ISMS insider intrusion prevention and detection

Richard E. Overill
Department of Computer Science, King’s College London, Strand, London WC2R 2LS, UK

Abstract

A wide variety of different techniques and technologies are potentially applicable for ISMS insider intrusion prevention and detection. In this report we examine three approaches that have not been reviewed in any great detail recently, namely: simulation and modelling, scenario gaming and game theory, and artificial learning technologies. We show how each of these diverse approaches might be applicable to particular corporate scenarios that may eventuate as a result of potential insider intrusions into an ISMS.

Keywords:
Insider intrusion
Simulation and modelling
Scenario gaming
Game theory
Economics of information security
Nash equilibrium
Artificial learning
Anomaly detection

1. Introduction and background

There are at least as many different reasons why a corporate stakeholder would attempt to perform a potentially intrusive action or series of actions upon a corporate information security management system (ISMS) as there are types of corporate stakeholder, since each type of stakeholder has a different perspective on the operation of the ISMS. As a consequence, the potentially intrusive activity may vary from benign (in the sense that the activity may not have been intentionally subversive, but may instead have been due to inattention or ignorance) on the one hand, through to malicious (in the sense that a deliberate attempt was made to subvert the intended operation of the ISMS) on the other.

It follows that a variety of distinctly different techniques and technologies would be likely to be useful in ISMS insider intrusion prevention and detection, more so than in the case of external intrusions or indeed in the case of general insider intrusions.

In this report we examine three such broad approaches which have not been reviewed in any great detail in the recent past: simulation and modelling, scenario gaming and game theory, and artificial learning technologies. We aim to demonstrate how each of these approaches might be applicable to particular scenarios that may eventuate as a result of potential insider intrusions into an ISMS.

2. Structure of an ISMS

An ISMS is defined in the information security management standard ISO 27001 (ISO, 2005) and comprises the systematisation of a number of information security management functions and processes. The different categories of stakeholder and their relationship to the ISMS can be described using the following diagram (Coles-Kemp, 2008).

The challenge for information security managers is that the stakeholder communities represented at the strategic, normative and operational layers of an ISMS are composed of a range of different professional teams, all of whom value information and its security in different ways, according to their view of the organisation. This is particularly challenging for information security managers because it implies that there is no single insider perspective and this means that the information security management processes have to be tuned in different ways to interact effectively with the different stakeholder communities. In Fig. 1 the security management processes are listed as education, anomaly detection, audit, management review and decision making. Each stakeholder community interacts with
These processes in different ways and this makes it extremely difficult for information security managers to identify whether one or more of these processes are malfunctioning.

This type of insider threat is significant for security management because an ISMS is designed to give an all-round view of an organisation and its information. The feeds to and from these processes, represented in Fig. 1 as FB.1.a, give the management its intelligence as to how effectively the security management structure is performing. Attacking these feeds, either by restricting or altering their output or input, could prove attractive to certain insider communities, particularly if the ISMS is felt to restrict operations or result in an unnecessary operational overhead. A compromise of one or more of these feeds, either intentionally or accidentally through poor design or execution, causes information security managers to become effectively partially sighted and less able to identify an attack of any kind. The categories of attack technique outlined in Sections 3–5 form the basis of approaches focused on modelling ISMS behaviour and comparing different models of ISMS. These techniques have particular resonance when part of the ISMS process is embedded into non-human stakeholder groups. Scenario gaming and game theory are particular techniques which have the potential to contribute to approaches for modelling an ISMS that includes third party, escrowed or outsourced service providers.

3. Simulation and modelling

Cohen was one of the earliest researchers to investigate the application of classical probabilistic simulation and modelling techniques to study intrusions into local or enterprise networks from the Internet. Given a particular network configuration and the probabilities of successful attacks upon each pre-defined network component, the simulations produced results for the effects of detection times and reaction times on defence success rates, the effects of defender strength on defence success rates, the inherently non-linear relationship between defender strength and defence success rates, and the effect on defence success rates of differing threat profiles. By adding in costs for the various processes within the simulation, the relationship between costs and expected losses was also studied, and the effects of applying various defence strategies were investigated (Cohen, 1998).

While Cohen’s simulation techniques were originally applied to external intrusions into a network, they are sufficiently general to be applicable to insider intrusions, and in particular to insider attempted intrusions into an ISMS. In this scenario the network architecture and its components are replaced by the ISMS architecture and its components; the various corporate stakeholders likewise replace the external intruders. The intrusion techniques, the associated costs, detection and reaction times, and the defence strengths must also be redefined appropriately for the ISMS scenario.

