Coordination and Concurrency Aware Likelihood Assessment of Simultaneous Attacks

Léa Samarji[1,2(✉)], Nora Cuppens-Boulahia[2], Frédéric Cuppens[2], Serge Papillon[1], Wael Kanoun[1], and Samuel Dubus[1]

[1] Alcatel-Lucent Bell Labs, Villarceaux, route de Villejust, 91620 Nozay, France
{lea.el_samarji,serge.papillon,wael.kanoun,
samuel.dubus}@alcatel-lucent.com

[2] Télécom Bretagne, rue de la Chataigneraie, 35510 Cesson-Sévigné, France
{nora.cuppens,frederic.cuppens}@telecom-bretagne.eu

Abstract. To avoid improper responses against attacks, current systems rely on *Attack Likelihood* metric. Referring to *NIST*, *Attack Likelihood* considers: the attack's complexity, the attackers' motivation, and potential responses. Previous work on *Likelihood* assessment are limited to individual attacks, missing thereby coordination and concurrency aspects between attackers. Moreover, they do not fulfill all NIST factors. Hence, we propose in this paper a new framework to properly assess the Likelihood of Individual, Coordinated, and Concurrent Attack Scenarios (LICCAS). We are first based on a coordination aware-*Game Theoric* approach to derive an *Attack Likelihood* equation. Then, we propose an algorithm to assess the *Scenario Likelihood* of each attack scenario, considering the concurrency between attackers. We finally experiment LICCAS on a VoIP use case to demonstrate its relevance.

Keywords: Attack likelihood · Risk · Game Theory · Coordinated attacks · Concurrent attacks

1 Introduction

With the evolution of attack tools, information systems are frequently targeted by simultaneous attacks that can be independent, concurrent or even coordinated. Coordinated attacks can cause deterioration in system's performance, induce great damage to physical assets, and reach attack goals faster by distributing the charge between collaborating attackers. Therefore, solutions to model and forecast attack scenarios where attackers may coordinate or may be concurrent were proposed [1,2]. However, in order to avoid launching improper responses against predicted attacks, systems should first perform Attack Likelihood (AL) assessment. Referring to the National Institute of Standards and Technology (NIST), a proper AL assessment should consider: (1) the existence of responses against the attack, (2) the nature of the vulnerability, and (3) the attacker motivation. Several works have been undertaken to assess the AL [3–6],

J. Tian et al. (Eds.): SecureComm 2014, Part I, LNICST 152, pp. 524–529, 2015.
DOI: 10.1007/978-3-319-23829-6_37

but they all suffer several limitations: they do not consider an AL aware of the potential coordination or the concurrency that may exists between attackers, and none of them fulfills the three above mentioned NIST factors. To fill in those gaps, we propose a new framework to assess the Likelihood of Individual, Coordinated and Concurrent Attack Scenarios.

In order to take into account the possibility of being stopped by the response system in the decision process of the attacker, thereby fulfilling factor (1), our framework computes a probability of attacking strategy p^*, based on a game theoretic framework. *Game Theory* offers the possibility to calculate the probability of playing strategy considering not only the interests of a player, but also those of the opponent. Existing models that analyze the behavior of an attacker and a system as a game, consider that payoffs are common knowledge. However, it is impossible for an attacker to have a complete knowledge of the real damage that he/she can cause to the system, and of the real cost of a reaction launched by the system against him/her. And vice versa, the system can not exactly know the reward that an attacker can get when he/she succeeds a certain attack, neither how much this attack will cost the attacker. Hence, to properly compute p^*, we propose a coordination-aware estimation of each player's payoffs from the standpoint of its opponent, based on the National Vulnerability Database (NVD)[1]. The attacker's motivation and the nature of the vulnerability (factors (2) and (3)) are considered by defining a Return On Attack Investment (ROAI). ROAI represents the effort/cost that an attacker invests to accomplish its attack, compared to the gain earned once the attack is successfully executed. Our framework also includes a new algorithm LSS (Likelihoods of Simultaneous Scenarios), to consider the interaction between concurrent attackers. Based on a Simultaneous Attacks Graph (SAG) [2] containing predicted scenarios for simultaneous attacks, and our AL equation, LSS calculates the likelihood of each attack scenario, including ones blocked due to concurrency with other attackers.

The paper is organized as follows: In Sect. 2, we propose our game model to calculate p^*, and then we define ROAI, to finally propose an AL equation. In Sect. 3, we propose LSS algorithm. Finally, Sect. 4 concludes our work.

