Cyber-Attack Risks Analysis Based on Attack-Defense Trees

Wenjun Sun[1(✉)], Liqun Lv[1], Yang Su[1], and Xu An Wang[1,2]

[1] Department of Electronic Technology,
Engineering University of the People's Armed Police Force,
Xi'an, Shaanxi, China
sunwenjun94@163.com
[2] Xidian University, Xi'an, Shaanxi, China

Abstract. Considering the lack of theoretical analysis for systems under complicated attacks, a framework was proposed to analyze attack risks based on attack-defense trees. The attack period was divided into attack phase and defense phase and metrics was defined. First, action nodes were constructed by collecting system vulnerabilities and capturing invasive events, and defense strategies were mapped to defense nodes in the tree structure. Besides, formal definitions were given and attack-defense tree with metrics was constructed using ADTool and relevant algorithms. In addition, concepts of ROA (Return on attack) and ROI (Return on Investment) were introduced to analyze system risk as well as to evaluate countermeasures. Finally, a risk analysis framework based on attack-defense trees was established and numerical case was given to demonstrate the proposed approach. The result showed that the framework could clearly describe the practical scenario of the interaction between attacks and defenses. The objective of risk analysis and countermeasures evaluation could be achieved.

1 Introduction

Cyber-attacks are becoming one of the main threats of cyber security of critical infrastructures (CI) and information systems since the last decade [1]. Recent cyber-crimes and cyber espionages have shown that stealthy and sophisticated attacks, such as advanced persistent threats (APT) will do great harm to information systems. For example, the famous security corporation RSA suffered from the compromise of private key server; Google e-mail servers were infiltrated and intercepted and the clients' information was leaked. Great economic and reputational damage came with such cyber-attacks [2].

Considerable countermeasures have been taken for the sake of information systems security. However, most current defending techniques based on border protection are of little effect faced with targeted and complicated attacks because they mainly focus on one-shot known types [3]. But to improve information protection, the interaction between attackers and defenders must be considered.

In this paper, a risk framework based on attack-defense trees to analyze the cyber-attack risks by calculating the benefits of both sides is proposed. Several metrics

L. Barolli et al. (eds.), *Advances in Internetworking, Data & Web Technologies*,
Lecture Notes on Data Engineering and Communications Technologies 6,
DOI 10.1007/978-3-319-59463-7_67

were defined as quantitative analysis. ROA (Return on attack) and ROI (Return on Investment) were introduced to illustrate the impact of taking relative countermeasures towards attacks. Besides, algorithms of how to generate attack-defense trees were given and ADTool [4, 5] was made use of as well. At last, the approach was demonstrated through a numerical case.

The remainder of the paper is as follows. In Sect. 2 we summarize related work on modeling attack and defense with tree structure. Our own framework is declared in Sect. 3. Application and numerical illustrations are depicted in Sect. 4. Finally, we discuss our results and draw conclusions.

2 Related Work

Attack tree has been widely utilized to systemically analyze attacks risks, which can implicitly illustrate the attack path. The concept of attack tree model was first introduced by Schneier [6]. In [7], the attack tree model was extended by adding attack scenarios and profiles. However, attack tree only works from the perspective of attackers and is complicated in visualization. To show the effect of defense mechanism, Edge et al. proposed protection trees from the perspective of defenders [8]. In [9], Bistarelli et al. proposed the defense tree model. But neither the protection tree nor defense tree is able to be employed without attack tree. To solve this problem, Roy et al. introduced attack countermeasure tree to combine attack and defense yet it's too complicated to be realized [10].

In [11, 12], Kordy et al. proposed attack-defense tree (ADTree) which combines attack tree and defense tree to one structure. ADTree describes the interactions between attacker and defender and the iterative counteraction for after the actions of both. Therefore, it can clearly show the system risks before and after the implementation of countermeasures towards specific domains. For the convenience of application, Kordy et al. later proposed tree construction tool namely ADTool to generate ADTree. By numerating system risks due to vulnerabilities and attack success possibility, the ADTree can be well applied to practical cases such as vehicle network [13] and CPS network [14] hence we employ it as the foundation of our analysis.

