AUTONOMIC FRAMEWORK FOR IT SECURITY GOVERNANCE

Sitalakshmi Venkatraman

School of Engineering, Construction and Design (IT), Melbourne Polytechnic, Australia,

ABSTRACT

With the recent service enhancements over the Internet, organisations are confronted with a growing magnitude of security intrusions and attacks. Current intrusion detection strategies have not been effective in the long term, as new and obfuscated security attacks keep emerging evading the surveillance mechanisms. With information technology (IT) playing a pivotal role in today's organizational operations and value creation, security regulatory bodies have identified this situation not solely as a technology issue, rather due to the weakness of an organisation's risk management practices and IT governance. Hence, recent attention has embarked on formulating proactive IT security governance for organisational sustenance. This paper proposes an autonomic framework for IT security governance that postulates a self-learning adaptive mechanism for an effective intrusion detection and risk management. Such a framework would facilitate autonomic ways of integrating existing context-dependent knowledge with new observed behaviour patterns gathered from network as well as host for detecting unknown security attacks effectively using mobile agents. In addition, this paper provides a roadmap for autonomic IT security governance by applying the proposed framework The roadmap employs a continuous improvement feedback loop. for achieving the targeted quality of service (QoS) in an organisation.

KEYWORDS

IT Security Governance, Intrusion Detection, Autonomic Framework, Self-learning & Mobile Agents

1. INTRODUCTION

Over the last years, information technology (IT) revolution has taken a steep growth with Internet providing a plethora of services for users worldwide. IT has emerged as the major driving factor of economic sustainability by supporting everyday business operations in every organisation. However, business services over the Internet face exceedingly increasing security attacks that are unknown and undetected by regular security solutions. Information security experts, researchers and businesses confront a stumble block when they encounter a new malicious attack [1][2][3]. Recent intrusions have successfully evaded from the radar of security solutions stealthily and have affected businesses with huge payouts [4][5][6]. Organisations are now increasingly required to take a closer examination of their IT security strategies for business sustainability.
Current intrusion detection systems (IDS) are aimed at identifying vulnerabilities and protecting the information assets of an organisation from malicious attacks [7]. To achieve this goal, existing IDS predominantly adopt signature-based techniques (e.g. matching known virus code patterns) and behaviour-based techniques (e.g. detection of anomalies) [8][9]. In addition, some tools perform data mining methods or collect alert data for further action by human security experts [10]. However, such systems, whether adopting Network Intrusion Detection Systems (NIDS) or Host Intrusion Detection Systems (HIDS), are caught unaware when a new wave of attack affect the systems [11] [12]. They seldom support the recognition of intrusions that are obfuscated with no previous known patterns of signature or behaviour that attackers employ to evade detection.

A persistent monitoring tool of the networks and computer systems could lead to performance trade-offs in the quality of service of day-to-day business operations that are increasing integrated

DOI : 10.5121/ijmit.2017.9301

with IT. With technological advancement, specific platform-based detectors are also being developed, such as hardware checks to determine if a particular operating system kernel is maliciously modified and other techniques that make use of the knowledge of interrupt address table or system vectors [13][14]. However, there is no single methodology that does a comprehensive analysis of intrusions and more importantly designed towards detecting multiple instances of their occurrence at different points of the host or the network [15][16]. The range of weaknesses found in the business environment are not due to technology alone, but also attribute to outdated security policies and procedures or gaps present in security risk management practices that fail to provide context-dependent safeguards for the organisation [17][18]. There is definitely a need for an effective IT security governance to collectively integrate, monitor and improve the security policies and mechanisms for a more efficient intrusion detection that could address zero-day attacks (unknown intrusions) of the present and the future [19] [20] [21].

This paper proposes autonomic framework for IT security governance that employs self-learning mechanisms using context-dependent mobile agents that are host-based as well as network-based for detecting malicious activities pre-emptively. Such an architecture provides the framework for performing runtime analysis intelligently and adaptively depending on the contexts of the possible intrusions in a fully-automated and coordinated manner. It uses machine intelligence and self-adaptive mechanisms to efficiently address the problem of zero-day attacks that are growing exponentially in recent years.

The structure of the paper is as follows. Section 2 provides the current state of IT security governance from literature and the need for aligning IT security with business objectives for enterprise governance and sustainability. Section 3 presents a self-learning autonomic architecture for an effective intrusion detection. Finally. a roadmap for autonomic IT security governance is described in Section 4 and Section 5 provides the conclusion and future work of this research.

