International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:5, No:11, 2011

An Inter-banking Auditing Security Solution for Detecting Unauthorised Financial Transactions entered by Authorised Insiders

*C. A. Corzo, N. Zhang, F. Corzo

Abstract—Insider abuse has recently been reported as one of the more frequently occurring security incidents, suggesting that more security is required for detecting and preventing unauthorised financial transactions entered by authorised users. To address the problem, and based on the observation that all authorised inter-banking financial transactions trigger or are triggered by other transactions in a workflow, we have developed a security solution based on a redefined understanding of an audit workflow. One audit workflow where there is a log file containing the complete workflow activity of financial transactions directly related to one financial transaction (an electronic deal recorded at an e-trading system). The new security solution contemplates any two parties interacting on the basis of financial transactions recorded by their users in related but distinct automated financial systems. In the new definition inter-organizational and intra-organization interactions can be described in one unique audit trail. This concept expands the current ideas of audit trails by adapting them to actual e-trading workflow activity, i.e. intra-organizational and inter-organizational activity. With the above, a security auditing service is designed to detect integrity drifts with and between organizations in order to detect unauthorised financial transactions entered by authorised users.

***Keywords*—**Intrusion Detection and Prevention, Authentication and Identification.

I. Introduction

The number of financial transactions performed by the banking sector has increased during the last decade [3]. Data published by the Bank of International Settlements (BIS) in March 2008 [6] showed that the number of transactions on the London Stock Exchange rose from 52.7 million in 2002 to 81.2 million in 2005. This is approximately a 54 percent increase in three years. Similarly, over the same period of time, the number of transactions executed on the New York Stock Exchange rose from 545.7 million to 918.9 million. This is an increase of approximately 68.3 percent during the three year period. By looking at the first calendar quarter of 2008, the London Stock Exchange reported that the total number of equity trades was up 46 percent to 70 million compared to the same period in 2007 [7]. More recently, in December 2010 a total of 19.1 million trades were carried out across the London Stock Exchange, up ten per cent compared to December 2009. The increase in performed trading transactions, on the banking industry and on the financial sector, may be due to the use of Information and Communications Technologies (ICT) [8].

ICT has become an important facilitator of financial transactions. The current processing time of performing one financial transaction is much shorter in comparison with the so-called traditional market or phone-call based trading systems. Services have helped reduce costs and increase operational efficiency. Thus, the speed at which money and market instruments circulate is much higher than ten years ago. Electronic trading (e-trading) can widen the access to a broader pool of potential investors [11]. There is quicker access to liquidity, further increasing the volume of banking business (powerful network economics) [12]. Unfortunately, the risks of fraud and forgery committed by both outsiders and authorised insiders have also increased and can cause greater damages to the institutions involved [13], and need to be addressed.

Moreover, the nature of current inter-banking e-services also allows authorised users to perform more fraudulent transactions within a given time period in comparison with past manual ways of performing transactions. Authorised users are in the position to more easily break any security barrier implemented in automated systems and services [2] and therefore they can pose a threat. Authorised users (insiders), e.g. banking employees, have privileges that allow them to access, to operate and to perform financial transactions using the financial services provided by automated banking systems.

Each year, billions of pounds are lost in the banking sector due to fraud committed through the exploitation of system vulnerabilities [1]. The 2008 CSI Computer Crime and Security Survey [9], for example, reported that financial fraud was the most expensive computer security incident costing an average of 500.000 USD for those who experienced the incident. Similarly, in the 2009 CSI Computer Crime and Security Survey [10], financial fraud was also reported to be one of the most costly security incidents. More concerning is the fact that insider abuse has been reported as one of the more frequently occurring security incidents, suggesting that more security is required for auditing and detecting unauthorised financial transactions entered by insiders.

To address the problem we have designed a new auditing system which is workflow oriented, and it is more dynamic and complete than current existing auditing systems. The solution is based on the observation that all authorised financial transactions are either triggered by or triggering another trans-

*C. A. Corzo was with the School of Computer Science, University of Manchester, UK, and is currently working with the Central Bank of Colombia - Banco de la República, Email: ccorzope@banrep.gov.co
N. Zhang is with the School of Computer Science, University of Manchester, UK, Email:nzhang@cs.man.ac.uk
F. Corzo is with Escuela Colombiana de ingeniería Julio Garavito, Bogotá, Colombia, Email:fcorzos@escuelaing.edu.co
* Disclaimer : The opinions expressed in this paper are those of the authors and do not represent the views of the Banco de la República or of its Board of Directors.

actions in a workflow. Thus, we have developed a redefined understanding of an audit workflow, one where there is an audit log file containing the complete workflow activity of financial transactions directly related to one financial transaction. The security solution is constructed on the basis of an e-trading workflow activity scenario. Current auditing systems do not contemplate dynamic interactions between two financial institutions, failing to present a complete workflow activity.

The new security service contemplates any two parties interacting on the basis of financial transactions recorded by their users in related but distinct automated financial systems. In other words, the new security service can detect multiple financial transactions that belong to one single transaction set, that is, a group of transactions that are triggered by an initial transaction. In the new definition inter-organizational and intra-organizational interactions can be described in one unique audit trail.

This concept expands the current ideas of audit trails by adapting them to actual e-trading workflow activity, i.e. intra-organizational and inter-organizational. In this audit workflow, external tasks cannot be isolated from directly related internal tasks of financial institutions. This is important since isolating the external tasks may lead to an inability to monitor the settlement of e-trading deals, that is, inability to trace the complete set of financial transactions triggered by a (trading) deal. Based upon the above findings, a workflow oriented auditing security service is designed to detect and prevent an integrity drift.