2 Attack Likelihood Assessment Based on Game Theory

The most appropriate game model, in our case, is a two-players nonzero-sum, and non-cooperative game. First, the attack entity's gain is not always equal to the system's loss. Second, coordinated attackers do not attack each others. Therefore, we consider a two-players game model for each couple of attack entity on one side and the defending system on the other side. An attack entity can be either a single attacker, or a Group of Coordinated Attackers (GCA). We represent our game with two 2×2 matrices: the first (Table 1) represents the attacker-centric payoffs, and the second (Table 2) represents the defending system-centric payoffs. Contrarily to other existing work, we think that payoffs can not be considered as common knowledge for both players. Hence, each player-centric payoffs should

[1] http://nvd.nist.gov/cvss.cfm.

Table 1. $E_S(M_{attacker})$.

	React	Not React
Attack	-$E_S(Attack\_Cost)$	$E_S(Reward)$ - $E_S(Attack\_Cost)$
Not Attack	**Hacker:** 0	
	Vandal: $E_S(DR\_Cost)$	0

Table 2. $E_A(M_{System})$.

	React	Not React
Attack	-$E_A(DR\_Cost)$	-$E_A(Impact)$
Not Attack	-$E_A(DR\_Cost)$	0

be estimated from its opponent's standpoint. Let $E_A(x)$ and $E_S(x)$ be the estimations of the term x respectively from an attacker standpoint and a system standpoint.

As demonstrated in [4], there is no pure strategy NE for such a game. Therefore, as in [3], we extend the analysis by considering mixed strategies of players defined as probability distributions on the space of their pure strategies. Let p and $1-p$ (resp. q and $1-q$) be the probabilities for strategies *Attack* and *Not Attack* (resp. *React* and *Not React*) of the attack entity (resp. the system). The pair $(p^*; q^*)$ is said to constitute a NE solution to our game if the payoffs of both attack entity and the defending system are optimum. Hence, the following payoff functions of both players must be maximized:

$E_S(Payoff_{AttackEntity}) = [p^\star\ (1-p^\star)] \times E_S(M_{attacker}) \times [q^\star\ (1-q^\star)]^T$;
$E_A(Payoff_{System}) = [p^\star\ (1-p^\star)] \times E_A(M_{system}) \times [q^\star\ (1-q^\star)]^T$;

The solution to the set of inequalities derived from the payoff functions constitutes the unique NE of the game. The following probability of *Attack* strategy p^* can be derived from these inequalities.

$$p^* = \frac{E_A(DR\_Cost)}{E_A(Impact)}; \tag{1}$$

Notice that, p^* depends on: (1) the investment cost of the system in the detection and response process, and (2) the impact of the attack on the system. This result can be interpreted as follows: it is more likely for an attack entity to choose to attack, if she estimates that the detection and response process cost for the system is very high. Additionally, the lower is the impact on the system, the higher is the probability of attacking, because responding to this attack would not be a priority for a system threatened by simultaneous attacks.

An attack entity is more likely to perform the attack that brings the highest return on its investment. In other words, the likelihood of executing an attack depends on the effort (*Attack_Cost*) that an attack entity invest to accomplish it, compared to the *Reward* earned once the attack succeeds. We, thus, define a Return on Attack Investment ROAI (see Eq. 2).

$$ROAI = \frac{E_S(Reward) - E_S(Attack\_Cost)}{E_S(maxReward) + E_S(maxAttack\_Cost)} \quad (2)$$

Finally, we define AL, in Eq. 3, as the product of ROAI and p^*.

$$AL = \frac{E_S(Reward) - E_S(Attack\_Cost)}{E_S(maxReward) + E_S(maxAttack\_Cost)} \times \frac{E_A(DR\_Cost)}{E_A(Impact)} \quad (3)$$

In order to leverage an estimation for each term in AL equation, we are based on NVD. This latter supports the Common Vulnerability Scoring System which provides an open framework for communicating characteristics IT vulnerabilities (e.g. impact, exploitability and the existing responses related to an attack).

In order to consider the collaboration between attackers in our framework, some of these terms are expressed regarding the number of attackers participating in an attack. For instance, $E_S(Attack\_Cost(a))$ depends on three factors: (1) The difficulty in exploiting attack a, $Exploitability(a)$ which can be extracted from CVSS. (2) The number of coordinated attackers $\mid GCA \mid$ performing a. We note that the higher is $\mid GCA \mid$, the shortest is the time needed to achieve a, and the less is the effort made by every attacker. And (3) the effort in terms of required Number of Atomic Actions (ANA) to succeed attack a. For instance, in a vertical port scanning, ANA is equal to the half of the number of well known ports in a machine. For 1024 ports, we estimate that in average, with 512 scanned ports, attackers can find opened ports in which they are interested. Thus, $E_S(Attack\_Cost(a))$, that we propose in Eq. 4 should increase when $Exploitability(a)$ or $ANA(a)$ grows, and should decrease when $\mid GCA \mid$ grows.

$$E_S(Attack\_Cost(a)) = \frac{1}{Exploitability(a)} \times \frac{ANA(a)}{\mid GCA(a) \mid}; \quad (4)$$

3 Scenario Likelihoods (SL) of Simultaneous Attacks

In order to efficiently assess the SL of an attack scenario, we define a number of claims describing SL evolution, considering the interaction with other simultaneously ongoing scenarios.