2. IT SECURITY GOVERNANCE

The definition of enterprise governance lays its roots in 2002 when the Professional Accountants in Business (PAIB) Committee of the International Federation of Accountants (IFAC) defined *Enterprise governance* as follows:

> " the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organisation's resources are used responsibly"[22].

Simultaneously, many enterprises had also started to realise the potential benefits of IT in supporting business activities and researchers had already theorized the concept of IT governance to form an integral part of enterprise governance [23][24]. Since enterprise activities were being integrated using IT, business operations became interlinked with IT activities. Hence, IT Governance Institute (ITGI) was commissioned to understand the issues and the strategic importance of IT for developing a best practice framework, so that the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. The initial focus of IT governance framework was to ensure that expectations for IT are met and IT risks are mitigated [25]. However, many other enterprise's challenges and concerns were identified and ITGI reported the following key requirements:

1. Aligning IT strategy with the business strategy
2. Cascading strategy and goals down into the enterprise

3. Providing organizational structures that facilitate the implementation of strategy and goals
4. Insisting that an IT control framework be adopted and implemented.

Overall, the concept of IT governance has been evolving from time to time with IT revolution and one of the early definitions of *IT governance* is given below:

> "an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives" [25].

IT governance is a framework that enables organizations to manage their information resources efficiently and effectively and helps them in achieving their enterprise objectives. Major areas to be addressed by IT governance are: meeting IT expectations, alignment of IT with business and mitigating the IT risks [26]. The five key focus areas of IT governance are given below:

- IT strategic alignment
- IT value delivery
- Risk management
- Performance measurement
- Resource management

Today, enterprise governance cannot achieve business performance without good practices of the IT function of an organisation [27]. While organizations started to harness the benefits of connectivity and technological advancement, their progress is at risk due to prevalence of increased cybercrime. Hence, the term IT security governance has gained importance recently and is defined by ISO 38500 as the system by which an organization directs and controls IT security [28]. It should provide the risk management framework such that security strategies are aligned with business objectives and consistent with the regulations in protecting the confidentiality, integrity and availability of the organisation's information assets and systems [29]. In today's context, the terms 'IT governance' and 'IT security governance' are being used interchangeably to focus on the risk management framework that shapes business plans, information architecture, security policies and operational practices [30]. In achieving this, the next section takes the first step to propose an autonomic architecture for security enforcement in an organisation.

3. Autonomic Architecture For Intrusion Detection

Autonomic capabilities refer to special characteristics such as self-learning and adaptability that are particularly beneficial in systems with diverse distributed data service requirements on the Internet [31][32]. A context-dependent agent that is designed to learn on its own and change its behaviour based on its previous experience is said to have autonomic capability as it is able to self-manage and adapt intelligently [33][34]. The proposed architecture described in this section leverages on mobile agents that possess autonomic capabilities and prior malware experiences for efficient intrusion detection.

3.1. Suitability Of Mobile Agents

With different types of devices being connected through wired and wireless networks, the IT environment is posed with many challenges leading to the development of new security models [35][36]. Intelligent models that can provide high levels of flexibility and connectivity deal with agents. An agent can be used in a variety of forms and its functionality ranges from the most simple to the most sophisticated one. An agent could be designed with a specific purpose or even as a multifunction application [36][37]. While a fixed agent has certain restrictions, a mobile agent travels from host to host, accessing the necessary resources or services, and performs the necessary tasks to accomplish its mission. Such mobile agents could be designed to have autonomic capabilities that are warranted for intrusion detection.

A closer look at the various mobile computing models that incorporate agents indicate that the following three types of agents exist:

1. Fixed agent with server
2. Fixed agents with client and server
3. Mobile agents

The fixed agent with server has the following main disadvantages:

- it cannot sustain disconnections for thick clients performing computations,
- requires modifications of client code for interaction with the agent,
- agent cannot optimize data from mobile client to the server.
-

While client-side and server-side fixed agents solve some of the above listed problems, such models have the following disadvantages:

- an agent pair is required for every application type,
- not appropriate for thin clients,
- two mobile clients cannot interact directly and require the connectivity of the server unless it is peer-to-peer.