All simulation and modelling techniques are limited by the quantity and quality of the available data, by the metrics chosen and by the sensitivity of the results to variations in the free parameters of the model. This implies that the results of any simulation need to be validated either against analytical results for a simple system or against observations of a well-controlled real-world system. In the case of ISMS intrusions the inherent complexity of the system renders the former option nugatory. However, field observations of a substantial number of ‘live’ ISMS have recently been made by Coles-Kemp and this approach offers some promise for performing the required simulation validations (Coles-Kemp, 2008).
4. Scenario gaming and game theory

RAND Europe is commonly credited with inventing the techniques of scenario gaming (sometimes alternatively referred to as seminar gaming) but in reality these appear to have evolved from the war gaming exercises developed by its parent US company RAND. The essential characteristics of a scenario game may be summarised as follows. The participants operate in groups (or teams); the discussion is centred upon a specific future situation (the scenario); each group’s discussion is focussed towards specific questions they must address concerning the scenario, and/or specific decisions they must make regarding the scenario (RAND).

In the case of a scenario involving an insider attack on an ISMS, each team might represent one type of stakeholder and would consider both why and how that stakeholder might decide to interfere with the normal operation of the ISMS. It should be noted that seminar gaming does not set out to solve the problem; its primary aim is to understand the problem better, both in terms of enhanced depth and increased range of perspectives, so that a solution may emerge more easily and naturally at a later stage. Other promoters of scenario gaming in the context of cyber security include Fred Cohen & Associates (FCA).

Game theory is a much more mathematically rigorous and analytical topic than scenario gaming. A fundamental conceptual distinction in game theory exists between zero-sum games and non-zero-sum games. The former are characterised as non-co-operative or pure rivalry contests in which the extent of the loss suffered by player A is exactly counterbalanced by the gain accruing to player B. Zero-sum games were studied and essentially solved by von Neumann and Morgenstern (1944). The more difficult problem of non-zero-sum games, in which there is the possibility of co-operative rivalry with mutual gain, was studied and essentially solved by Nash (1950). In so doing he discovered the so-called Nash Equilibrium which is the state in which no player has an incentive to deviate from their chosen strategy since no player can choose a better strategy, given the strategy choices of the other players. The goodness of a chosen strategy is measured by the payoff received by the player using that strategy. The payoffs in a two-person game where each player has the choice of N strategies are usually defined in an $N \times N$ matrix, each entry of which is a dupe $(a,b)$ where $a$ represents the payoff for player A and $b$ is the payoff for player B when they play their respectively chosen strategies. If the various payoffs are considered as economic incentives (positive payoffs) or disincentives (negative payoffs) then players will co-operate as required in order to maximise their individual payoffs.

Game theory together with market analysis and related techniques has encouraged the recent development of the economics of information security, promoted by a series of annual international Workshops on the Economics of Information Security (WEIS, 2002; WEIS, 2003; WEIS, 2004; WEIS, 2005; WEIS, 2006; WEIS, 2007; WEIS, 2008). In the context of information security engineering in general, a contest between an intruder and a defender can be regarded as a two-player game with various available intrusive and defensive strategies, and an accompanying payoff matrix. Similarly, insider intrusions into an ISMS can be viewed as a game between $S$ stakeholders where each stakeholder possesses at least one intrusive strategy along with one or more defensive strategies. The crux of the problem is then to construct the entries in the $S$-dimensional payoff matrix in such a way that all the stakeholders find that their individual payoffs are maximised by employing only non-intrusive strategies. That is, the Nash Equilibrium for the system (ISMS plus stakeholders) is attained by the use of co-operative strategies.

5. Artificial learning technologies

The detection of (internal or external) intrusions can be viewed as a form of anomaly detection. A number of artificial learning technologies have been applied with some degree of success to various real-world anomaly detection problems under the auspices of the UK government’s former DTI Management of Information research programme (DTI-MI) between 2000 and 2005. The projects included several examples of detecting either internal or external financial fraud in public sector and private sector organisations.

Provided that an adequate description of normal or expected behaviour can be supplied or acquired, it should be possible to detect any anomalous behaviour in terms of significant deviations from the expected behaviour. A number of computational methodologies have been developed which aim to detect anomalous behaviour in this manner. These include artificial immune systems (AIS), artificial neural networks (ANN), Bayesian belief networks (BBN), classifier systems (CS), case based reasoning (CBR), genetic algorithms (GA), stepwise linear regression (SLR), and support vector machines (SVM).