II. Infrastructure related to the Inter-banking E-trading

Inter-banking e-trading transactions are mainly related to clearing and settlement processes involving two banks. These processes are triggered by a trade confirmation and continue through the clearing process (the payment) up to the actual settlement of a trade (the transfer of a market instrument). The payment and transfer of market instruments are supported by automated systems that provide the required financial services and which constitute an infrastructure.

A. E-Payment

Payment systems are automated financial services, also known as Automated Clearing Houses (ACHs), which enable the transfer of an amount of money from one account to another.

There are two types of systems for inter-banking payments [5]: real time gross systems (RTGS) and netting systems. A RTGS is a payment system which processes the transfer of funds in real time [14]. No waiting period is required for the payment to be made. Netting systems may have to wait some time before the payment is made. The United States Fedwire system is an example of an inter-bank RTGS [15], whereas the Clearing House Interbank Payment System (CHIPS) is an example of a net payment system [16].

Also, payments can be classified, depending on the amount of money transferred, into two types [4]: wholesale payments and retail payments. Retail payments are low-value payments. Wholesale payments are large value payments (LVP). There is no defined limit on what amount would be a LVP. Usually, inter-banking payments are categorized as wholesale payments.

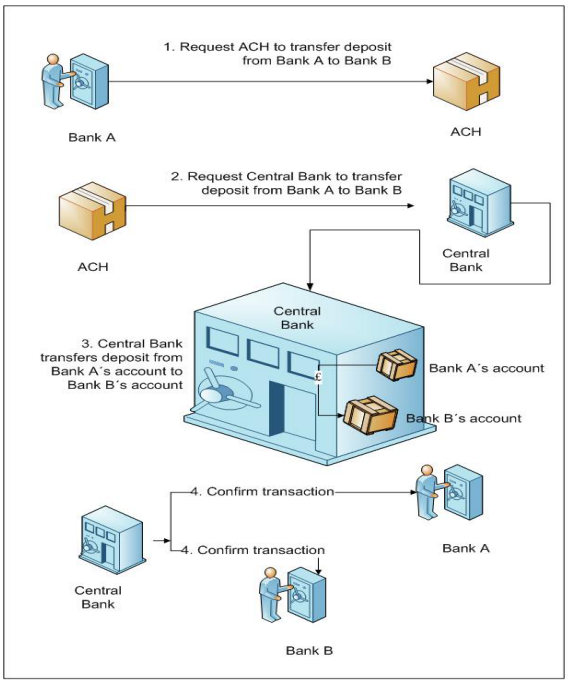

Fig. 1. Graphical representation of an Inter-banking payment process

An Inter-banking payment between two banks (bank A and bank B) can be summarized as follows (See Fig 1); First, Bank A requests ACH to make a deposit transfer to Bank B. Then, a deposit transfer is made to a Central Bank by an ACH. This request is usually performed using a secure messaging service [18], for example, via the Society for World Wide Interbank Financial Telecommunications (SWIFT) network. Inter-banking payments are usually settled at a Central Bank [17]. If the process requested can take place then a debit and a corresponding credit is made on both parties' account at the Central Bank, that is, the sender (Bank A) and the receiver (Bank B) of the payment. A confirmation message of the payment is then sent to both parties. The Central Bank plays, therefore, two roles at the same time, that of payee and of payer.

B. E-transfers of Market Instruments

Similarly to payment systems, a Central Security Depository (CSD) automated financial service enables the transfer of market instruments from one account to another. Therefore, users are required to have an account number associated to their assets at a central securities depository. The process is facilitated by financial services usually provided by CSDs.

CSD automated financial services can be interconnected in different ways to other cross border CSD systems. Three main types of infrastructures have been clearly identified in [19]

(see Fig 2): the CSD-link model, the Hub and Spokes model, and the European CSD model.

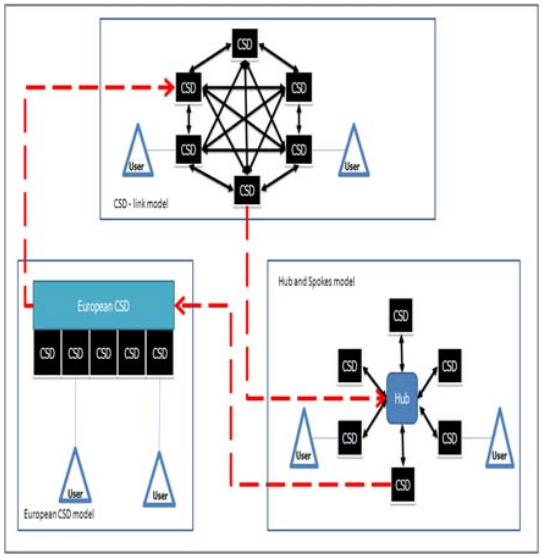

Fig. 2. CSD financial services' infrastructure interdependence

In the CSD-link model, each CSD system is connected directly to all the CSD systems where connections are required in order to perform a securities financial transaction. The problem with this model is that each CSD has to be interconnected to every CSD to which it is inter-linked. The CSD-link model requires a highly redundant infrastructure.

The Hub and Spokes model is a less redundant interconnecting infrastructure. In this model each CSD system is interconnected to one central party, through which each settlement is directed to other CSDs. The advantage of this model is that only one interconnection is required from each CSD. Also, the implementation time of this model is lower compared to the CSD link model. The Link-Up Markets is a joint venture in Europe by seven CSDs, and it is an example of the Hub and Spokes model.

The European CSD model is a Securities Settlement System that consolidates on the same platform more than one CSD. All operations performed by CSDs would be performed by the same CSD. Unfortunately, the implementation time for this model is considered very high compared to the CSD-link model and the Hub and Spokes model. Nonetheless, transfer costs are considered the lowest compared to the other previously mentioned models. The Euro-clear Settlement system for Euronext-zone Securities is an example of the European CSD model.

