, article 6 of the draft directive, which refers to traffic and billing data, can play a fundamental role in the ASPeCT context since it specifically refers to the use of these data for purposes of fraud detection and makes this use subject to certain conditions.

An analysis of this and other provisions of the draft directive on privacy and telecommunications will be included in our final report, underlining the practical consequences for the ASPeCT project.

3. **Provisional conclusion**

The principles of both directives will certainly not constitute an obstacle to the development of fraud detection systems in the context of ASPeCT if adequate measures are taken to fulfil the conditions imposed by them and to respect their principles. Our final report will include clear guidelines in this sense.

Also the national legislation will be analysed in order to check if additional obligations should be respected at national level.

10.2.2 Legal value of detected fraud data

The law of evidence has always been biased in favour of paper documents. However, this situation is changing as electronic documents become more and more common in today's world. This phenomenon is known as the "dematerialisation" of paper documents. The bias in favour of visible documents may pose a problem for ASPeCT as most of the fraud evidence will be in the form of electronic data. The question is whether this form of evidence is admissible in Member State Courts?

10.2.2.1.1.1 The main systems of the law of evidence

The law of evidence is a particularly complex and difficult subject to deal with. The main reason is that it relates to the innermost concepts and traditions of the legal system of a nation.

A complete and concise definition of evidence in its legal context is given in the Oxford English Dictionary as "*information, whether in the form of personal testimony, the language of documents, or the production of material objects, that is given in a legal investigation, to establish the fact or point in question*". The evidence by which facts may be proved or disproved in Courts takes mainly three forms, namely oral evidence, documentary evidence and things. However, we will concentrate on documentary evidence in this study: in all technological cases, oral evidence or things are not the most important part of evidence.

This study will reflect the difference that exists between the common Law and civil Law approaches to the Law of Evidence.

10.2.2.1.1.2 The common law approach

At common law, evidence is categorised as *direct evidence* or *hearsay evidence*. Direct evidence is that given, orally or in writing, by a witness of things he has actually seen. Hearsay - named also "*indirect evidence*" - may be defined as "*any statement, other than one made by a witness in the course of giving his evidence in the proceedings in question, by any person, whether it was made on oath or unsworn and whether it was made orally, in writing or by signs and gestures, which is offered as evidence of the truth of its contents*" [11]. In other words, it is that evidence which is reported by a witness having personal knowledge of those facts from other sources. This basic distinction also applies to documents.

The basic common law principle is that direct evidence is admissible, that is, receivable by Courts, whilst indirect or hearsay evidence is not.

---

[11] Keane A., *The modern law of evidence* (3rd ed.), Butterworths 1994, pp. 8-9.

The basis of the hearsay rule was that electronic data could not be admitted as evidence in Court. However, over the centuries, the hearsay rule has been relaxed, and nowadays statutory and common law exceptions [12] exist which recognise the value of electronic evidence.

10.2.2.1.1.3 The civil law approach

Civil law countries have a different approach to the issue. In some civil law jurisdictions all relevant evidence is admissible. These systems are based upon the principle of *freedom of evidence*: all means of evidence may be produced and have free evidentiary value. Therefore, the only problem a Court faces when considering computer evidence is the weight to attach to it.

In others, the law sets out an exhaustive list of admissible evidence. Accordingly, legislation defines precisely which types of evidence are admissible in Court. The principle of *legal proof* holds that only the types of evidence explicitly mentioned in legislation are admissible in Court. In some civil law countries computer printouts may not be admissible as evidence while in others the Court may exercise its inherent discretion and thereby admit such evidence.

10.2.2.1.1.4 Constraints arising out of the law of evidence

It ought to be also noted that the term "*writing*" appears to require the existence of a physical document. However, if the law *only* refers to a "*document*", and there is no stipulation that it be in a visible form, there seems to be no reason why electronic evidence should be excluded. Much therefore depends on the language used in the national legislation.

10.2.2.1.1.5 Legal qualifications of fraud

This study will attempt to categorise the different types of fraud and then match those categories with legal provisions which may be relevant to this area of fraud.

It will be determined whether any category of fraud actually falls outside the terms of existing legal provisions at domestic and European Union level. In addition, ICRI will examine whether there are any legislative proposals at domestic and/or European Union level to block existing loopholes.

Does the law distinguish between technical frauds which are operated for financial gain and fraud which relates more to the personal use of mobile telephones without necessarily involving financial gain? [13]

10.2.2.1.1.6 Possible legal remedies

Once again there may be significant differences between the laws of the Member States in terms of legal remedies. ICRI's national correspondents will carry out an analysis of all the possible legal remedies available to a prejudiced party. These reports will, in turn, be critically analysed by ICRI.

The legal remedies may take a number of forms. They are as follows:

10.2.2.1.1.6.1 Contractual:

The possibility of fraud arising is usually provided for in contracts. Fraud constitutes a breach of contract and would entitle the prejudiced party to terminate the contract. The prejudiced party may be able to sue for damages for economic loss suffered arising from the breach of contract.

10.2.2.1.1.6.2 Criminal prosecution and sanctions

The area of fraud is usually covered by the criminal laws of a Member State. In a criminal case the State is the prosecuting party (the Plaintiff) whereas in civil cases the Plaintiff is usually an individual or a company. Theft of a SIM card would, for example, fall under criminal law rather than civil law. Criminal sanctions may include the possibility of a jail sentence.

---

[12] A House of Lords case - *Myers v. DPP*, [1965] A.C. 1001 - where it has been established that the categories of common law exceptions to the hearsay rule are closed and therefore only the Parliament may expand them by statute.

[13] See p. 4 of the ASPeCT Confidential document: "Fraud Scenarios in Mobile Telecommunication Networks" (Contributing Authors: C. Cooke and J. Brown) where this classification is described.

10.2.2.1.1.6.3 Compensation for damage suffered

Damage can be defined as "loss or harm, physical or *economic*, resulting from a wrongful act or default.[14] Compensation is the payment made for the loss or injury suffered. This compensation is often called "damages" and these are the "Court's estimated compensation in money for detriment or injury sustained by the plaintiff in contract or tort".[15] Service providers and Network operators may sue for damages when it becomes apparent that they have suffered economic loss arising from fraud.

10.2.2.1.1.6.4 Breach of Intellectual Property Law

Another possible legal remedy is to sue for breach of intellectual property law. For example, the act of cloning a mobile telephone may be an infringement of Patent Law. A patent is an exclusive right conferred on someone who invents or discovers some process, machine etc., to make, use sell or assign it for a certain period (usually 20 years) which may be extended[16]. Infringement of a Patent occurs when someone makes the product without the consent of the proprietor.

10.3 Conclusions

As in other areas of the communications sector which impinge on privacy or data security, there is an ongoing tension between

- fostering the development and widespread use of cost-effective information safeguards for individuals, commerce and industry
- safeguarding the rights and expectations of individuals to accepted levels of privacy
- protecting against new opportunities for illicit actions whether against individuals, economic actors or the member states.

Workpackage WP2.6 will continue the work of clarifying the legal issues, and providing direction to ensure the effectiveness of evidential information available from the fraud detection process.

[14] See page 98 of "A dictionary of Law" Second Edition, by L B Curzon.
[15] Ditto.
[16] See page 269 of "A dictionary of Law" Second Edition, by L B Curzon.