Fraud Detection from a Business Perspective: Future Directions and Challenges

Ulrich Flegel[1] and Julien Vayssière[1] and Gunter Bitz[2]

[1] SAP Research Center Karlsruhe, Germany
[2] SAP Fraud Prevention Competence Center, Walldorf, Germany
{ulrich.flegel|julien.vayssiere|gunter.bitz}{@}sap.com

Abstract. This contribution summarizes the state of the art of fraud detection in practice and shows the relations between the technology for fraud detection and intrusion detection. We identify prospective directions for further investigation and imminent challenges.

1 Introduction

With the introduction of IT to conduct business we accepted the loss of a human control step. For example, orders would leave the company electronically and fully automated, with no human intervention. For this reason, the introduction of new IT systems was accompanied by the development of the authorization concept. That is why it is of paramount importance that due care is exercised in analyzing this system for risks and then minimizing them. This is, of course, also supported by software nowadays. But since, in reality, there is no such thing as 100 per cent security; auditors are commissioned to examine all transactions for misconduct. Since the data exists in digital form already, it makes sense to use computer-based processes to analyze it. Such processes allow the auditor to carry out extensive checks within an acceptable timeframe and with reasonable effort. Once the algorithm has been defined, it only takes sufficient computing power to evaluate larger quantities of data.

2 State of the Art in Practice

The research community has come up with a number of different approaches over the years to the problem of fraud detection: data mining, machine learning, signature-based or anomaly detection. However, the state of the practice of fraud detection by professional auditors is very different: most of the tools used are simple tools for data import and analysis that leave the detection and classification of potential fraud cases entirely to the human being. In a recent survey, nearly half the auditors who responded reported using generic tools such as Microsoft Excel or Microsoft Access to do their work. This is clearly a sign that the current offering of Computer-Assisted Auditing Tools (CAATS) is not sufficient, and that existing research results have failed to transfer into usable tools for auditors.

We distinguish between generic, specialized and custom-built fraud detection tools. Studying the offers in detail, we realized that the seemingly primitive state of the field

Dagstuhl Seminar Proceedings 08302
Countering Insider Threats
http://drops.dagstuhl.de/opus/volltexte/2008/1795

can be explained by the fact that most of the advanced tools developed are either custom-built, and therefore very rarely publicized, or are used in very specialized solutions that, for commercial reasons, like to remain discrete on how exactly they achieve fraud detection. Another thing to keep in mind is that the target audience for fraud detection tool, i.e. fraud auditors, cannot be described as tech-savvy. As a result, it is hard to find people with the right combination of computer science expertise and auditing expertise to match the various approaches to the actual problems faced by auditors.

3 Relation to Intrusion Detection

An approach that has been tried in the past is to apply techniques developed for Intrusion Detection Systems (IDS) to the problem of fraud detection. The art and science of detecting intrusions and fraud in monitoring and transaction data has a history of over 25 years. We roughly distinguish 3 approaches of detection methods: (1) misuse detection, modelling the behavior to be detected (by specification) and matching the models to current behavior; (2) anomaly detection, modelling the normal behavior (by training) and detecting deviations from current behavior; (3) specification-based detection, modelling allowed behavior (by specification) and detecting deviations from current behavior.

All three approaches have been used for intrusion detection purposes and were applied to to lower level system concepts, such as network packets, system call sequences and parameters, as well as web application parameters. In the domain of fraud detection, anomaly detection techniques are mainly used to flag unusual behaviour that needs further manual examination, and misuse detection heuristics that are employed to detect known application level, domain-specific fraud schemes. Such solutions for fraud detection are by necessity highly specific to the application at hand and in extension also to the specific business model of the company and to its industry sector. Widely applicable solutions have currently not been developed.

We also argue that the detection of insider fraud is a very different problem from that of detecting intrusion at host or network level. One reason may be that attacks against networks are more automated and frequent than attempts at perpetrating fraud through enterprise information systems, which we believe show more variability. However, as networks attacks become more sophisticated, through polymorphic exploit code and multi-step attacks, and as fraudsters have the possibility to automate attacks by leveraging service-oriented architectures and business process engines, we could see the two types of attacks eventually converge. The fact remains, however, that we have very little data available to study patterns of fraud in enterprise systems.

3.1 Future Directions for Fraud Detection in SOA-enabled Business Processes

We intend to cross-fertilise both areas – intrusion detection and fraud detection – by addressing the gaps of missing specification-based methods for fraud detection, and for missing applications at the level of business processes. We propose investigating specification-based detection methods for detecting business process level fraud, where business services are orchestrated by means of Web Services SOA technology. This

approach bears the promise of low false positive and low false negative rates, while detecting previously unknown fraud schemes. Our novel idea involves exploiting the Web service description models developed during design-time in order to automatically generate specifications of allowed behaviour for fraud detection and possibly manually enrich them. In order to bridge the syntactic gap between incident situations detected during run-time and existing fraud models, an appropriate ontology is required. We propose to use the ontology to map the current incident situation to known fraud models to enable enriching the incident alarm with information.

4 Challenges

We would like to list a number of challenges faced today by the designers of fraud detection solutions, which we hope will help steer the community in the right direction.

The first challenge is to bridge the gap between existing fraud detection tools and the business level. We need tools that any auditor can use. Tools that the auditor can parameterize using concepts that make sense at a business, and tools that output potential fraud cases at the same level of abstraction.

Another challenge that appeared in the last decade is the increasing outsourcing of non-core functions of a company to external entities. Even if the legal frameworks in place extend auditing requirements to these outsourcing companies, lots of technical and sometimes legal barriers exist to cross-company fraud detection. Classical interoperability problems come in the way here, and even mundane issues of clock synchronization can cause headaches. In addition, data protection regulations on employee privacy laws sometimes restrain the scope of what can be done.

Finally, and this is more of a business issue than strictly a research one, the enterprise applications industry needs to lower the Total Cost of Ownership of detecting fraud in enterprises. We need to come to the point when installing and using anti-fraud tools pays for itself through the money recovered. This is not an inaccessible goal when one knows that, according to the American Association of Certified Fraud Examiners, companies loose on average 5% of their revenues to fraud.