Efforts have been made by the financial institutions to promote the integration of clearing and settlement systems (see Fig 3). For example, France, Holland, Belgium, and Portugal use one common trading platform, i.e. Euronext. The United Kingdom has the London Stock Exchange (LSE) for trading. Both Euronext and the LSE use the London Clearing House (LCH) Clearnet for the cash securities business and use the custody and settlement capabilities of Euroclear. There are financial systems in other countries, like Switzerland and

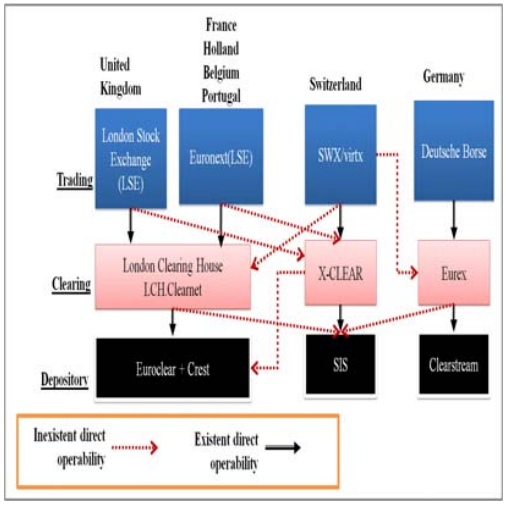

Fig. 3. Graphical representation of European clearing and settlement systems' interdependence, taken from [22]

Germany, which remain isolated. Full interoperability has not yet been achieved between all European financial services.

Although in the last years efforts have been made to integrate the securities and payment systems, they are still largely fragmented and showing inefficiencies in cross borders settlements. Complete integration between all CSD systems seems to be unlikely because of the multiple variables (such as currencies, none standardized market instruments and internal market policies) that need to be set between the different parties before interconnected infrastructures can be arranged. For the mean time, the resulting global infrastructure is a hybrid model of interconnected CSD and payment systems which according to several studies can pose a risk to the financial system.

III. Risks of Inter-banking Infrastructure

The post trade process can rise settlement risk. That is, the buyer of a market instrument is exposed to making a payment but not receiving the delivery. The seller of a market instrument is exposed to delivering but not receiving the payment. As a countermeasure, banks implement delivery versus payment (DVP) mechanisms.

Clearing and settlement systems can use one of three possible DVP mechanisms. In Model 1, systems settle transfer instructions for both, market instruments and payment, on a gross basis. The payment and transfer of the market instrument take place at the same time. In Model 2, systems settle market instrument transfer instructions on a gross basis whereas payment instructions are settled on net basis. The transfer of the market instrument takes place first and at a later time the payment is made. In Model 3, systems settle payment instructions on a gross basis whereas market instrument transfer instructions are settled on net basis. The payment takes place first and at a later time the transfer of the market instruments is made.

However, for DVP mechanisms to work, automated financial systems need to be interconnected otherwise they cannot

be implemented. Furthermore, even with DVP mechanisms present there is a possibility that the process is completed but an inappropriate procedure is performed by an insider user. This risk, known as operational risk, may result from inadequate or failed internal processes originated by authorised users. Operational risk is a current concern for banking institutions. Banking institutions through the Basel Committee on Banking Supervision, a working group composed of people from central banks and other banking institutions, address the problem in the risk management principles for electronic banking [23]. The problem is concerning in the e-trading scenario.

Unfortunately, the interconnection of inter-banking systems does rise other risks. The interdependence of clearing and settlement systems worldwide has increased the potential for disruptions to extend rapidly and broadly across systems [21] [6] [24]. Interdependencies can propagate from one system to another. For example, if a bank fails to settle a payment, the liquidity shortfall may be transferred to other banks which may also fail to make their payments. Therefore, any risk that threatens to affect the clearing and settlement process of one bank can affect the complete financial market.

IV. The Inter-Banking E-Trading Workflow Activity

Assuming a scenario where systems are not inter-connected the following gives a more detailed description about the e-trading activity.

Four systems are related to an e-trading activity:

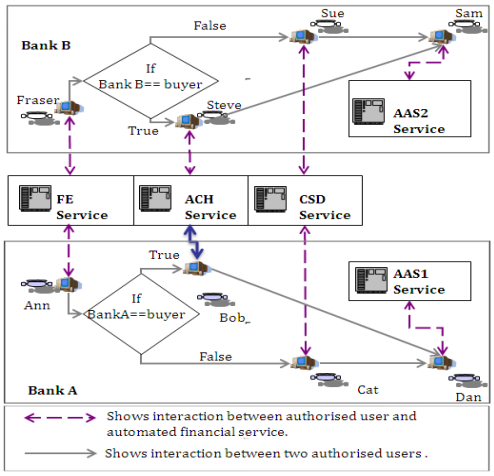

Fig. 4. Graphical Example of a workflow e-trading activity

- An electronic trading system, usually directly associated to an exchange, is where buyer and seller of market instruments are brought together through an exchange. The electronic trading system is usually known as a Financial Exchange (FE) and the process is known as the execution step.
- An electronic Central Security Depository system (CSD) is where an entry book is kept to maintain trace of the ownership of a market instruments. It is also where the exchanges of the market instruments takes place.
- An electronic payment system, usually known as an Automated Clearing House (ACH), is where electronic payments take place.
- An electronic Automated Accounting System (AAS) is where settled settled market instruments and payments are registered.