On the other hand, mobile agents could overcome all the issues listed above and could deal with weak connectivity, persistence and have the advantage of communicating with each other directly through wireless network. They need not worry about fixed network connections and they can migrate to find appropriate resources. Thus, a mobile agent not only has the main feature of mobility of migrating between processes in a wireless as well as a fixed network, but also has the ability to carry out autonomous tasks. This makes a mobile agent capable of inheriting one or more of the four autonomic computing properties, namely, self-configuring, self-healing, self-optimising, and self-protecting.

3.2. Proposed Architecture For Intrusion Detection

As described earlier, a mobile agent that is designed to learn on its own and change its behaviour based on its previous context-based experience is said to have autonomic computing capability as it is able to self-learn and adapt intelligently. Hence, to address the current IT security issues, we propose a mobile agent architecture with autonomic capabilities for intrusion detection. Figure 1 gives a pictorial overview of the proposed autonomic architecture that employs mobile agents to detect intrusions by collectively monitoring both the client and server environments.

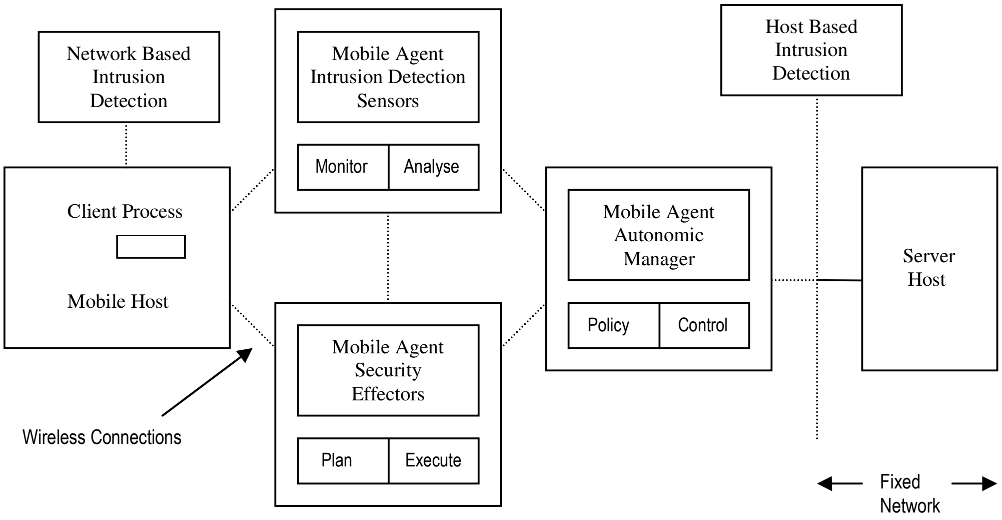

Network Based Intrusion Detection
Mobile Agent Intrusion Detection Sensors
Monitor
Analyse
Host Based Intrusion Detection
Client Process
Mobile Host
Mobile Agent Autonomic Manager
Policy
Control
Server Host
Mobile Agent Security Effectors
Plan
Execute
Wireless Connections
Fixed Network

Figure 1. Proposed autonomic architecture for intrusion detection

As shown in Figure 1, mobile agents could be designed to correspond to the autonomic elements that form the building blocks of autonomic systems [37]. These mobile agents continuously monitor intrusion detection over the wireless network through *sensors* and make adjustments through *effectors*. By monitoring behaviour through sensors and analysing the client data behavior, the mobile agents could then plan what action to be taken and to execute that action through effectors. This creates a kind of *control loop* as described in the theory of autonomic computing [31][32].

A mobile agent autonomic manager is a component that implements a particular control loop by using high-level policies to execute the most efficient options for carrying out security policy management tasks. It executes the control loop by sharing knowledge with the sensors and effectors so as to accomplish the four operations of the control loop (known as the MAPE loop) - Monitor, Analyze, Plan and Execute. Each mobile agent intrusion detection sensor could be composed of several special-purpose mobile agents that interact and collaborate with each other to achieve their goals. The mobile sensors mainly gather information about the client requests and perform in-depth analysis of security issues using business intelligence techniques. While analysing the data, they compare the information gathered as against a symptom service and knowledge base, as behaviours can be programmed by means of reactions to wireless communication events. Similarly, mobile agent security effectors could consist of several special-purpose mobile agents that collaborate with each other as well as with the sensors. The effectors receive the analysis outputs as a set of possible solutions from the sensors so as to plan and execute the processing of the intrusion detection requests in an optimal manner. Based on the policy rules forwarded by the mobile agent autonomic manager, the plan element of the effectors selects one of the optimal solutions and the execute element carries out the actions for that solution. Before triggering the resulting action, the mobile agent autonomic manager uses the self-learning policy engine to sense any symptom of problem or conflicts for implementing these actions that would trace the MAPE loop again until the QoS attributes are achieved. A pictorial representation of the MAPE control loop for the mobile agent autonomic manager that self-learns and adapts from one instance to another of the feedback loop is given in Figure 2.