3 Modeling with ADTree

3.1 Attack-Defense Tree Model

In an attack-defense tree model, the scenario is divided into the attack phase and defense phase and the properties are abstracted as nodes. The targeted node of the attacker is the root of the tree and to complete his compromise, the attacker has to start exploiting from the leaf node and move progressively layer by layer until managing the invasion of the root node. Meanwhile, the defenders have to take countermeasures relative to each node in the attack path to keep the attacker from continuing his move. Attention that during each move of both sides there is a cost of move. To better understand the model, the formal definition of ADTree is as the following.

Definition 1. The ADTree is a triad $ADT = (N, E, R)$. $N = (N_a, N_b)$ is the set of nodes the tree while N_a represents the set of attack nodes which is also the property node of the system compromised and N_d represents the set of defense nodes which, in other words, represents the defense countermeasures. We also define $Pa(N)$ as the parent node set of N. $E = \left(N_i, N_j\right)$ represents the edge between N_i and N_j. $R = (AND, OR)$ is defined as the relations of attacks. In this paper, the basic relation operators are "AND" and "OR", which mean that the attacker/defender has to complete all his attack/defense to move on to the higher layer and the attacker/defender just needs to complete at least one respectively.

An instance is given in Fig. 1 to illustrate the structure of ADTree. Notice that the circular nodes are the attack nodes and the rectangular nodes represent the defense nodes. Corresponding defense countermeasures are depicted as the dotted line. Child nodes with arc represent *AND* operation nodes while those without represent OR operation nodes.

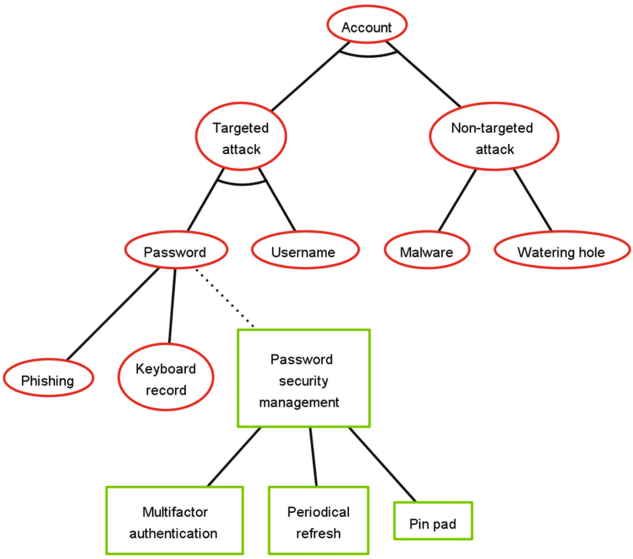

Fig. 1. An instance of attack-defense tree. This shows the possible attack path of illegally obtaining accounts and corresponding countermeasures towards password safety

3.2 Risk Analysis Framework with ADTree

Based on the ADTree theory and some concepts in [14], we establish the risk analysis framework by introducing several metrics. Our goal is to evaluate the risks resulting from potential attacks and the effects of countermeasures undertaken.

Step 1. Understanding system vulnerability
Attackers always take good advantage of vulnerabilities to exploit information system. It cannot be denied that some cyber-attacks, APT attacks for example, utilizes unidentified vulnerabilities such as 0 day vulnerabilities, but most do not. Common

system vulnerabilities could be found on the lists of CVE (Common Vulnerabilities and Exposures) and defenders can score them with CVSS (Common Vulnerabilities Scoring System)[1].

Step 2. Gathering attack information
After understanding system vulnerabilities, corresponding countermeasures should be made and attack path should be predicted according to the occurrence probability and extent of damage. Defense cost need to be taken into consideration as well. Attack information such as attack target, attack nodes, attack success probability, attack/defense cost and impact loss could be obtained from detection of attacks and vulnerability scanning. Besides, attack behavior database is also reference which needs regular updates. For the sake of convenience, definitions of such information are as follows.

Definition 2. Attack success probability p_i: the possibility of successfully committing an attack through risk $i(i = 1, 2, \ldots, m)$ which ranges from 0 to 1.