Each of the above automated financial systems have users which could be insider users. For example, assume that Ann, Bob, Cat, and Dan are employees from Bank A (See Fig 4). Each employee has an assigned job and is a user of one of the systems. Ann is a trader at the front office[1] and her job is to negotiate securities (market instruments) in an electronic financial exchange (FE). A negotiation can end up with an agreement to either buy a market instrument or to sell a market instrument. Bob and Cat both work in the back office[2]. If Ann's agreement is to buy a market instruments then Bob will make the payment making use of the ACH system. If Ann's agreement is to sell a market instrument then Cat will ensure that the market instrument is passed on to the new owners by changing the ownership details using the electronic CSD system. Finally, any settlement should be registered in an Automated Accounting System. Usually, two books can be used for this purpose, one where only securities activities are registered and one where cash flow activities are registered. Here, for clarity, we assume that only one book is used and that all accounting activities are registered in the automated accounting system of each bank.

In the above e-trading activity there are two types of data flows. When two users, within the same financial institution, interact to fulfil an obligation we say there is a horizontal data flow. For example, when Ann asks Bob to pay Bank B for a market instrument which has been bought by bank A a horizontal data flow is said to be generated. When a user of a financial service interacts with the service in order to fulfil an obligation we say there is vertical data flow. For example, when Bob pays Bank B for a market instrument which has been bought by Bank A. The interactions depicted in all horizontal and vertical data flows is what we call a complete workflow.

V. An Analysis of a Security Problem in an E-Trading Scenario

The problem with the above activity is that the horizontal data flow is usually conducted manually because inter-banking automated financial systems are not inter-connected. In such circumstances, an employee can change or manipulate data within the data flow of information causing what is known as an integrity drift. This poses a risk to the integrity of the entire transaction set. The data flow between two users can be manipulated unintentionally or maliciously by an authorized user i.e. by an employee who has been assigned privileges to use an electronic system.

[1]Department of a financial institution where business is initiated
[2]Department of a financial institution in charge of trade processing and settlements

Several scenarios are possible in the example depicted in Fig 4:

- Ann may alter her report before it is passed on to Bob and as a result, Bob would be performing a transaction that has already been modified.
- Bob may receive a truthful report from Ann but alter it when performing the transaction.

Although the above is not a usually reported scenario, it is true that rogue traders have been reported to present performed financial transactions different from wht they where supposed to have been.

- Jack may impersonate Ann or Bob to perform transactions on their behalf by making use of their user name and password.

Furthermore, the following factors may make these wrongdoings more difficult to detect.

- Ann and Bob are both authorized users.
- Institutional arrangements on settlements worldwide, despite globalisation, remain fragmented along national borders, thus, making cross border e-trading activities complex. Cross-country settlement problems can arise due to factors such as:
  - Time differences between countries
  - Currency differences of different countries, which require conversion processes.
  - Settlement arrangements for different types of securities.
  - Differences regarding regulations.
- The volume of daily transactions in a financial exchange, that is, a vertical data flow, is usually very high. The London Stock Exchange Group, for example, reached a record 29.6 million in October 2008. The average daily number of trades per month reached to 1.3 million, and the average daily value traded was £10.7 billion (€13.6 billion) [7].
- The automated financial systems, where most of the e-trading activities takes place, may be independent of each other. Therefore there is no automated reconciliation of all the financial transactions generated by an e-trading activity with those reported to executives of a financial institution.

As long as authorised users are able to manipulate reports on e-trading activity, as long as there is no auditing system capable of tracing the complete workflow of all transactions, financial institutions will be vulnerable to authorised users.

VI. The proposed solution

Here we present the Agent Based Distributed Workflow Oriented Auditing Architecture (ADA^2). The aim of ADA^2 is to enable the detection of an integrity drift during the e-trading workflow activity. In order to achieve this aim, the objective of ADA^2 is to construct, and monitor workflow oriented auditing log files, which we have named Automated Banking Certificates.

A. Main Design Requirements

The following are defined as design requirements for ADA^2:

- A collaborative environment: an environment in which a group of parties can work in collaboration to achieve the same goal (a workflow oriented auditing system).
- A distributed environment: an environment in which the auditing process can be split to run separately in different computers.
- A dynamic environment: an auditing environment which can be constructed between any two banks.

In addition, the following assumptions are made:

- Financial transactions in the workflow are performed in a defined sequence. That is, a financial transaction recorded in the ACH_System is assumed to be recorded after a financial transaction recorded in the FE_System. A financial transaction recorded in the CSD_System is assumed to be recorded after a financial transaction recorded in the ACH_System.
- Users from Bank A can see who is the counterpart trader bank which they made a deal with. Therefore, they make payments and transfer the market instrument directly to the counterpart bank.

B. Main Components

ADA^2 has two main components: ABCs and software agents. An ABC is a workflow oriented audit data structure, which was first introduced in . A software agent is a self contained software. It takes input data and performs a defined task. Software agents can act in an autonomous way on behalf of another party. A software agent is used to perform a role within a business process. Agents in a multi-agent environment can operate and interact with each other. They are usually used to accomplish a business process. In ADA^2, there are two types of software agents: the SP_Agent(s) located in the automated financial services and User_Agent(s) located at the client PC of a user of each automated financial service.

