A Test Bed for Data Hiding in Financial Transactions

Dylan Leigh [s3017239] <dylan.leigh@rmit>

Supervisor: Dr Ron van Schyndel
RMIT CS&IT Summer Studentship Project

***Abstract*—**

The aim of this project is to develop a framework to allow experiments with data hiding in financial transactions, and for detecting the use of information hiding in financial transactions.

An analysis is made of electronic funds transfer systems in use within Australia, particularly those used for direct credit transactions. A model of financial transaction networks based on Australian systems is developed and a simulator framework which implements the model described is developed for conducting further research. Several example data hiding techniques and scenarios are presented.

I. Introduction

Much research has been recently been conducted on covert financial networks operating over covert channels, but there is little if any research on using standard financial networks as a medium for covert channels. The aim of this project is to develop a framework to allow experiments with data hiding in financial transactions, and detecting the presence of this hidden data.

Covert channels in financial networks can be used for many purposes including both money laundering and money laundering detection.

It is necessary for this project to model individual transactions to add the covert channel or watermark to them. This "bottom-up" approach is different to many existing financial network models which use an aggregate, graph based model to analyze the flow of funds.

II. Review of Financial Networks

Most of the early work on this project involved an in depth analysis of existing financial networks to find channels which can be used for data hiding. The systems operated by Australian Payments Clearing Association (APCA) and the Society for Worldwide Interbank Financial Telecommunication (SWIFT) were examined as they are the dominant Australian and International financial networks.

Seven financial networks were analyzed; three APCA networks which focus on high volume, low value transactions were examined in detail (these transactions are most useful for data hiding). These networks operate by transferring files across "Infrastructure Systems" - three of these were analyzed.

Many details of these systems are classified and are only available to members of APCA (i.e. the financial institutions connected to the systems). Access to the classified sections was unavailable, however some classified details are possible to determine from references in the unclassified sections.

III. Model

Based on the analysis of APCA and other financial networks, a 4 layer model for financial network simulation has been developed.

The *Infrastructure Layer* specifies the general format and transmission of files, to allow them to be inter-operated by the other layers. The *Operations Layer* specifies operations which can be performed on records and files. The *Protocol Layer* specifies a number of financial network protocols. Protocols are defined in terms of their operations. The *Node Layer* determines the parties involved in the simulation by defining a set of nodes (banks, customers, etc) and the other nodes they interact with (using one or more protocols).

IV. Simulator

The simulator is designed around the exchange of files containing transaction records (similar to the APCA protocols).

Initially, a prototype version was developed in Python which used a hard-coded algorithm and contained only three programs: a transaction generator, an insertion operation and an extraction operation.

Once the concept and program was shown to be feasible the existing modular simulator was then developed, which supports six operations and plug-in modules for the data hiding algorithm. Three simple algorithm modules were developed for this project as a proof of concept. It is anticipated that developing more cryptographically advanced modules will be a significant component of future research.

V. Challenges

There were three significant difficulties encountered working on this project:

The APCA documentation was in total over 1200 pages, written using unfamiliar legal and financial terminology and many sections were classified. This made analysis of the protocols a difficult and time consuming task.

Literature searches for covert channels in finance were complicated as this is a new area of research. Financial networks and money laundering detection research is constantly evolving as well - some of the references used were released in January 2012.

Real transaction data - even anonymized transaction data - could not be obtained, as it is considered proprietary information by financial organizations. Substantial work was involved in searching for this data, and in its absence, attempting to generate the most accurate random transactions possible.

VI. Applications

The main applications of covert channels are in money laundering detection and in money laundering itself. In the former case, watermarking techniques can be used to trace suspect transactions,and to determine the degree of separation between suspects.

Covert channels may be used by money launderers to communicate with each other (see example 1). In this case, further research would focus on steganographic analysis to detect the presence of hidden data and possible countermeasures to disrupt the channel.

Example 1.
Covert Channels for Money Laundering

Bob is part of a money laundering network (MLN). He runs a small retail shop. Bob's suppliers are also agents in the money laundering network.

Bob receives money from other members of the MLN who come to his shop as customers and pay him inflated prices for the merchandise. Bob transfers the dirty money on via inflated prices on his purchases to the suppliers. When Bob makes an order from these suppliers, he transfers the money using the "direct credit" or "wire transfer" service available from his bank.

The suppliers need to know who to pass the money on to, so Bob uses the cents value of the bank transfer to encode the the next recipient in the MLN. Amounts ending in 01 cents are transferred to Alice, amounts ending in 02 are transferred to Claire, amounts ending in 03 are transferred to David, and so on.

VII. Future Work

There are many areas which the simulator can be improved and features added:

- Algorithms and software for steganographic analysis of transactions.
- Simulation of special purpose financial networks (e.g. used for EFTPOS or cheque clearing).
- Support for unusual events such as transaction cancellation, bouncing/dishonour and failure to settle.
- Further data hiding algorithms and modules.
- More flexibility in the transaction generator and insert operation to allow tweaking the function of these programs.
- More realistic simulation of transaction time and date (this would require more data on real transactions).
- Advanced tools (possibly graph or flowchart based GUI tools) for constructing protocols and node networks.