Definition 3. Attack cost $c_i \in (0, \infty)$: the resource required to commit an attacks, including human resource and physical resource needed.

Definition 4. Defense cost $d_i \in (0, \infty)$: the resource required to undertake countermeasures, capital of purchasing and employing security equipment and human resource included.

Definition 5. Potential loss l_i: the potential loss that may be resulted from attacking through risk i and can be divided into 1 to 10 levels according to the severity.

Step 3. Constructing ADTree
After completing step 1 and step 2, it is necessary to construct ADTree model for attack and defense

The risk i is composed of atom attacks numbering $1, 2, \ldots, n$ and can be expressed as the son nodes of one attack node. For the simplicity of calculation and comparison, monetary unit is introduced as a measure of attack costs and protection costs. Human resource consumed can be regards as monetary units, such as 100 *dollars* per hour. Assuming that the attacker employs his attack through risk i at time t, the defender shall undertake responding measures at time $t + 1$ after monitoring the attack. Therefore, the values of c_i, d_i and l_i shall change as a result of defense action. t is regarded as the attack time and $t + 1$ as the defense time. First, the expressions of metrics at attack time are as shown in Table 1. Notice that under the different relations of "AND" and "OR", the expressions differ.

Extents of system risk can be reflected in p_i and l_i. The greater p_i and l_i are, the more risks the system is facing. Besides, attack cost matters and rational attackers tend to choose the attack profile which costs less. As a consequence, system risk assessment metrics $r_i(t)$ can be expressed as

[1] Available at https://www.first.org/cvss.

Table 1. Metric equation during attack phase (t)

	AND	OR
Attack success probability	$p_i(t) = \prod_{k=1}^{n} p_k(t)$	$p_i(t) = 1 - \prod_{k=1}^{n} (1 - p_k(t))$
Attack cost	$c_i(t) = \sum_{k=1}^{n} c_k(t)$	$c_i(t) = \frac{\sum_{k=1}^{n} p_k(t) \times c_k(t)}{\sum_{k=1}^{n} p_k(t)}$
Potential loss	$l_i(t) = \frac{10^n - \prod_{k=1}^{n} (10 - l_k(t))}{10^{n-1}}$	$l_i(t) = Max_k^n(l_k(t))$

$$r_i(t) = \frac{p_i(t) \cdot l_i(t)}{c_i(t)} \tag{1}$$

Now that the basic metrics have been defined, it is important to construct ADTM (ADTree with metrics). The key algorithm pseudocode is as follows.

```
Algorithm 1 ADTM_generation( ADT, metrics, r )
input: ADT = (N_a, E, R) , metrics = ( p, c, l )
output: ADTM = ( N_a, E, R, p, c, l, r )
init ADTM ;    /* Initialize each metric of ADTM empty */
set N_a, E, R ;    /* Copy each attack node, edge and relation of ADT to
N_a, E, R */
for (each leaf node i in ADT )
    set p_i, c_i, l_i ;
end for (03)
for(each parent node j )
    if ( metrics(j) == null && metrics(childnode(j)) != null )
        compute p_j, c_j, l_j ;
        compute r_i ;
        j = parentnode(j) ;
    else if ( k == childnode(j) && metrics(k) == null )
        j = k ;
    end if (07)
end for (06)
return ADTM
```

Step 4. Countermeasures implementation

The defender implements corresponding countermeasures to counter with attacks or to diminish the possibility of potential attacks hence the attack cost, defense cost and potential loss are not as the same as what they are at *t*. It is difficult to determine the value of attack success probability p_i as it changes as the attack-defense environment.

First, for the convenience of analysis, assuming that p_i keeps stable during the time interval $[t, t+1]$ namely $p_i(t) = p_i(t+1)$.