C. High Level Overview

ADA^2 has three actors (see Fig 5 for the corresponding use case diagram):

- SP_Agent represents a software agent associated with an automated financial service. For example, the software agent at the FE automated financial service is called the FE_SP_Agent. The software agent at the ACH automated financial service is called the ACH_SP_Agent. The software agent at the CSD automated financial service is called the CSD_SP_Agent. An SP_Agent retrieves key data from a financial transaction recorded at an automated financial service, constructs an Intra-system ABC (Ia_ABC), i.e. an audit log file, for the transaction and then delivers the ABC to a User_Agent.
- User_Agent represents a software agent that can cross-check and verify the authenticity of an Intra-system ABC. It runs a transaction authentication process to verify the authenticity of Intra-system ABCs recorded in an e-trading workflow. It constructs and signs Inter-system

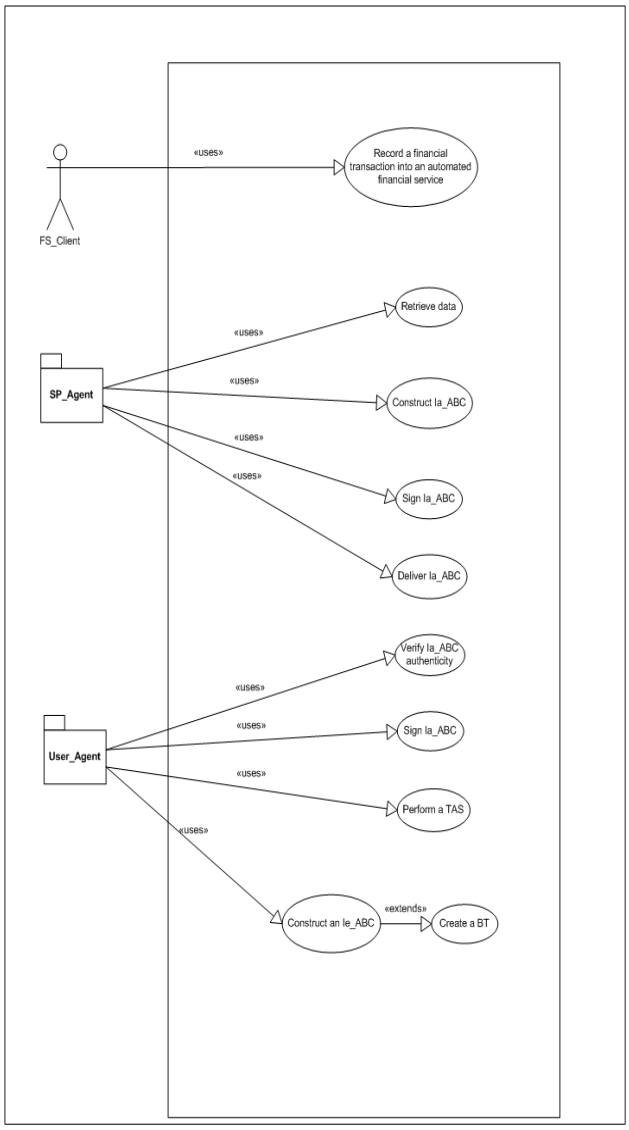

Fig. 5. Use case diagram

ABCs. Finally, it delivers Inter-system ABCs to other $User\_Agents$ within the same Bank. Each client PC used by a user of an automated financial service hosts one $User\_Agent$. The $User\_Agent$ which lays on Ann's PC is called $FE\_User\_Agent_{Ann}$. The agent in Fraser's PC is called the $FE\_User\_Agent_{Fraser}$. The agent in Steve's PC is called $ACH\_User\_Agent_{Steve}$. The agent in Bob's PC is called the $ACH\_User\_Agent_{Bob}$. The agent in Sue's PC is called $CSD\_User\_Agent_{Sue}$. The agent in Cat's PC is called $CSD\_User\_Agent_{Cat}$.

- FS_Client represents a person from a Bank which has the privileges to perform inter-banking financial transactions in one of the automated financial systems, i.e. FE, ACH or CSD system.

D. Detailed Description

Processes in ADA^2 are performed by each actor in an asynchronous way. The sequence of the processes associated to the FE, ACH, CSD are depicted in Fig 6 respectively, Fig 7 and Fig 8.

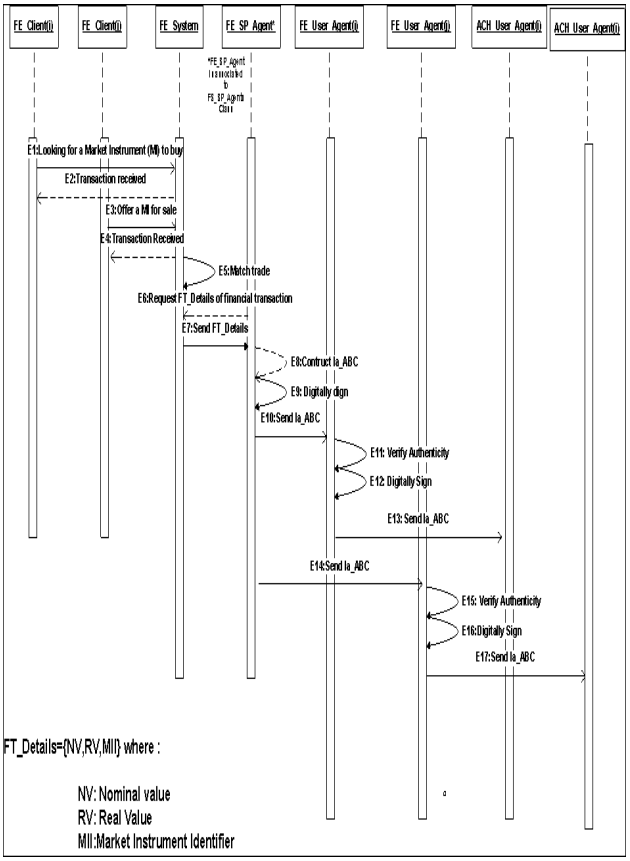

Fig. 6. Sequence diagram of ADA^2 associated to FE

Fig 6 shows the sequence of processes in ADA^2 with which the FE system is associated (in terms of our defined scenario).

