

Network Defence Using Attacker-Defender Interaction Modelling

Jana Medková, Pavel Čeleda

▶ **To cite this version:**

Jana Medková, Pavel Čeleda. Network Defence Using Attacker-Defender Interaction Modelling. 10th IFIP International Conference on Autonomous Infrastructure, Management and Security (AIMS), Jun 2016, Munich, Germany. pp.127-131, 10.1007/978-3-319-39814-3_12 . hal-01632737

HAL Id: hal-01632737

https://inria.hal.science/hal-01632737

Submitted on 10 Nov 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Network Defence Using Attacker-Defender Interaction Modelling

Jana Medková and Pavel Čeleda

Institute of Computer Science
Masaryk University, Brno, Czech Republic
jana.medkova@mail.muni.cz, celeda@ics.muni.cz

Abstract Network security is still lacking an efficient system which selects a response action based on observed security events and which is capable of running autonomously. The main reason for this is the lack of an effective defence strategy. In this Ph.D., we endeavour to create such a defence strategy. We propose to model the interaction between an attacker and a defender to comprehend how the attacker's goals affect his actions and use the model as a basis for a more refined network defence strategy. We formulate the research questions that need to be answered and we discuss, how the answers to these questions relate to the proposed solution. This research is at the initial phase and will contribute to a Ph.D. thesis in four years.

Keywords: network defence, defence strategy, attacker-defender interaction modelling

1 Introduction

In network security, we can consider the reaction to an attack to follow a recurring cycle of detecting and understanding security events, making decisions and taking response actions [6]. However, if the defence is carried out by a human and the attack is automated, the response action might occur too late. In order to react quickly to an attack, the network defence has to be able to operate autonomously. In order to create an autonomous defence system, each part of the cycle has to be fully automated.

This has already been partly accomplished: the gathering of information from various sources is automated by Intrusion Detection Systems (IDS), which generate security alerts when malicious or suspicious activity is observed [2,11]. The received information is automatically processed to form situation awareness by Security Information and Event Management systems (SIEM), which provide a real-time analysis of security alerts [10]. The selected response actions can be carried out automatically using Software Defined Networking (SDN) [8,5].

However, the selection of response actions is still performed by a security expert or unsophisticated decision algorithms, which take actions only where certain thresholds are exceeded. These thresholds are usually very high to avoid blocking

legitimate users. Such systems are not capable of handling more complicated situations. If we want to be able to create a system capable of selecting response actions autonomously or work as a decision support for a security expert, we need a more efficient, refined defence strategy. In the proposed Ph.D. thesis, we would like to address this issue.

We propose to create a mathematical model of the interaction between an attacker and a defender and use it as a basis for a network defence strategy. Through modelling, we gain insight. Through insight, we gain understanding. Through understanding, we can form a strategy. However, to form a strategy based on the model several challenges have to be overcome.

1. The interaction between an attacker and a defender on the network is very complex. The network can be large, change over time and the number of attack vectors is ever growing. Moreover, each action has to be considered not individually but in the context of its future implications.
2. We are always uncertain about the state of the network, the attacker's objectives and previous actions (and whether he is an attacker at all). The best we can do is to operate on our beliefs – a probability distribution over the possible states updated whenever we receive new information.

Attempts have been made towards an autonomous network defence strategy. The Response and Recovery Engine [13] selects a response action using game theory. The system showed promising results in simulated scenarios, however, it has limited usability since it assumes that an agent system is installed on each host. In [1] the authors propose a network defence system using reinforcement learning and dynamic risk assessment. However they admit that the overall performance was not optimal and further improvement is needed. A general overview of the model's requirements applicable for modelling the interaction between an attacker and a defender was given in [9].

2 Research Questions

The main goal of the proposed research is **to model the interaction between an attacker and a defender and use the model as a basis for a network defence strategy**. We have defined following research questions, which need to be answered to achieve this goal:

1. **How can we model the interaction between an attacker and a defender?** The model of the interaction between an attacker and a defender provides a formal description of the workings of the interaction. It is necessary that the description is accurate, so that it captures the underlying principles of the interaction. At the same time, the model has to simplify the situation since we want to use the model to optimise the defender's actions. Balancing the accuracy and simplicity is crucial. We have to define the model that can be solved with reasonable computational complexity even for large networks and still be capable of capturing the essence of the interaction.

2. **How can we use the model to form a network defence strategy?** The model of the interaction between an attacker and a defender only describes the interaction in a simplified manner. However, it enables us to better comprehend the dynamics of the interaction between an attacker and a defender, which in turn enables us to find the best response actions for the defender. We will use these actions to form a defence strategy.
3. **Can human instinct and experience be included in the defence strategy?** While the model can capture principles applicable in real life, it has its limitations. It is not unusual that the security expert observed similar attacks in the past or has better intuition. It would be therefore very desirable to use this information to improve the decision based on the model. Such a concept exists in economics, namely the Black-Litterman model [3].

3 Proposed Approach

Our approach to creating a defence strategy consists of modelling the interaction between an attacker and a defender. We consider the interaction only on the defended network. Without the loss of accuracy, we also assume that the attacker's malicious intent is targeted on the network and he tries to maximise his utility by employing a series of attacks. On the other hand, the defender makes his best effort to defend the network based on his observations and available response actions. We assume both the observation and the response actions are made at the network level since it allows us to cover all connected hosts. Moreover, in reality, the defender usually does not have administration rights on the hosts in the network. In a fully autonomous defence, the role of the defender is taken on by a system capable of network monitoring and reconfiguration.

