# Security challenges for Security Information and Event Management Systems in mobile money transfer services

Chrystel Gaber*† ‡ §, Saïd Gharout*, Mohammed Achemlal*† ‡ §, Marc Pasquet † ‡ § and Pascal Urien ¶
*Orange Labs - France Telecom 42 rue des coutures, F14000 Caen, France
†Université de Caen Basse-Normandie UMR 6072 GREYC, F-14032 Caen, France
‡ENSICAEN, UMR 6072 GREYC F-14050 Caen, France
§CNRS, UMR 6072 GREYC F-14032 Caen, France
¶Telecom Paristech UMR 5141, 37/39 rue Dareau 75014, Paris, France
Email: {chrystel.gaber, said.gharout, mohammed.achemlal}@orange.com
marc.pasquet@ensicaen.fr
pascal.urien@telecom-paristech.fr

***Abstract*—Mobile based money transfer services are promised to a large success in the future. Frauding such a system can be lucrative and will always draw the attention of criminals. Fraudsters are innovative and always looking for new ways to avoid detection. Security Information and Events Management (SIEM) systems can be a solution to this problem. However, these systems are originally designed to deal with network infrastructures. In order to address security and fraud issues in Mobile Money Transfer Services, SIEM systems have to be adapted in some significant fields such as multi-level correlation, scalability and resiliency. This article's objective is to put forward the challenges of fraud detection in a mobile based money transfer service for SIEM systems.**

## I. Introduction

The interest for mobile payment services has widely grown in the last few years. However, this type of service is quite strategic and security sensitive. Indeed, money is an attractive target for attackers and fraudsters. The service can also be misused for money-laundering and illegal funding. Moreover, this type of service should comply with the financial policy enforced in the country where the service is installed. These issues can be tackled through reinforced security measures or surveillance of anomalies and irregularities. This article addresses these kinds of mechanisms.

Studying relevant transactional data from a mobile payment service can give information about a possible failure or fraud. There already exist systems fulfilling this task for other payment services like credit cards. However, they do not target mobile payment services which introduce specific challenges. Security Information and Event Management (SIEM) systems are tools able to analyse data in real-time, correlate various events, raise alarms and launch counter-measures. However, today, these systems are mostly adapted to network surveillance and it is difficult to adjust them for specific application use. The European project " MAnagement of Security information and events in Service InFrastructure (MASSIF) " [MAS10] [PDR+11] proposes to improve SIEM systems in order to address these issues. The aim of this paper is to describe one of the four scenarios taken into account in MASSIF as well as the challenges presented by this scenario for SIEM systems. This scenario considers fraud detection in a mobile payment service.

In this paper, we consider the Mobile Money Transfer (MMT) system and architecture components. It is a system where electronic money, called mMoney (for mobile money), is used to carry out various types of money transfers and transactions like purchasing goods, receiving one's salary, paying bills, taking loans, paying taxes or receiving social benefits.

The first part of this article will present the example of money transfer service based on mobile phones which is considered in MASSIF. The second part presents SIEMS. Finally, the third part deals with the challenges of this scenario for SIEM systems.

## II. Mobile Money Transfer Service

The MMT service enables users to handle electronic money to carry out various types of money transfers and transactions. According to [CG96], [Eur98] and [Uni09], electronic money is a monetary value paid in advance by the user, it is stored electronically and it can be used to pay actors other than the issuer. The money can be stored in a device owned by the user, this is the case of hardware-based products named electronic purses. It can also be stored in a server which can be accessed by a specialised software installed on a device owned by a user, this corresponds to software-based products named virtual accounts or virtual wallets [CG96]. The system considered here is a virtual account available on mobiles. We consider in this article that the mobile based money transfer service is a branchless banking service [Mas09] proposed by

a telecommunication operator. It follows the non-bank model [LIS06]. Therefore, the operator owns the Mobile Money Transfer Service platform and is responsible of its working order. Banks have a limited role in this case. The following sections describe various aspects of the mobile money transfer service.