- E1: FE_Client (i), that is a user from Bank A, introduces into the FE_System the terms in which he would like to make an inter-banking e-trading deal to buy a Market Instrument.
- E2: The FE_System registers the request.
- E3: FS_Client (j), that is a user from Bank B, introduces into the FE_System the terms in which he would like to make an inter-banking e-trading deal to sell a Market Instrument.
- E4:The FE_System registers the requirement.
- E5: The terms and conditions of the FS_Client (i) match with those of the FS_Client (j). Therefore, the FE_System creates a deal.
- E6: The FE_SP_Agent detects the new deal and requests the details of the financial transaction.
- E7: The details of the financial transaction are delivered to the FE_SP_Agent upon request.

- E8: The FE_SP_Agent issues a new Ia_ABC$_{FE}$ (Intra-system ABC) audit log file using the data of the financial transaction retrieved from the FE_System.
- E9: FE_SP_Agent signs the Ia_ABC$_{FE}$.
- E10: The FE_SP_Agent sends the Ia_ABC$_{FE}$ to the FE_User_Agent(i)
- E11: FE_User_Agent(i) verifies the signature contained in Ia_ABC$_{FE}$.
- E12: Upon successful verification of Ia_ABC$_{FE}$, FE_User_Agent(i) signs Ia_ABC$_{FE}$.
- E13: FE_User_Agent(i) sends Ia_ABC$_{FE}$ to ACH_User_Agent(i).
- E14: The FE_SP_Agent sends the Ia_ABC$_{FE}$ to the FE_User_Agent(j)
- E15: FE_User_Agent(j) verifies the signature contained in Ia_ABC$_{FE}$.
- E16: Upon successful verification of Ia_ABC$_{FE}$, FE_User_Agent(j) signs Ia_ABC$_{FE}$.
- E17: FE_User_Agent(j) sends the Ia_ABC$_{FE}$ to ACH_User_Agent(j).

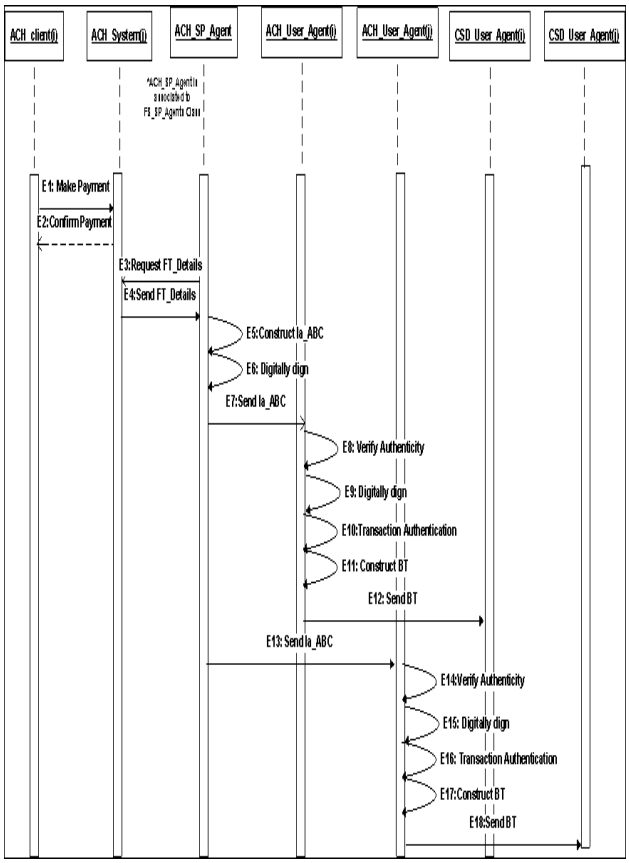

Fig. 7. Sequence diagram of ADA^2 associated to ACH

Fig 6.3 shows the sequence of processes in which the ACH system is associated.

- E1: ACH_Client (i) pays for the market instrument using the ACH_System.
- E2: The ACH_System makes the required payment, and confirms that the process has been completed.
- E3: The ACH_SP_Agent detects the payment and request the details of the financial transaction.
- E4: The details of the financial transaction are delivered to the ACH_SP _Agent upon request.
- E5: The ACH_SP_Agent issues a new Ia_ABC$_{ACH}$ (Intra-system ABC) audit log file using the data of the financial transaction retrieved from the ACH_System.
- E6: ACH_SP_Agent signs the Ia_ABC$_{ACH}$.
- E7: The ACH_SP_Agent sends the Ia_ABC$_{ACH}$ to the ACH_User_Agent(i).
- E8: ACH_User_Agent(i) verifies the signature contained in Ia_ABC$_{ACH}$.
- E9: Upon successful verification of Ia_ABC$_{ACH}$, ACH_User_Agent(i) signs Ia_ABC$_{ACH}$.
- E10: ACH_User_Agent(i) takes the newly received Ia_ABC$_{ACH}$ and runs the Transaction Authentication Service with Ia_ABC$_{FE}$. That is to say that the Transaction Authentication Service is used to detect the FE financial transactions that triggered the ACH_Client(i) to make the payment.
- E11: After identifying the matching Ia_ABC$_{FE}$ and the Ia_ABC$_{ACH}$, the FE_User_Agent$_i$ will construct an Inter-system ABC. The new Inter-system ABC is bound to the two directly related Intra-system ABCs, i.e. BT$_{FE-ACH_i}$.
- E12: ACH_User_Agent$_i$ sends BT$_{FE-ACH_i}$ to CSD_User_Agent$_i$.
- E13: The ACH_SP_Agent sends the Ia_ABC$_{ACH}$ to the ACH_User_Agent(j).
- E14: ACH_User_Agent(j) verifies the signature contained in Ia_ABC$_{ACH}$.
- E15: Upon successful verification of Ia_ABC$_{ACH}$, ACH_User_Agent(j) signs Ia_ABC$_{ACH}$.
- E16: ACH_User_Agent(j) takes the newly received Ia_ABC$_{ACH}$ and runs the Transaction Authentication Service with Ia_ABC$_{FE}$. That is to say that the Transaction Authentication Service is used to detect the FE financial transactions that triggered the ACH_Client(i) to make the payment.
- E17: After identifying the matching Ia_ABC$_{FE}$ and the Ia_ABC$_{ACH}$, the FE_User_Agent$_j$ will construct an Inter-system ABC. The new Inter-system ABC is bound to the two directly related Intra-system ABCs, i.e. BT$_{FE-ACH_j}$.
- E18: ACH_User_Agent$_j$ sends BT$_{FE-ACH_j}$ to CSD_User_Agent$_j$.