Define the increment of attack cost due to the implementation of defense actions as $\Delta c_k(t)$ at $t+1$. Theoretically, $\Delta c_k(t)$ is proportional to the value of defense cost. With the scale factor λ, the incremental equation is as follows:

$$\Delta c_k(t) = \lambda \times d_k(t) \tag{2}$$

λ is influenced by security strategy, security operation and personnel training. Meanwhile the potential loss can be updated at $t+1$

$$l_i(t+1) = \alpha \times l_i(t) \tag{3}$$

where $\alpha = 1 - \varphi$ represents surplus factor as a representative of the vulnerability rate that cannot be repaired due to the capability constraints of defenders. The formulation of φ is defined as

$$\varphi(t+1) = \frac{N_g(t+1)}{N_c(t+1)} \tag{4}$$

where N_g represents the number of vulnerability that can be repaired through undertaking countermeasures and N_c represents the number that cannot. From the equations above, metrics at $t+1$ can be derived as numerated in Table 2.

Table 2. Metric equation during defense phase $(t+1)$

	AND	OR
Defense cost	$d_i(t+1) = \sum_{k}^{n} d_k(t+1)$	$d_i(t+1) = \frac{\sum_{k=1}^{n} p_k(t) \times d_k(t+1)}{\sum_{k=1}^{n} p_k(t)}$
Attack cost	$c_i(t+1) = \sum_{k=1}^{n} c'_k(t)$	$c_i(t+1) = \frac{\sum_{k=1}^{n} p_k(t) \times c'_k(t)}{\sum_{k=1}^{n} p_k(t)}$
Potential loss	$l_i(t+1) = \sum_{k}^{n} \alpha \times l_k(t)$	$l_i(t+1) = Max_{k=1}^{n}(\alpha \times l_i(t))$

Step 5. Risk analysis

In order to evaluate system risk, the concepts of *ROA* (Return on Attack) and *ROI* (Return on Investment) are defined as follows.

Definition 6. *ROA*: the expected return rate of the attacker after his investment on the attacks. Its formulation is

$$ROA(t+1) = \frac{p_i(t) \times l_i(t+1)}{c_i(t+1)} \tag{5}$$

Definition 7. *ROI*: the expected return rate of the defender after his investment on the defense actions for the system security. Its formulation is

$$ROI = \frac{\Delta ALE}{CI} \tag{6}$$

In (6), ΔALE is the differential of loss resulting from the attacker after and before the implementation of countermeasures, expressed as $ROA(t+1) - ROA(t)$. While *CI* is the countermeasures cost of defenders which can also be represented as $d(t+1)$. The reason to define as this is to associate *ROA* and *ROI* to evaluate the effects of countermeasures. Consequently, (6) is turned to

$$ROI = \frac{ROA(t+1) - ROA(t)}{d(t+1)} \tag{7}$$

Now it's necessary to update Algorithm 1 to generate UADTM (updated ADT with metrics). The key algorithm pseudocode is as follows.

Algorithm 2. UADTM_generation($ADTM$, N_d , d)
input: $ADTM = (N_a, E, R, p, c, l, r)$, N_d , d
output: $UADTM = (N_a, N_d, E, R, p, c, l, ROA, ROI)$
init $UADTM$;
set N_a, E, R, p, c, l, r ;
if ($defense\_state[i] == True$)
    insert N_{di} ;
    set d_i ;
end if (03)
for(each defense node i)
   compute d_i ;
end for (07)
for(each parent node j)
   if ($childnode(j) \in N_d$)
        update $metrics(j)$;
    else if ($updates(metrics(childnode(j))) == True$)
        update $metrics(j)$;
    end if (11)
end for (10)
compute ROA , ROI ;
return $UADTM$

Considering that system risk can be represented with attack utility, it's reasonable that *ROA* and $r(t)$ have the same expression to simplify the analysis. Therefore, the risk value is substituted by *ROA* in Algorithm 2.

From the perspective of the attacker, the goal is to maximizing *ROA* while minimizing the attack cost; while for the defender, the goal is to maximizing *ROI* while keeping the defense cost to the least level. Therefore, the defender shall consider how to minimize *ROA* and for the attacker, on the contrary, is to minimize *ROI*.

4 Risk Analysis Framework

In this section, a framework towards network attacks will first be established according to the metrics and definitions above, as shown in Fig. 2. Then numerical illustrations are given as a demonstration.