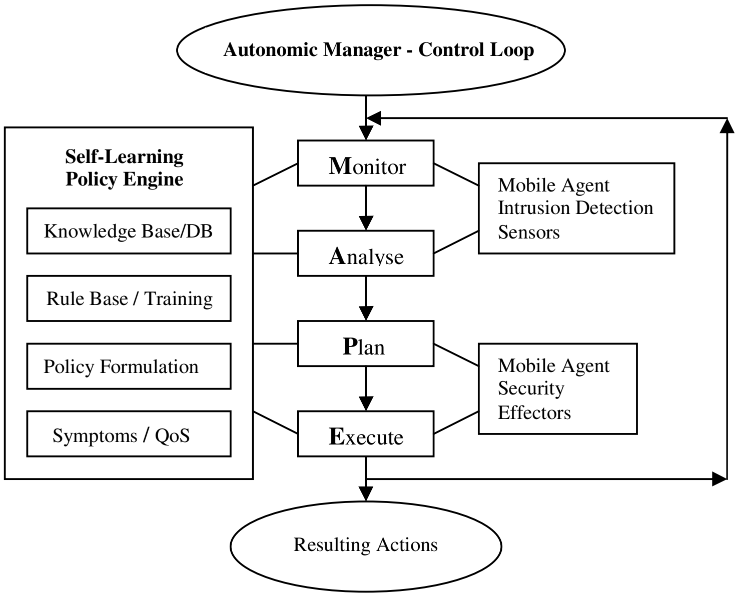

Autonomic Manager - Control Loop
Self-Learning Policy Engine
Knowledge Base/DB
Rule Base / Training
Policy Formulation
Symptoms / QoS
Monitor
Analyse
Plan
Execute
Mobile Agent Intrusion Detection Sensors
Mobile Agent Security Effectors
Resulting Actions

Figure 2. An adaptive control loop for the autonomic manager

Overall, the mobile agent autonomic manager controls the events in the loop by having expert rules embedded as programs for coordinating agent interactions [38][39]. By the use of knowledge base and expert rules pertaining to the organisation's security contexts, it can provide mechanisms for dynamically defining (self-configuring), modifying (self-healing and self-optimising), and securely (self-protecting) forwarding these rules to the mobile agents. An intrusion detection requires highly flexible, secure and coordinated processing in a dynamic distributed heterogeneous environment. Hence, a dynamic intrusion detection service should cater to several security policy parameters that need to be adjusted for tuning the performance and thereby meeting the QoS requirements. As shown in Figure 2, mobile agents with autonomic computing architecture have the necessary capabilities of formulating revised policies by adjusting the parameters during runtime in order to achieve the best QoS for organisations in real-time environment.

4. ROADMAP FOR AUTONOMIC IT SECURITY GOVERNANCE

The autonomic intrusion detection architecture proposed in the previous section is postulated to monitor several behaviour patterns of networks and multiple system instances in order to characterise their state as normal or abnormal and advances further from previous work [40] to embrace appropriate IT security governance in an organisation. The MAPE control loop is capable of incorporating autonomic capabilities such as self-configuring, self-healing, self-optimising and self-protecting techniques that cater to detecting new and obfuscated intrusions. However, such an effective IT solution does not alone suffice in addressing the ever-increasing security incidents faced by organisation today. The recent trend of the security infiltrations indicate that attackers do not solely rely on weaknesses in technical safeguards and solutions. Instead, they probe and exploit the organisation’s weaknesses in security policies and procedures as well as gaps found in risk management practices. IT security governance is the mechanism that can provide the necessary directions and shape up an organisation’s business goals, information architecture, security policies, and operational, risk management practices. In this section, we provide a roadmap for incorporating IT security governance using the proposed autonomic architecture for intrusion detection. Figure 3 shows a 4-step roadmap of such an autonomic IT security governance framework as described next.