Fig 6.4 shows the sequence of processes in which the ACH system is associated.

- E1: CSD_Client (i) requests the transfer of a market instrument by using the CSD_System.
- E2: The CSD_System makes the required transfer. It confirms the transaction was successfully performed.
- E3: The CSD_SP_Agent detects the transfer and request the details of the financial transaction.
- E4: The details of the financial transaction are delivered to the CSD_ SP_Agent upon request.

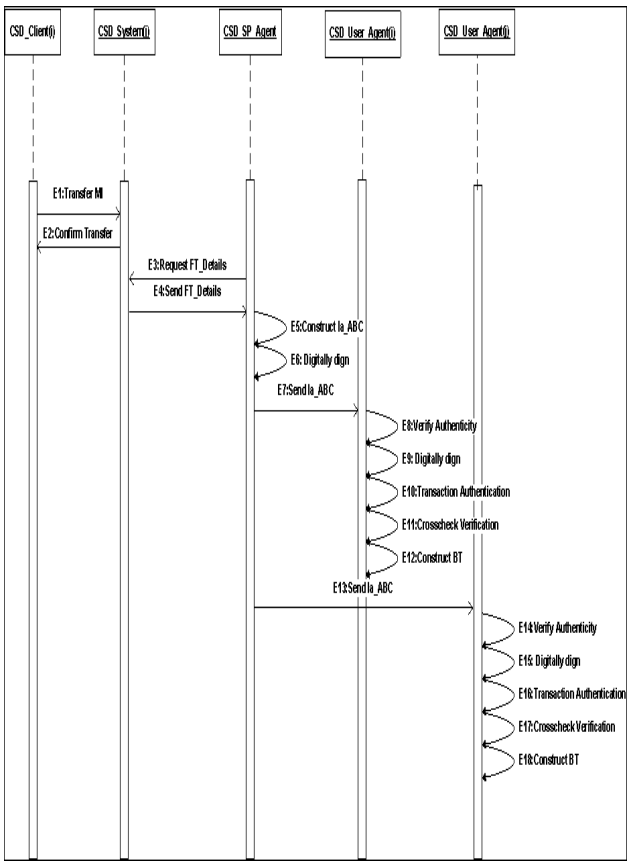

Fig. 8. Sequence diagram of ADA^2 associated to CSD

- E5: The CSD_SP_Agent issues a new Ia_ABC$_{CSD}$ (Intra-system ABC) audit log file using the data of the financial transaction received from the CSD_System.
- E6: CSD_SP_Agent signs the Ia_ABC$_{CSD}$.
- E7: The CSD_SP_Agent sends the Ia_ABC$_{CSD}$ to the CSD_User_Agent(i).
- E8: CSD_User_Agent(i) verifies the signature contained in Ia_ABC$_{CSD}$.
- E9: Upon successful verification of Ia_ABC$_{CSD}$, CSD_User_Agent(i) signs Ia_ABC$_{CSD}$.
- E10: CSD_User_Agent(i) takes the newly received Ia_ABC$_{CSD}$ and runs the Transaction Authentication Service in order to find the Ia_ABC$_{FE}$ in the BT$_{FE-ACH_i}$ that is associated to it. That is to say that the Transaction Authentication Service is used to detect the FE-ACH financial transactions that triggered the CSD_Client(i) to make transfer of the market instrument.
- E11: CSD_User_Agent(i) performs a crosscheck verification of the information contained in Ia_ABC$_{CSD}$ to that in the Ia_ABC$_{CSD}$ of BT$_{FE-ACH_i}$.
- E12: After identifying the matching Ia_ABC$_{FE}$, Ia_ABC$_{ACH}$ and the Ia_ABC$_{CSD}$ the CSD_User_Agent(i) will construct an Inter-system ABC. The new Inter-system ABC is bound to BT$_{FE-ACH_i}$ into a Merkle Hash Tree structure, i.e. BT$_{FE-ACH-CSD_i}$.
- E13: The CSD_SP_Agent sends the Ia_ABC$_{CSD}$ to the CSD_User_Agent(j).
- E14: CSD_User_Agent(j) verifies the signature contained in Ia_ABC$_{CSD}$.
- E15: Upon successful verification of Ia_ABC$_{CSD}$, CSD_User_Agent(j) signs Ia_ABC$_{CSD}$.
- E16: CSD_User_Agent(j) takes the newly received Ia_ABC$_{CSD}$ and runs the Transaction Authentication Service in order to find the Ia_ABC$_{FE}$ in the BT$_{FE-ACH_i}$ that is associated to it. In other words, the Transaction Authentication Service is used to detect the FE-ACH financial transactions that triggered the CSD_Client(i) to make the transfer of the market instrument.
- E17: CSD_User_Agent(j) performs a crosscheck verification of the information contained in Ia_ABC$_{CSD}$ to that in the Ia_ABC$_{FE}$ of BT$_{FE-ACH_j}$ to see that they match.
- E18: After identifying the matching the Ia_ABC$_{FE}$, the Ia_ABC$_{ACH}$ and the Ia_ABC$_{CSD}$ the CSD_User_Agent(j) will construct an Inter-system ABC. The new Inter-system ABC is bound to BT$_{FE-ACH_i}$, i.e. BT$_{FE-ACH-CSD_j}$.