In this Section, we outline the steps that need to be taken in order to answer the research questions. We describe each step and a proposed approach.

Modelling the interaction between an attacker and a defender – We believe that game theory is a suitable mathematical tool for modelling the interaction between an attacker and a defender since it can model situations in which multiple parties with conflicting interests compete with each other [4]. We can use a game-theory toolset to compute the optimal strategies (in a game-theoretic meaning) for the defender and base the defence strategy (in a network defence meaning) on them. When defining the model, we have to keep in mind, that at some point in future we will need to compute the optimal actions of the defender and the attacker. Therefore, the model should be designed so that this task is computationally feasible.

Translating network information into model parameters – We have to estimate the input parameters of the model from information about the network in an automated fashion. The information should be passed in the form of a formal network description: the topology of the network, the hosts and services present in the network, the required levels of confidentiality, availability and integrity of these services and their interdependence. Based on this information, we can compare how desirable different outcomes are for the defender.

Network defence strategy – When formulating the strategy, we have to take into account uncertainty about the state of the network and the attacker's previous actions and goals. A possible approach would be to use the alerts generated by an intrusion detection system to maintain beliefs about the current state of the network, the attacker's past actions and his goals. Based on these beliefs we can use the model and select the best response action in a given situation. Since the computational complexity of optimising the response action is most likely going to be very high, we do not suppose that this selection would be computed at runtime, more likely it would be computed for the network in advance and only the precomputed results will be used.

Strategy verification – The efficiency of the decision algorithm has to be verified. First, we plan to test the proposed strategy in a simulated environment using a cloud-based testbed for simulating cyber attacks [7]. Then, we plan to compare the strategy with decisions made by teams in the Computer Security Incident Response Team (CSIRT) training exercise [12]. In this exercise, teams of CSIRT employees defend their network and are scored based on the success of the attacks. The strategy would represent the fifth team and its score will be compared to the "real" teams score.

Adding human intuition to decision output – The strategy will base the defence on beliefs about the state of the network, the attacker's past and future actions and his goals. Any refinement of these beliefs will lead to better results. Humans have expertise and intuition which cannot be emulated by any model, no matter how sophisticated. They could have seen similar situations before, guess what will the attacker do next or have additional information which is not included in the strategy. We can include human opinion on the situation into the decision by updating the current beliefs.

4 Conclusion

The role of a defender in network security is difficult. If the defender cannot protect his network, he fails. If he impairs a legitimate user by his actions, he fails. Moreover, the defender is never certain about the state of the defended network since the observations of the network might be incorrect. Currently, automated network defence systems select response actions based only on the observed security events. They react only in unambiguous situations and the rest of the events must be investigated by security experts. We want to refine the decision making process by including also the motivation of the attacker. By comprehending how his goals affect his actions, we gain more information and we can select the response action more accurately.

Acknowledgement

This research was supported by the Security Research Programme of the Czech Republic 2015 - 2020 (BV III / 1 VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20162019014 Simulation, detection, and mitigation of cyber threats endangering critical infrastructure.

References

1. Beaudoin, L., Japkowicz, N., Matwin, S.: Autonomic computer network defence using risk state and reinforcement learning. Cryptology and Information Security Series 3, 238–248 (2009)
2. Bhuyan, M.H., Bhattacharyya, D.K., Kalita, J.K.: Network Anomaly Detection: Methods, Systems and Tools. IEEE Communications Surveys & Tutorials 16(1), 303–336 (2014)
3. Black, F., Litterman, R.: Global Portfolio Optimization. Financial Analysts Journal 48(5), 28–43 (1992)
4. Hamilton, S.N., Miller, W.L., Ott, A., Saydjari, O.S.: The role of game theory in information warfare. In: 4th Information survivability workshop (ISW-2001/2002), Vancouver, Canada (March 2002)
5. Hu, F., Hao, Q., Bao, K.: A survey on software-defined network and openflow: From concept to implementation. Communications Surveys Tutorials, IEEE 16(4), 2181–2206 (2014)
6. Kott, A., Wang, C., Erbacher, R.F.: Cyber Defense and Situational Awareness. Springer (2014)
7. Kouřil, D., Rebok, T., Jirsík, T., Čegan, J., Drašar, M., Vizváry, M., Vykopal, J.: Cloud-based testbed for simulation of cyber attacks. In: Network Operations and Management Symposium (NOMS), 2014 IEEE. pp. 1–6 (May 2014)
8. Kreutz, D., Ramos, F., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., Uhlig, S.: Software-defined networking: A comprehensive survey. Proceedings of the IEEE 103(1), 14–76 (2015)
9. Liu, P., Zang, W., Yu, M.: Incentive-based modeling and inference of attacker intent, objectives, and strategies. ACM Transactions on Information and System Security 8(1), 78–118 (2005)
10. Miller, D., Harris, S., Harper, A., VanDyke, S., Blask, C.: Security information and event management (SIEM) implementation. McGraw Hill Professional (2010)
11. Shameli-Sendi, A., Ezzati-Jivan, N., Jabbarifar, M., Dagenais, M.: Intrusion response systems: survey and taxonomy. Int. J. Comput. Sci. Netw. Secur 12(1), 1–14 (2012)
12. Čeleda, P., Čegan, J., Vykopal, J., Tovarňák, D.: KYPO - a platform for cyber defence exercises. In: STO-MP-MSG-133: M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization (2015)
13. Zonouz, S.a., Khurana, H., Sanders, W.H., Yardley, T.M.: RRE: A game-theoretic intrusion response and recovery engine. IEEE Transactions on Parallel and Distributed Systems 25(2), 395–406 (2014)