Security in the Context of Multi-Agent Systems (Extended Abstract)

Gideon D. Bibu
Department of Computer Science, University of Bath, Bath, UK
G.D.Bibu@bath.ac.uk

ABSTRACT

Security of systems and information has always been a challenge to organisations and industries. Many technical solutions including firewalls, encryption and anti-virus software have been used, yet security still remains a problem. These security solutions failures are largely due to the fact that as systems become more complex, a lot of interaction is involved between various actors. Some of these interactions usually leave room for security vulnerabilities which are simply not accounted for by the technical security solutions: there are just too many possibilities.

My research is focused on this aspect of organisational security. The proposed approach to this involves the monitoring of events for traces of behaviours that may eventually circumvent the security regulations of the organisation. The methodology includes organisational modeling and simulation of self monitoring agents using a normative framework.

Categories and Subject Descriptors

I.2.11 [**Artificial Intelligence**]: Distributed Artificial Intelligence—*Multiagent Systems*

General Terms

Security, Multi-agent Systems

Keywords

Multi Agents Systems, Security, Organisational Modeling, Institutions

1. INTRODUCTION

Security in large, heterogeneous distributed systems has faced with many challenges due to the increased richness and complexity of interconnections between systems and the interactions between subsystems. Security research — and the solutions provided — have been largely focused on technical issues such firewalls, encryption and anti-virus software. While these solutions have been implemented, they have not been able to deliver the desired level of security [2]. This concern has drawn the attention of researchers in the security domain who have identified issues including human factors [7] and lack of early identification and integration of security requirements in systems development [5]. With the widespread of application of software systems and their usage in almost every part of human life, security of such systems is no longer a mono-dimensional technical issue but a multi-dimensional challenge that encompasses technology, people, and processes. The research literature abounds with advocations for the consideration of security from the early stages and throughout the software development life cycle. There is therefore the need to develop mechanisms that support the analysis of these dimensions of security threats.

Organizations are made up of individual human actors who interact with each other and with various organizational resources such as information and data as they carry out their duties. As such, they have the tendency to exhibit behaviours that may circumvent the security efforts of such organizations, for practicality and convenience more than malice. Such behaviours are difficult to elicit during design and so constitute a major source of security vulnerabilities that become evident at run time. This research aims to

- Use security *misuse cases* to analyse the static security properties of a system. This will help system developers understand the nature of security threats to expect in the system thereby enabling them set up appropriate mitigation mechanisms.
- Model such organisations as a multi-agent system and use event monitoring connected to a normative framework to identify security vulnerabilities in practice. Events initiated by actors will be monitored and analysed for the presence or absence of traces of anomalous behaviours that may or may not lead to violation of security policies. This strategy of monitoring events should help in the early detection and eventual prevention of security breaches within the organisation.

2. RELATED WORK

Event monitoring has been widely used in intrusion detection and prevention systems where an intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches. Patcha and Park [6] summarised intrusion detection as the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a system/network. An intrusion detection system is capable of detecting all types of malicious network traffic and computer usage. The network packets that are collected are analyzed for rule violations by a pattern recognition algorithm. When rule violations are detected, the intrusion

Cite as: Security in the Context of Multi-Agent Systems (Extended Abstract), Gideon D. Bibu, *Proc. of 10th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2011)*, Yolum, Tumer, Stone and Sonenberg (eds.), May, 2–6, 2011, Taipei, Taiwan, pp. 1339-1340.

detection system alerts the administrator. This approach has been applied to solving various levels of computer network security problems [6, 4]). Event monitoring has also been used in process mining [8], where events are monitored, logged, and analysed for the purpose of improving business processes. These approaches require the existence of separate monitoring and analysis entities. However, we are using the approach in a dynamic way to address the problem of eliciting security threats that are due to the vulnerabilities that arise as a result of the interaction between the various actors in a system.

Misuse Cases document conscious and active opposition in the form of a goal that a hostile agent intends to achieve, but which the organization perceives as detrimental to some of its goals. A Misuse Case and its hostile agent implies a dynamic and intelligent pattern of threats, not just the single threatening goal that is actually named. Misuse cases therefore, concentrate on interactions between the application and its misusers (e.g., cracker or disgruntled employee) who seek to violate its security. It allows for the analysis of security threats from the view of the attacker. Because the success criteria for a misuse case is a successful attack against an application, misuse cases are highly effective ways of analyzing security threats [3].