This resulting data structure is a complete ABC.

VII. Conclusions

We have presented current e-banking infrastructure, and described the existence of tight inter-relationships between financial services. This new emerging interdependence worldwide has increased the potential for disruptions to extend rapidly and broadly across systems. Based on the above new inter-institutional oriented security controls are required to be able to detect insider abuse.

Here we present the Agent Based Distributed Workflow Oriented Auditing Architecture (ADA^2). A security solution which tackles the problem of integrity drifts within an e-trading scenario. The audit data structure constructed within this architecture holds the evidence of a complete set of transactions related to one e-trading deal. We hope we can present very soon the prototype of the Agent Based Distributed Workflow Oriented Auditing Architecture (ADA^2).

The model presented here is a simplified version of inter-banking workflow activity. A more complex scenario can be defined to improve the current proposed security solution. For example, some e-trading entities do not allow their counterpart to know their identities.

References

[1] Bank for International Settlements: Risk Management Priciples for electronic Banking found at www.bs.org/publ/bcbs98.htm on January 2006
[2] Corzo, C.,Zhang, N.: Towards a real-time solution to the security threats posed by authorised insiders, Proceedings of the ECIW 2004: The 3rd European conference on information warfare and security, Royal Holloway, University of London, UK, (2004) 51–60
[3] David, L., Graeme B.: Managing Technology in the Operations Function, Securities Institute, ISBN 0 7506 5485 6, 2002
[4] Group of Ten, Report on Consolidation in the Financial Sector, Bank of International Settlements, International Monetary Fund Organization for Economic Co-operation and Development, www.bis.org, 2001

[5] David Folkerts-Landau, Peter Garber, and Dirk Schoenmaker, The Reform of Wholesale Payment Systems, The World Bank, Finance and Development, pages 25-28, June 1997
[6] CPSS Group, Statistics on payment and settlement systems in selected countries, Committee on Payment and Settlement Systems-Bank of International Settlements, pages 1-331, ISBN 92-9131-679-2, 2008
[7] The London Stock Exchange, www.londonstockexchange.com/NR/exeres /D28B12F2-E15C-4FC8-93AE-CB4E31DC898E.htm, Electronic Order Book Trading Grows 33 Per Cent During March, cited April 2009, 7th April 2008
[8] Ranee Jayamaha, Impact of IT in the Banking Sector, BIS Review 13, 2008
[9] Robert Richardson, CSI Director, CSI Computer Crime & Security Survey, http:gocsi.com, 2008
[10] Robert Richardson , CSI Director, CSI Computer Crime & Security Survey, http:gocsi.com, 2009
[11] Helen Allen and John Hawkins and Setsuya Sato, Electronic trading and its implications for financial systems, BIS papers No 7, pages 30-52, 2008
[12] Ben Bernanke, Regulation and financial innovation, BIS Review 49, pages 1-5, 2007
[13] Timothy Geithner, Challenges facing the global payment systems, BIS Review 59, pages 1-5, 2004
[14] Committee on Payment and Settlement Systems (CPSS) - Bank for International Settlements, Real-time gross settlement systems, Publication No 22, www.bis.org, March 1997
[15] Board of Governors of the Federal Reserve System, FEDWIRE FUNDS TRANSFER SYSTEM - Assessment of Compliance with the Core Principles for Systemically Important Payment Systems, www.federalreserve.gov/paymentsystems/files/fedfunds _coreprinciples.pdf, March 2009
[16] Paras Verma, FCHIPS:Clearing House Inter-Bank Payment Systems, http://knol.google.com/k/paras-verma/chips /3mh4aumwkgjuc/3, accessed on October 2009, July 2008
[17] Dan Zhu, Security Control in Inter-bank Fund Transfer, Journal of Electronic Commerce Research, V3, pages 15-22, 2002
[18] FIN Copying Services, www.swift.comsolutions...SWIFT_MS_ FIN_ copying_services_200808.pdf, FIN Copying Services, cited April 2009, 2008
[19] Torsten Schaper, Integrating the European Securities Settlement, IFIP International Federation for information processing 2009, 385-399, 2009
[20] Committee on Payment and Settlement Systems (CPSS) - Bank for International Settlements, www.bis.org, Payment and settlement systems in selected countries - CPSS Red Book, cited April 2009, April 2003
[21] Committee on Payment and Settlement Systems (CPSS) - Bank for International Settlements, www.bis.org/publ/cpss84.htm, The interdependencies of payment and settlement systems - CPSS - Publications No 84, cited October 2009, June 2008
[22] Francis Braeckevelt, Clearing, settlement and depository issues, Bank of International Settlements , BIS paper No 30, pages 284-332, November 2006
[23] Committee on Payment and Settlement Systems (CPSS) - Bank for International Settlements, Risk Management Principles for Electronic Banking, www.bis.org, accessed on October 2009, 2003
[24] Francis Braeckevelt, Clearing, settlement and depository issues, Bank of International Settlements, BIS paper No 30, pages 284-332 , November 2006
[25] Linda Goldberg and John Kambhu and James Mahoney and Asani Sarkar, Securities Trading and Settlement in Europe: Issues and Outlook , Current Issues in Economic and Finance-Federal Reserve Bank of New York, V8, 4, pages 1-2 , 2002