STEP1: EMBRACE A SELF-LEARNING IT SECURITY VISION:

In this step, the security vision of the organisation is aligned with the business goals and QoS targets so that the security policy and procedures not only meet the standard regulations but also the business requirements across all divisions, departments, structures and processes of an organisation [41]. The self-learning culture should be developed through shared security procedures and practices across all organisational activities. This will enable employees at all levels of an organisation to embrace the security policy as part of their day-to-day work practices. Today, security attacks and threats are inevitable in every organisation since crime groups are a step ahead in employing sophisticated tools and methods to gain unauthorised access to the information assets resulting in business function disruptions. Therefore, the main purpose of a synergised security vision in this step is to be aligned with the business goals using a self-learning feedback loop mechanism for achieving continuous improvement in the quality of service that is warranted for the changing environment of the future.

STEP 2: DEVELOP AUTONOMIC FRAMEWORK FOR SECURITY RISKS:

Any security threat is considered as a financial risk by the management of an organisation. There is a need to effectively assesses and manage risk across all stakeholders of the organisational network in order to safeguard the integrity and availability of public information as well as the protection of non-public information. In this step, appropriate standard IT governance frameworks such as ITIL, COBIT, ISO38500, etc. are adopted to blend good practices from various sources in order to establish a risk management strategy [25][28][30]. Every project activity needs to identify risks as well as roles and responsibilities for accountability as defined in the Responsible-Accountable-Consulted-Informed (RACI) model of risk management of the organisation. Information systems should support what-if dashboards and other graphical tools for autonomous assessment and identification of business operational risks for the present and the future. Appropriate security awareness program and culture could then be developed for various stakeholders in the business network to understand their roles and responsibilities in order to proactively participate in such an autonomous risk management framework. The management should adopt good communication, consultation, transparency and consistency methods among the stakeholders in for establishing the required security policy compliance and standards. This step would not only facilitate in meeting the legal, regulatory and contractual obligations but more importantly in achieving uninterrupted business operations and services availability for the stakeholders across the organisation's network.

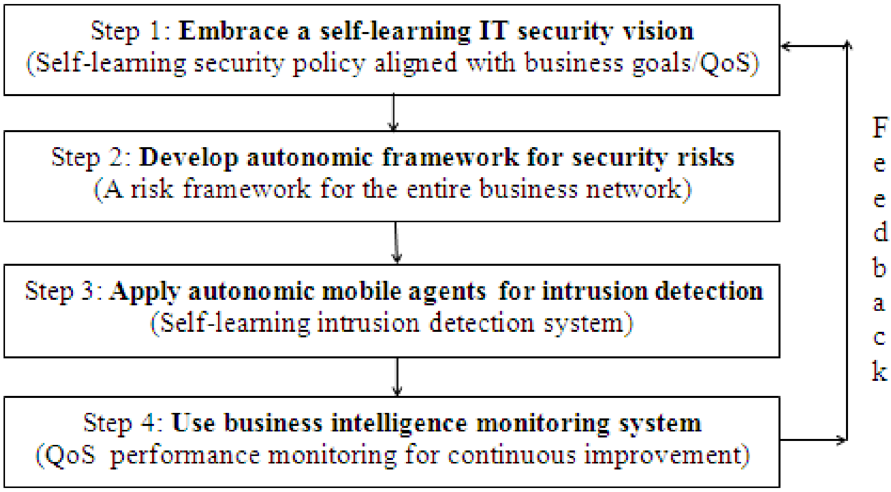
STEP 3: APPLY AUTONOMIC MOBILE AGENTS FOR INTRUSION DETECTION:

This step involves employing the necessary tools and techniques for applying the autonomic intrusion detection framework using mobile agents that is proposed in the previous section. As shown in Figure 1, the mobile agents retrieve various data by probing the host and sniffing the network collaboratively so as to find out the organisation's context-dependent information (e.g, network protocol, host O/S, application platform, etc.). This will help to create, modify and update the knowledge base for an organisation's business context. At any instant, prior knowledge of the host and network are retrieved from the knowledge base and new behaviour patterns are gathered and communicated to the Self Learning Policy Engine as shown in Figure 2. Different mobile agents would work collaboratively on specialised capabilities using signature-based or behaviour-based or heuristic techniques to detect anomalies in the system. They share knowledge between host-based and network-based anomalies and with the aid of Self Learning Policy

Engine they get trained with synthetically generated polymorphic datasets of malicious attacks. A variety of data mining and machine learning algorithms are applied in the inference engine to arrive at accurate predictions for intrusion detection using feature measures, symptom controls and context-dependent parameters associated with the host and network of the organisation. Any new knowledge (related to fuzzy weights of inference rules, threshold values, feature measures, etc.) gained would be used to update the Self Learning Policy Engine and perform intelligent alerts to the business processes affected. The management could then initiate the necessary actions based on the severity of the alerts. A major action plan may be required if a denial-of-service (DoS) attack is predicted. Such an adaptive expert rule-based policy engine that makes use of autonomic capabilities would then be able to proactively detect new intrusions of the future as well.