### A. Actors

Four categories of actors are involved in this service and each category is made of several roles. Each of them are associated to specific actions in the platform. The first type of actors is end-user. They are individuals who use their mobile phones to carry out transactions. The second type of actors are composed of service providers who provide services or goods to end-users. Payments usually occur between end-users and service providers. This category of actors are made of several roles. A service provider can for example be a merchant who sells goods or services or a biller who also sells goods or services but on a regular basis like an electricity company. Service providers can also be employers who pay their employees by using the MMT service or a government collecting taxes or providing social benefits. The third category of actors in the system is channel users. They are in charge of the distribution of electronic money. Other actors of the system can either acquire or sell electronic money from or to them. Channel users also deal with the registration or the termination of contracts. The roles which compose this category are wholesalers and retailers. Wholesalers buy electronic money from the operator and sell it to retailers. Retailers then sell electronic money to end-users. Administrators form the last category. They are employees of the operator who are in charge of the MMT platform and its set-ups. This category is made of a super administrator, network administrators and customer care operators.

There may be other stakeholders such as the operator or the central bank but their role isn't developed because this article mainly focuses on the actors who interact directly with the MMT platform.

### B. Description of the Mobile Money Transfer use case

The main use cases which will be considered in our research are payments and management of accounts. The possible payments with the MMT service can be broken down into four categories according to the nature of the actors taking part in the transaction:

- Money transfers between individuals. Remittances, pocket money and all sorts of transfers which can occur between two persons fall into this category.
- Payments from individuals to companies. This category concerns purchases, subscriptions, bills, insurance contributions or taxes.
- Payments from companies to individuals. These are for example social benefits, reimbursements.
- Money transfers between companies. An example is the payment of suppliers.

Both remote and proximity payments are possible in the MMT service. In the payment model described here, we consider that both types of payments are made online and require a communication with the MMT platform. Generally, a payment sequence respects the following pattern. Firstly, the sender is authenticated. Secondly the sender's payment instructions and transaction details are transmitted to the MMT platform. Thirdly, the MMT platform checks whether the transaction is possible or not and authorises the transaction. Fourthly, the MMT platform sends a notification to the receiver. Fifthly, the receiver is authenticated in order to receive the funds. Finally, the sender's account is debited, the receiver's account is credited and a notification message is sent to both of them. Management operations include changing of authentication information, checking up an account's balance, opening and closing accounts, creating electronic money. They also involve operations for the administration of the platform.

### C. Technical infrastructure

In this section, the technical infrastructure of the service is detailed. Figure 1 shows a global overview of the Mobile Money Transfer Service. End-users use their phones and access to the MMT platform through the network provided by their operator. The service providers and the channel users can access to the MMT platform through their cell phones or through web applications. Finally, the administrators of the system can access the platform through the internet.

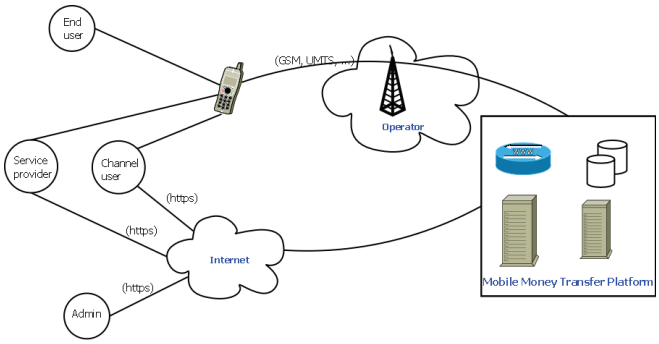


Fig. 1. Global view of the Mobile Money Transfer Service infrastructure

Figure 2 shows a functional view of the architecture of the core MMT system. The input of the system is an operation request received from mWallet holders. An operation request corresponds to any request that an end-user, a service provider or a channel user sends to the MMT platform. The nature of the request is not only financial, it can also be a request relative to application's settings for example. An operation request can for example be a request to modify the user's authentication code as well as a request to make a transfer or to check the account's balance. The outputs of the system are the notification about the operation's success/failure, the registration of transaction and operation information as well as the realisation of the requested operation.
The various functions of the MMT service are:

- Interface with the user. This function is carried out by the operations server. This consists in collecting the operation requests and sending out notifications.
- Process operation request. This function is also carried out by the operations server. Once an operation request is received by the system, it is either processed by the operations server itself or sent to the account management system according to its nature. The requests processed by the operations server are those unrelated to financial information and operations.
- Manage accounts. This is the account management system's function. This function concerns financial transactions and information. It is related to the control of accounts and operations of credit and debit.
- Register history of accounts. This function is handled by the data warehouse which registers the history of the movements of accounts.
- Register operation requests. This function is performed by the logs server which registers all the messages exchanged with the operation server.

Data that are relevant to analyse abnormal activities can be found in the logs registered in the log server and in the data warehouse. The logs contain a wide range of information such as requests for PIN modification, failed authentication, transaction request, transaction success notification, etc... This information can for example be used to detect in real-time events related to simple fraud cases. The data warehouse contains historical data about accounts and can be useful to analyse customer behaviour and detect more complex fraud cases.

## III. SIEM SYSTEMS

Security Information and Event Management (SIEM) systems provide two major functions. The first one corresponds to information management. It consists in managing logs and generating reports with relevant information collected in the logs. This function enables data storage, proof of compliance and long term analysis of data. The second function of SIEM systems corresponds to event management. It consists in analysis and management of real-time or near real-time events and incidents. There are some softwares which provide only one of these functions SIM (Security Information Management) systems and SEM (Security Event Management) systems are specialised in the real-time management of events.

The Security Information and Event Management process can be divided into five major steps. First, data is collected thanks to various sensors set in the system. Examples of sensors are firewalls, routers, or servers. The second step consists in normalising the collected data. Indeed, as the data come from heterogeneous sources their formats are generally very dissimilar and therefore are difficult to compare. Normalisation is a kind of translation which transforms all the data into a single format. The aim of this phase is also to identify and specify which fields of the data will be used. The third step is the aggregation of data. It consists in assembling various fields within the data to create new information. The next phase is the correlation. During this phase, various data are confronted with each other. The various structural or functional relationships are studied in order to discover and evaluate risks. A correlation engine is used for this step. After the correlation, alerts are generated and counter-measures are taken. These actions correspond to the last step of security information and event management.

As shown in figure 3, the architecture of SIEM systems is made of four layers which reflect the different steps of security information and event management.

Each layer has its own challenges. The major issues related to data collection are management of heterogeneous data as well as the performance and scalability of the data collection. In the case of data storage, the major problems are related to the optimisation of the memory necessary for storage, the integrity and security of data or the possibility to use the data as a legal proof. The data analysis layer major problems are the relevance and significance of the extracted information, the improvement of the quantity and the speed of data analysis as well as the scalability of the correlation engine. The last layer's issues mostly concern the user interface as well as alerts and reports generation.

## IV. SIEM SYSTEMS FOR MMT SURVEILLANCE : ISSUES AND CHALLENGES

In order to address the problems specific to MMT system surveillance, some functionalities should be added to current SIEM systems. The needs of MMT systems considered here are related to fraud detection. The following part describes the aspects on which fraud detection in the MMT service challenges SIEM systems today.

### A. Complexity of the scenario

This scenario is quite complex. Indeed, as seen earlier, there are many actors and many possible operations. This means that the SIEM system will have to handle many different cases and many different rules. The challenge here is to extract relevant information from the wide variety of collected events. Moreover, in this use case, the data handled come from the application layer. Application-level events are very different from network-level events which are targeted by todays SIEM systems. In order to detect fraud, SIEM systems should be able to take into account events from the application layer.

### B. Multi-parameter correlation

A SIEM system should enable to create rules which take several parameters into account. For example, a rule able to detect transactions with a certain amount for a specific receiver. It should also be possible to create a rule which is able to examine events from different sources. For example, it should be possible to correlate information found in the messages exchanged with the operations server with information from the account history.