The foregoing remarks conceal an important distinction between two types of anomaly detection by means of artificial learning technologies: supervised versus unsupervised learning. In the former case, a sizeable sample which is guaranteed to consist solely of normal or expected behaviour is available at the outset, and the system then learns on the basis of this sample how to classify all subsequent instances of behaviour. In the latter case, no sample of normal or expected behaviour is available at the outset, so the system has to acquire knowledge of what constitutes normal behaviour by some other means. One such possibility is by initially assuming that some fraction of the data represents normal behaviour and then gradually revising this assumption in the light of the data subsequently encountered. It goes without saying that the logical converse also applies: in the (unlikely) event that a sizeable sample of purely anomalous behaviour is available a similar process of discriminate on can be performed. Clearly, unsupervised learning is a significantly more complex task than supervised learning.

In the case of retail sector insider fraud detection by means of an AIS in conjunction with association rule mining (ARM) technology (Kim et al., 2003), no defining sample of normal behaviour was available at the outset and consequently the unsupervised learning paradigm had to be employed. In this case, although the AIS was able to highlight a number of anomalous transactions for scrutiny by forensic accountants, the complexity of the transaction data sets (as measured by
within the context of an AIS (Ong, 2007). The use of AIS in and confidence of mined association rules when employed to AIS have defined many of the restrictions on the support critically reviewed recently (Overill, 2007).

If the above experience is translated into the problem domain of detecting insider attacks on an ISMS two issues become apparent. Firstly, it is likely to be an unsupervised (and hence difficult) learning task; secondly, it may not be possible to capture and process the multifaceted detail and complexity associated with all the interactions within fully operational ISMS and its stakeholders. However, a simplified model of the ISMS together with its stakeholders should be feasible for most if not all of the artificial learning technologies mentioned above, provided that all the crucial ISMS components and interactions are retained during the simplification process.

6. Summary and conclusions

Each of the three broad classes of techniques considered in this article, namely simulation and modelling, scenario gaming and game theory, and artificial learning technologies may well have an important role to play in the detection and/or prevention of insider attacks on an ISMS. However, at the present time none of these techniques has been explored in any depth or detail in this particular context, and further research in this direction would appear to be well motivated. This is especially significant as the trend of increasing dependence by global enterprises upon their ISMS infrastructures (including the stakeholders) continues to accelerate over time.

Acknowledgement

The author is grateful to Lizzie Coles-Kemp for many constructive comments and suggestions.

REFERENCES

CIFD. Available from: http://www.dcs.kcl.ac.uk/staff/richard/CIFD_final_report.doc; 2003 [accessed 15.08.08].

DTI-MI, Available from: http://www.dti.gov.uk/dti-mi/ [accessed 15.08.08].
FCA, Available from: http://all.net/games/index.html [accessed 15.08.08].
von Neumann J, Morgenstern O. The theory of games and economic behavior; 1944; Princeton University Press, Ch.3.
RAND, Available from: http://www.rand.org/ranendeurope/research/ipu/ [accessed 15.08.08].
WEIS. Available from: http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/; 2002 [accessed 15.08.08].
WEIS. Available from: http://www.cpppe.umd.edu/rhsmith3/; 2003 [accessed 15.08.08].
WEIS. Available from: http://www.dtc.umn.edu/cgi-bin/seminars.php?eventdesc=207; 2004 [accessed 15.08.08].
WEIS. Available from: http://infosecon.net/workshop/index.php; 2005 [accessed 15.08.08].
WEIS. Available from: http://weis2006.econinfotec.org/; 2006 [accessed 15.08.08].

Richard E. Overill obtained his PhD at the University of Leicester, UK. He joined the faculty of the Department of Computer Science, King’s College, University of London in 1987.

He has published over 75 refereed papers in international journals and conference proceedings covering topics in computational science, algorithmetrics, performance analysis, and information assurance.

His current research interests focus on ISMS security, anomaly/abnormality detection (including fraud detection, intrusion detection and terrorism detection); cyber-crime and cyber-forensics. He was PI for the UK DTI/EPSRC Management of Information project Computational Immunology for Fraud Detection (CIFD) 2000–2003, in collaboration with Royal Mail Group and Anite Public Sector. He has undertaken consultancy work for BAE Systems and UK MoD, and currently holds a Partnership Award in digital forensics from ICUK.