STEP 4: USE BUSINESS INTELLIGENCE MONITORING SYSTEM:

Organisations are required to deliver the IT security governance and monitor their performance. They would establish and implement an audit and review compliance framework in order to ensure that the business goals and QoS targets are known throughout the organization,. Typically, employees from different departments or functional areas could become representative members of a security audit team to identify and monitor the threats and associated risks of the organisation. Audit trails to detect and respond to intrusion events determined in Step 3 are maintained and security procedures and policies are evaluated and periodically reviewed. Overall, this step of the proposed roadmap involves using business intelligence monitoring tools and techniques that are employed in Step 3 to incorporate suitable metrics in measuring the business goals as well as QoS targets determined in Step 1. Such a performance monitoring system with dashboards and what-if data analytic tools [42] could be employed by the security audit team effectively for IT security governance. This step helps to review the risk-based policies, procedures and controls based on monitoring the activity of authorized users and unauthorized access as well as the impact of tampering with nonpublic information by unauthorized users. The security audit team will then be able to follow the direct lines of reporting to the management and regulatory bodies, thereby providing feedback for continuous improvement and business sustainability. The outcomes of this step serve as input to Step 1 of the feedback loop of the organisation's IT security governance framework.


Step 1: **Embrace a self-learning IT security vision**
(Self-learning security policy aligned with business goals/QoS)

Step 2: **Develop autonomic framework for security risks**
(A risk framework for the entire business network)

Step 3: **Apply autonomic mobile agents for intrusion detection**
(Self-learning intrusion detection system)

Step 4: **Use business intelligence monitoring system**
(QoS performance monitoring for continuous improvement)

Figure 3. Roadmap for autonomic IT security governance

The above four steps of the roadmap would aid in the ongoing review and implementation process of security practices towards achieving a successful IT security governance in an organisation. The tightly aligned security strategies with business goals and QoS and periodic adjustments necessary to ensure that effective risk management is possible by adopting the autonomous intrusion detection, monitoring and feedback loop proposed in these steps. As IT becomes part and parcel of everyday business operations, organization-wide responsibility in establishing transparent and effective IT security governance is essential and the above roadmap provides a practical guideline towards achieving this.

5. CONCLUSIONS

Today's organisations are unable to achieve adequate security and governance of their information assets using technology-based solutions alone due to the increasing sophistication in cybercrime and intrusions witnessed that affect their everyday business operations [19][20]. On one hand, IT experts are improving technical solutions for intrusion detection, on the other hand, regulatory bodies are developing new standards and requirements for a more organisation-wide risk management and IT governance. Both aspects are important and this paper has advanced further to achieve this. In this paper, an autonomic architecture for a proactive intrusion detection as well as a roadmap for an organisation-wide framework for effective IT security governance are proposed. A generic autonomic intrusion detection architecture that makes use of context-dependent mobile agents at the network-level and host-level to monitor, analyse, plan and execute (MAPE) in an intelligent and collaborative manner is presented. A 4-step roadmap for IT security governance is also presented as a practical implementation guideline in applying the proposed autonomic intrusion detection architecture for effectively safeguarding and detecting unknown attacks. The proposed framework focused on the self-learning capabilities of autonomic feature so that organisations can make use of the continuous improvement feedback loop to proactively monitor and identify their weaknesses and finetune their security policies and procedures for an improved QoS.

REFERENCES

[1] Lab K., (2015) “Kaspersky Security Bulletin,” Kaspersky Lab, Tech. Rep.

[2] Symantec, (2016) “Internet Security Threat Report: Trends for 2016,” Symantec, Tech. Rep. vol. 21, p. 81.

[3] McAfee Labs, “McAfee Labs Threats Report,” Intel Security, Tech. Rep., 03 2016.

[4] Microsoft, “Microsoft Security Intelligence Report,” Microsoft, Tech. Rep., 12 2015.

[5] HP Enterprise, “HPE Security Research Cyber Risk Report,” Hewlett Packard Enterprise, Tech. Rep., 2016.