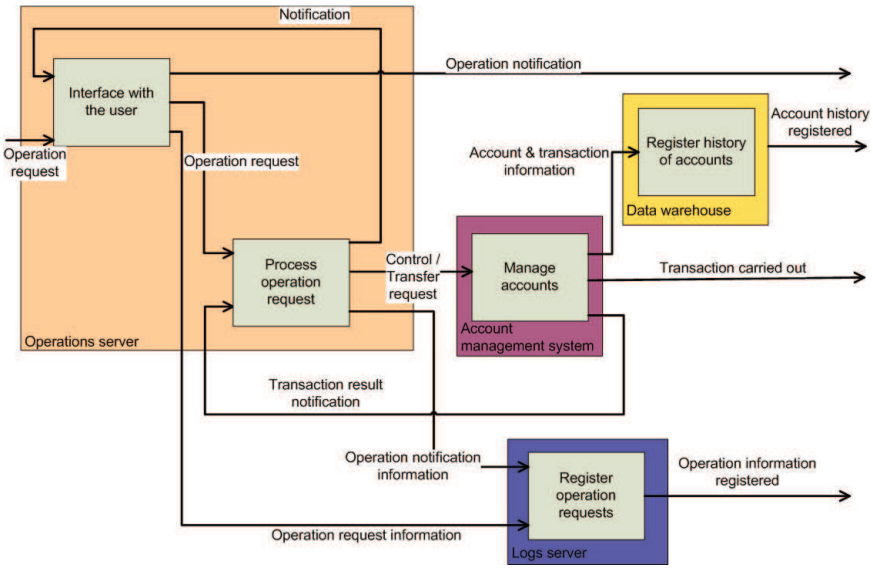


Fig. 2. Functional architecture

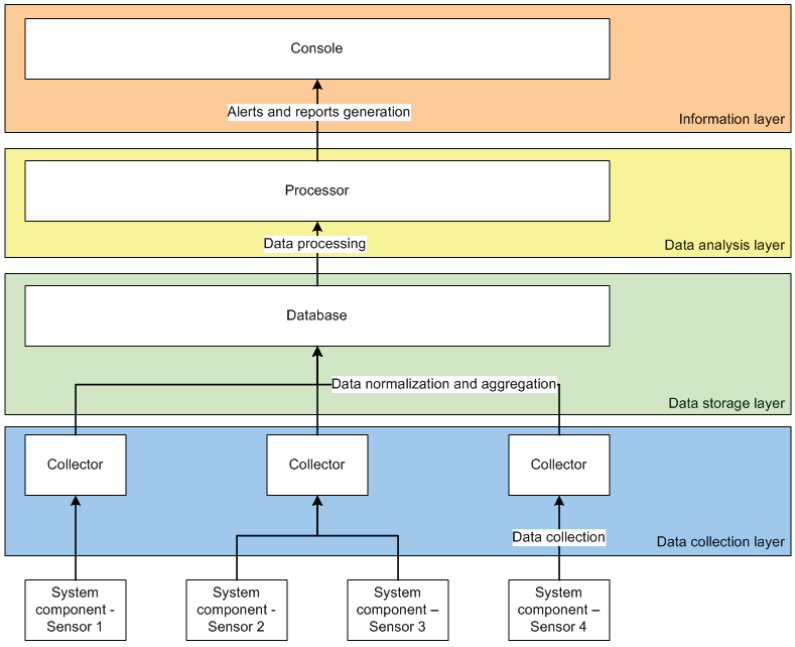


Fig. 3. SIEM architecture

### C. *Real-time detection using historical and real-time collected events*

One-shot frauds usually result in limited losses and therefore are not the major concern for financial organisations. Systemic frauds and money-laundering are the problems which mostly hold the attention of financial organisations. Such cases cause more serious damage than one-shot frauds, and may take place on longer periods. Thus, detecting such cases relies on the observation of events on a large period of time and should not be limited to events collected in real-time. It is necessary to study events collected in real-time as well as events collected and stored earlier.