Claim 1. *If an attack scenario S_i blocks another simultaneous one S_j from continuing its scenario, then both scenarios should have the same SL.*

As explained in [2], simultaneous attackers may be concurrent, and thus, block each others. In such a case, the probability of having scenario S_j blocked is equal to that of having S_i executed until the end.

Claim 2. *A scenario containing time breaks (No Operations) should have a lower likelihood than the same one without breaks.*

Claim 3. *The SL increases when the attack entity gets closer to its goal.*

To fulfill this claim, we calculate the SL as the product of ALs of the actions (attacks or No Operations) composing the scenario (see Proposition 1) .

Proposition 1. *If $S_K = \{a_1, a_2, \ldots, a_n\}$ is a scenario of n actions, AL_i is the AL of a_i, and SL_k is the SL of S_k, then $SL_k = AL_1 \times AL_2 \times \ldots \times AL_n$.*

Suppose that one SAG^i predicted the following sequence for an attack entity A: $S_K^i = \{a_1, a_2, a_3, a_4\}$. Suppose that after a time duration T sufficient for attackers to progress in their scenarios, we regenerate another set of attack graphs, and one of them predicts the following sequence for A: $S_K^{i+T} = \{a_2, a_3, a_4\}$. This means that during T, A has executed the first attack a_1 of the sequence predicted in SAG^i. If SL_k^i is the SL of S_K^i, SL_K^{i+T} is the SL of S_K^{i+T}, and AL_1 is the AL of a_1, then applying Proposition 1, we have $SL_K^i = AL_1 \times SL_K^{i+T}$. Referring to Eq. 3, AL is always smaller than one ($AL_1 \leq 1$). Thus, $S_K^{i+T} \geq S_K^i$. Consequently, Proposition 1 fulfills Claim 3.

In order to compute SLs taking into account all the above mentioned claims, we propose LSS algorithm. LSS takes all the attacks scenarios figuring in a given attack graph SAG, to generate a SL for each scenario. LSS proceeds as following: First, it starts by calculating the AL for each attack, applying Eq. 3. Then, it computes likelihoods for No operations, fulfilling by this Claim 2. Finally, it applies Proposition 1 to computes the SL of each scenario, taking into consideration blocked scenarios and fulfilling by this Claims 1 and 3.

4 Conclusion and Future Work

We proposed a new framework to assess the likelihood of simultaneous attack scenarios considering the factors defined by NIST. Being able to model the possibility of reaction by the response system, in the decision of the attacker, *Game Theory* provides the most adequate framework to propose an Attack Likelihood AL equation. This latter considers the number of collaborating attackers, making our model able to consider coordinated attacks. Moreover, our framework includes an algorithm that computes the likelihood of a whole attack scenario, considering the concurrency with other simultaneous scenarios. Due to our work, systems can prioritize the most likely attack scenarios and properly react against them. As a future work, we intend to leverage means to properly estimate each term in our AL equation, and apply our framework on a VoIP use case.

References

1. Braynov, S., Jadliwala, M.: Representation and analysis of coordinated attacks. In: Proceedings of the 2003 ACM Workshop on Formal Methods in Security Engineering, FMSE 2003, NY, USA, pp. 43–51 (2003)
2. Samarji, L., Cuppens, F., Cuppens-Boulahia, N., Kanoun, W., Dubus, S.: Situation calculus and graph based defensive modeling of simultaneous attacks. In: Wang, G., Ray, I., Feng, D., Rajarajan, M. (eds.) CSS 2013. LNCS, vol. 8300, pp. 132–150. Springer, Heidelberg (2013)
3. Alpcan, T., Başar, T.: A game theoretic approach to decision and analysis in network intrusion detection. In: Proceeding of the 42nd IEEE Conference on Decision and Control, Maui, HI, pp. 2595–2600, December 2003

4. Liu, Y., Comaniciu, C., Man, H.: A Bayesian game approach for intrusion detection in wireless ad hoc networks. In: Proceeding from the 2006 Workshop on Game Theory for Communications and Networks, GameNets 2006, NY, USA. ACM (2006)
5. Kanoun, W., Cuppens-Boulahia, T., Cuppens, F., Dubus, S., Martin, A.: Success likelihood of ongoing attacks for intrusion detection and response systems. In: Proceedings IEEE CSE 2009, 12th IEEE International Conference on Computational Science and Engineering, Vancouver, Canada. IEEE Computer Society (2009)
6. Zhu, Q., Tembine, H., Basar, T.: Network security configurations: a nonzero-sum stochastic game approach. In: American Control Conference (ACC) 2010, pp. 1059–1064 (2010)