3. SOLUTION APPROACH

The model consist of a world model, (potentially several) institutional frameworks, and agents. It is based on the notion of observable events that capture the notion of physical world events and institutional events that only have meaning within a given social context. Institutional events are not observable, but are created through Conventional Generation, whereby an event in one context Counts As the occurrence of another event in a second context. Taking the physical world as the first context and by defining conditions in terms of states, institutional events may be created that count as the presence of states or the occurrence of events in the institutional world. Thus, an institution is modelled as a set of states that evolve over time subject to the occurrence of events, where an institutional state is a set of institutional fluents that are considered true at some instant.

From this approach, institutional frameworks provide a mechanism to capture and reason about "correct" and "incorrect" behaviour within a certain context, which in this case is security. The definition of norms here is taken to include security rules and policies. The participants of our normative framework are governed by security rules and policies specified in the norm. The framework monitors the permissions, empowerment and obligations of their participants and generate violations when norms are not adhered to. Information of the norms and the effects of participants actions is stored in the state of the framework. The constant change of the state over time as a result of these actions provides participants information about each others behaviour. This follows from the concept that "little" facts collected about events/actions over time may eventually lead to "big" facts that reveal vital information about a participant's behaviour i.e conformance to or violation of security rules.

Security is, and always will, be a major concern in any IT infrastructure. However, what makes smart grid security issues more daunting is the pervasive and massive deployment of networked smart meters and other IT-enabled components. Also, there are other business solutions that will emerge such as the integration of various business-to-business (B2B) and business-to-consumer (B2C) smart networks. This will result in a lot of interaction taking place between and within different domains of the energy grid, hence a huge amount of information flowing within the grid, including customers' private information. The distributed nature of the smart grid, and the intelligent autonomous behaviour expected of it, naturally lend itself to multi-agent methodology [9]. However, no research has directly addressed security issues. We have chose to use the NISTIR 7628 guideline for smart grid cyber security [1], to provide the scenario for evaluating our proposed model.

4. FUTURE PLANS

My aim is to develop a methodology for formalising and analysing security threats in systems and tools for analysing security vulnerabilities in an organisation arising from interactions between actors. To test this, I will use scenarios from the publicly available NIST specification for smart grid security to develop misuse cases and organisational models. The misuse cases will specify potential misuses that can result in (information) security breaches, while the organisational model will specify and validate the dependencies between actors. My research timeline is 1. organizational modelling with Operetta (3 months) 2. evaluation of the organizational models using agent-based simulation in Jason and Agentscape (9 months) 3. development of behaviour monitoring tool (6 months) 4. scaling up simulation (in parallel) 5. writing up (6 months). The most significant research challenge I foresee is how to express security misuse goals with multiple subgoals in terms of norms and how they may properly influence agent behaviour.

5. REFERENCES

[1] Guidelines for smart grid cyber security: Vol.1, smart grid cyber security strategy, architecture, and high-level requirements, August 2010. `http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf` Accessed Oct. 18, 2010.

[2] Information security breaches survey 2010. Technical report, PriceWaterHouseCoopers, April 2010. `http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf` [Accessed November 1, 2010].

[3] D. Firesmith. Security use cases. *Journal of Object Technology*, 2(1):53–64, 2003.

[4] A. Lauf, W. H. Robinson, and A. Peters. A distributed intrusion detection system for resource-constrained devices in ad-hoc networks. *Elsevier Ad-hoc Networks*, 8(3):253–266, May 2010.

[5] H. Mouratidis and J. Jürjens. From goal-driven security requirements engineering to secure design. *Int. J. Intell. Syst.*, 25(8):813–840, 2010.

[6] A. Patcha and J.-M. Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51(12):3448–3470, 2007.

[7] B. Schneier. *Secrets and Lies: Digital Security in a Networked World*. Wiley Publishing, Inc., 2000.

[8] W. van der Aalst, V. Rubin, H. Verbeek, B. van Dongen, E. Kindler, and C. GÃijnther. Process mining: a two-step approach to balance between underfitting and overfitting. *Software and Systems Modeling*, 9:87–111, 2010. 10.1007/s10270-008-0106-z.

[9] P. Vytelingum, T. Voice, S. D. Ramchurn, A. Rogers, and N. R. Jennings. Intelligent agents for the smart grid. In W. van der Hoek et al., eds, *AAMAS 2010*, volume 1, pages 1649–1650, Toronto, Canada, May 10-14 2010. IFAAMAS.