### D. *Scalability*

The market of mobile payment services is still expanding. It is expected to develop more and more in the next years. Moreover, the mobile payment service M-PESA has shown that it is possible for a mobile payment service to expand and gain success in a short time span [JTT10]. Therefore, it seems important for SIEM systems to be scalable in order to face the rapid growth of a mobile payment service. Another aspect

which requires scalability of the fraud detection system is the seasonal variation of the number of transactions. For example, it is predictable that the number of transactions will be higher before holidays, religious feasts or important celebrations. This challenge is not only about the load supported by the SIEM, it is also about the robustness of fraud detection methods. A change of the number of users or transactions should not have any impact on the quality of fraud detection.

### *E. Multi-layer correlation*

One of the major challenges for SIEM systems is to combine events from different levels. For fraud detection in the MMT service, relating events from the network layer with events from the application layer can make fraud detection easier and more efficient. It can also result in new fraud indicators. This type of approach may help to detect frauds where networks are used to spread a virus which will carry out fraudulous financial transactions. This was the case of the fraud targeting online banking customers with the URLZone Trojan [M8610]. The attack consisted in two phases. First of all, a malware was spread to retrieve data and authentication information of various personal accounts. Then the malware would perform some money transfers from the user's account to a mule's account. The report [M8610] highlights the fact that this attack was difficult to detect for traditional anti-viruses. We believe that this type of attack would be more easily detected with a solution which would jointly analyse events linked to the network and to the sensitive application.

## V. Perspectives

Now that the security challenges of Mobile Money Transfer services have been identified, further work has to be carried out to propose security and detection features for these services. In the future, we are going to carry out a security study in order to identify the vulnerabilities of the system as well as the types of frauds and fraud scenarios which can be related to the Mobile Money Transfer use cases presented here. Future works will also focus on fraud detection and security features for mobile payment services.

## VI. Conclusions

This article presents one of the scenario studied in the European project MASSIF which concerns fraud detection in a mobile payment system. The aim of the article is to highlight the limits of SIEM systems withe regards to the problem of fraud detection in mobile based money transfer systems. An example of such a system is presented in the article . The architecture and functionalities of SIEM systems are depicted. The article also explains what are the challenges of fraud detection in mobile payment systems. The next steps of this work consist in identifying fraud schemes which can threaten the Mobile Money Transfer service, proposing security features addressing these frauds as well as adapting data mining algorithms for fraud detection.

## VII. Acknowledgements

This work was partly financed by the European Project MASSIF (MAnagement of Security information and events in Service InFrastructures) [[PDR+11] [MAS10] which is a collaborative project co-funded under the European commission's FP7 ICT Work Programme 2009 (FP7-ICT-2009-5).

## References

[CG96] Committee on Payment and Settlement Systems and Group Computer Experts of the central banks of the Group of Ten countries. Security of electronic money. Technical report, Committee on Payment, 1996.

[Eur98] European Central Bank. Report on electronic money. Technical report, European Central Bank, 1998.

[JTT10] William Jack, Suri Tavneet, and Robert Townsend. Monetary theory and electronic money: Reflections on the kenyan experience. *Economic Quarterly*, 96-1(96):83–122, First Quarter 2010 2010.

[LIS06] Timothy R. Lyman, Gautam Ivatury, and Stefan Staschen. Use of agents in brachless banking for the poor : rewards, risks, and regulation. Focus note 38, CGAP (Consultative Group to Assist the Poor), October 2006.

[M8610] M86 Security. Cybercriminals target online banking customers - use trojan and exploit kits to steal funds from major uk financial institution. Technical report, M86 Security, 2010.

[Mas09] Ignacio Mas. The economics of branchless banking. *Innovations: Technology, Governance, Globalization*, 4(2):57–75, 2009.

[MAS10] MASSIF partners. Massif project website. http://www.massif-project.eu/, 2010. Last visited on 22/05/2011.

[PDR+11] Elsa Prieto, Rodrigo Diaz, Luigi Romano, Roland Rieke, and Mohammed Achemlal. Massif: A promising solution to enhance olympic games it security. In *International Conference in Global Security Safety and Sustainability (IGS3)*, 2011.

[Uni09] European Union. Directive 2009/110/ce, 2009.