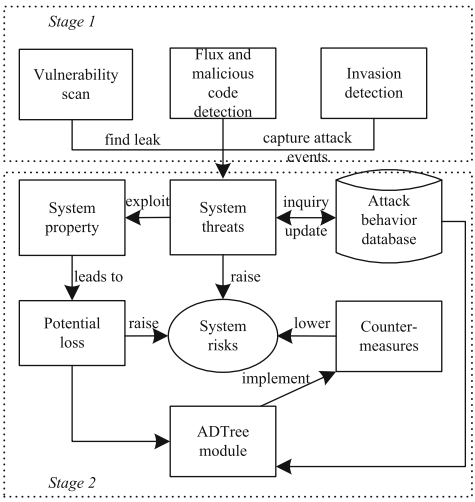

Fig. 2. Framework of system risk analysis based on ADTree including two stages

4.1 Framework Construction

Based on the approach given, the framework of network risk analysis could be established as follows. The process is composed of the system risk understanding and the construction of ADTree.

Stage 1. Understanding system risks

The main task in this phase is to collect system vulnerability and attack information detected.

First, network properties shall be modeled and assigned values. Then techniques such as vulnerability scanning, flux monitoring and malware detection are utilized to understand the risk information. Besides, potential attack path could be illustrated and

the loss shall be estimated thru the inquiry of attack behavior database. Risks can also be scored referring to CVSS.

Stage 2. Establishing attack-defense tree analysis framework

After gathering the necessary information, relative metrics before and after the implementation of countermeasures need to be taken into consideration. Based on the five steps proposed, analysis framework could be established through the following three steps.

(1) ADTree construction. By employing ADTool, input the values of the parameters at t and construct the tree based on Algorithm 1 proposed to generate ADTM.
(2) Countermeasures undertaken. System metrics change at the defense time $t + 1$ and need to be updated and generate UADTM based on Algorithm 2.
(3) Risk evaluation. After generating ADTM and UADTM, values of *ROA* and *ROI* of each node need to be calculated as the reference.

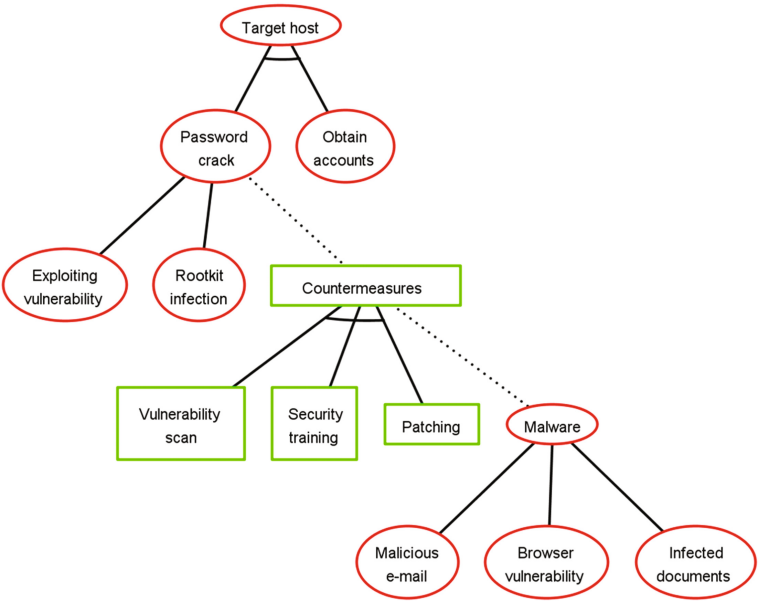

Fig. 3. ADTree structure for modeling attack path and corresponding countermeasures

4.2 Numerical Illustrations

In this section, numerical illustrations are given to demonstrate the framework proposed. As for the possible attack path, we consider Night Dragon attack [15], one example of APT attacks, whose goal is to infect target hosts, install remote control tools, establish stealthy transfer tunnel and steal confidential documents. The ADTree of the attack and some defense actions are shown in Fig. 3.