[6] IBM X-Force, (2015) “IBM X-Force Threat Intelligence Report 2016,” IBM, Tech. Rep., 2016.

[7] Vasilomanolakis, E. Karuppayah, S. Mühlhäuser, M. and Fischer, M. “Taxonomy and Survey of Collaborative Intrusion Detection,” ACM Computing Surveys, vol. 47, no. 4, pp. 55:1–55:33.

[8] Sommer R. and Paxson V., (2010) “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” in Proceedings of the 2010 IEEE Symposium on Security and Privacy. IEEE Computer Society, pp. 305–316.

[9] Jang, J.-w. Yun, J. Mohaisen, A. Woo, J. and. Kim, H. K (2016) “Detecting and Classifying Method Based on Similarity Matching of Android Malware Behavior with Profile,” SpringerPlus, vol. 5, no. 1, p. 1.

[10] Nguyen, A. Yosinski, J. and Clune, J. (2015) “Deep Neural Networks Are Easily Fooled: High Confidence Predictions for Unrecognizable Images,” The IEEE Conference on Computer Vision and Pattern Recognition.

[11] Schmugar, C. (2007) "The future of cybercrime", Sage: Security Vision From McAfee Avert Labs, 1(2), 1-5.

[12] Faruki, P. Bhandari S., Laxmi, V. Gaur M., and Conti, M. (2016) “DroidAnalyst: Synergic App Framework for Static and Dynamic App Analysis,” in Recent Advances in Computational Intelligence in Defense and Security. Springer, pp. 519–552.

[13] Li, W.-X. Wang, J.-B. Mu, D.-J. and Yuan, Y. (2011) “Survey on Android Rootkit,” Microprocessors, vol. 32. no.2, pp. 68-72.

[14] Kim, S. Park, J. Lee K., You, I. and Yim K., (2012) “A Brief Survey on Rootkit Techniques in Malicious Codes,” Journal of Internet Services and Information Security, vol. 2, no. 3/4, pp. 134–147.

[15] Lam, P. Wang L.-L., Ngan, H. Y. T. Yung, N. H. C. and Yeh, A. G.-O. (2015) “Outlier Detection In Large-Scale Traffic Data By Naïve Bayes Method and Gaussian Mixture Model Method,” arXiv.

[16] Yang, J. Deng, T. and Sui, R. (2015) “An Adaptive Weighted One-Class SVM for Robust Outlier Detection,” in Proceedings of the 2015 Chinese Intelligent Systems Conference. Springer, pp. 475–484.

[17] Pereira, G.V. Luciano, E. M. Macadar, M. A. and Daniel, V.M. (2013) “Information technology governance practices adoption through an institutional perspective: The perception of brazilian and american CIOs,” 46th Hawaii International Conference on System Sciences, pp. 4446–4455.

[18] Turel O. and Bart, C. (2014) “Board-level IT governance and organizational performance,” Eur. J. Inf. Syst., vol. 23, no. 2, pp. 223–239.

[19] Borth, M. A., and Bradley, R. V. (2009). "Unexplored Linkages between Corporate Governance and IT Governance: An Evaluation and Call to Research Information Technology Governance and Service Management: Frameworks and Adaptations" IGI Global. pp. 202-220.

[20] Buchwald, A. Urbach, N. and Ahlemann, F. (2014) “Business value through controlled IT: Toward an integrated model of IT governance success and its impact,” J. Inf. Technol., vol. 29, no. 2, pp. 128–147.

[21] Yu, S. Wang, G. and Zhou, W. (2015) “Modeling Malicious Activities in Cyber Space,” IEEE Network, vol. 29, no. 6, pp. 83–87.

[22] IFAC (2004), "Enterprise Governance-Getting the Balance Right", PAIB Report to IFAC.

[23] Cumps, B., Viaene, S., & Dedene, G. (2012). "Linking the Strategic Importance of ICT with Investment in Business-ICT Alignment: An Explorative Framework". In W. Van Grembergen & S. De Haes (Eds.), Business Strategy and Applications in Enterprise IT Governance (pp. 37-55). Hershey, Pennsylvania, USA: IGI Global.

[24] De Haes S. and Van Grembergen, W. (2015) "Enterprise Governance of Information Technology", Cham: Springer International Publishing.

[25] ITGI (2003), "Board briefing on IT governance", 2nd Edition, Information Systems Audit and Control Foundation, 2003.

[26] Bartens, Y ., Schulte, F., & Vos, S. (2014). "E-Business IT Governance Revisited: An Attempt towards Outlining a Novel Bi-directional Business/IT Alignment in COBIT5", Paper presented at the 47th Hawaii International Conference on System Sciences (HICSS), 2014.

[27] Chou, Y.-C., Chuang, H. H.-C., & Shao, B. B. M. (2014). "The impacts of information technology on total factor productivity: A look at externalities and innovations". International Journal of Production Economics, 158, 290-299.

[28] ISO/IEC 38500, (2015) "Information Technology - Governance of IT for the organization" ISO/IEC 38500:2015, 2nd Edition, ISO:Switzerland.

[29] OECD (2005) Corporate Governance. OECD glossary of statistical terms, Organisation for Economic Co-operation and Development (OECD),

[30] Stroud, R.E. (2012). "Introduction to COBIT 5" . ISACA.

[31] Kephart, J. and Chess, D. M. (2003) "The vision of autonomic computing", IEEE Computer, vol. 36, no. 1, pp. 41-50.

[32] Ganek, A. G. and Corbi, T. A. (2003) "The Dawning of the Autonomic Computing Era". IBM Systems Journal. vol. 42, no. 1, pp. 5-18.

[33] Dudley, G., Joshi, N., Ogle, D.M., Subramanian, B. and Topol, B.B. (2004) "Autonomic self-healing systems in a cross-product IT environment", Proceedings of the International Conference on Autonomic Computing), 312-313.

[34] Dobson, S. Sterritt, R. Nixon, P. and Hinchey. M. (2010) "Fulfilling the vision of autonomic computing". Computer, vol. 43, pp. 35-41.

[35] Vidales, P., Baliosian, J., Serrat, J., Mapp,G., Stajano, F. and Hopper, A. (2005) "Autonomic System for Mobility Support in 4G Networks". IEEE Journal on Selected Areas in Communications. vol. 23, no. 12, pp. 2288-2304.

[36] Sancho G., Villemur T. and Tazi S., (2010) “An Ontology-driven Approach for Collaborative Ubiquitous Systems”, International Journal of Autonomic Computing (IJAC) InderScience Publishers Mai pp 263 - 279.

[37] Cabri, G., Leonardi, L. and Zambonelli, F. (2002) "Engineering Mobile Agent Applications Via Context- Dependent Coordination". IEEE Transactions on Software Engineering. vol. 28, no. 11, pp. 1040-1058.

[38] Russell, S.J.; Norvig, P. (2010). Artificial intelligence: A modern approach (3rd ed. ed.). Upper Saddle River: Prentice Hall.

[39] Alizadeh, H. Khoshrou A., and Zúquete, A. (2015) “Traffic Classification and Verification using Unsupervised Learning of Gaussian Mixture Models,” in International Workshop on Measurements & Networking. IEEE.

[40] Venkatraman, S. (2010) "Self-Learning Framework for Intrusion Detection", Proceedings of The 2010 International Congress on Computer Applications and Computational Science (CACS 2010), 4-6 December, Singapore, pp. 517-520

[41] Cui, T., Ye, H., Teo, H. H., & Li, J. (2015) "Information technology and open innovation: A strategic alignment perspective". Information & Management, vol. 52, pp. 348-358.

[42] Yu, S. Guo, S. andStojmenovic, I. (2015) “Fool Me if You Can: Mimicking Attacks and Anti-Attacks in Cyberspace,” IEEE Transactions on Computers, vol. 64, no. 1, pp. 139–151.

AUTHORS

Sita Venkatraman is currently the Information Technology Lecturer and Discipline Leader for Business Information Systems at the School of Engineering, Construction & Design, Melbourne Polytechnic, Australia. She earned her PhD in Computer Science, with a doctoral thesis titled “Efficient Parallel Algorithms for Pattern Recognition”, from National Institute of Industrial Engineering in 1993. In the past 25 years, Sita's work experience involves both industry and academics - developing turnkey projects for IT industry and teaching a variety of IT courses for tertiary institutions, in India, Singapore, New Zealand, and more recently in Australia since 2007. Her recent research areas are predominantly in Business Intelligence, Data Mining, Cloud Computing and Information Security. Sita has published eight book chapters and more than 100 research papers in internationally well-known refereed journals and conferences. She also serves as Member of Register of Experts at Australia's Tertiary Education Quality and Standards Agency (TEQSA).

..