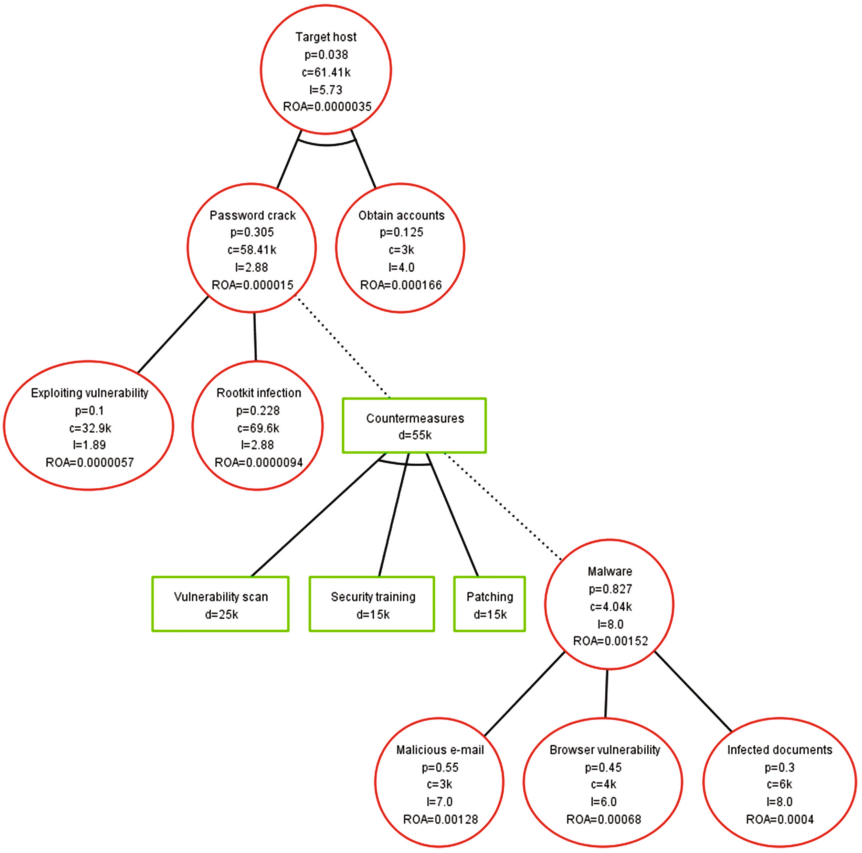

Fig. 4. ADTree structure for modeling attack path and corresponding countermeasures with metrics. This structure is in the case of $\lambda = 0.5, \alpha = 0.3$

In the case of $\lambda = 0.5, \alpha = 0.3$, the updated metrics are shown in Fig. 4. The calculation of each metric has been defined in the previous page. As is shown in Fig. 4 and Table 3, when the defender implements countermeasure worth 55 k dollars toward the node of *password crack*, the attack cost increment is 22.81 k dollars. Attention that for the convenience of analysis, attack success possibility p is assumed to remain unchanged. The loss impact drops from 7.78 to 5.53 and the values of *ROA* diminishes by 54.55%. It can be inferred that by taking specific defense actions, the risk of

Table 3. Metric values and variations of the password crack node

Metrics	Values before defense	Values after defense	Variations
ROA	0.0000077	0.0000035	−54.55%
p	0.038	0.038	–
c	38.6 k	61.41 k	+59.09%
l	7.78	5.73	−26.35%
d	0	55 k	–

password cracked reduces by 54.55%. From Fig. 4, it can also be inferred that both the attacker and defender can learn from the interaction of attack-defense. Considering the persistent characteristics of current cyber-attacks, the process can be derived iteratively between the attacker and defender. The closer is the attack node to the root node, the more the corresponding defense cost is while defense cost comes to the least on the leaf nodes. This illustrates that countermeasures should be implemented as soon as the attack has been detected. Besides, attacks might be deterred if the attack cost is too high while the return on attack is little as a consequence of defense actions.

5 Conclusion

Considering the interaction of the attacker and defender, a framework of tree structure to evaluate the system risks caused by network attacks was established based on the theory of attack-defense tree. By constructing ADTree for specific attack-defense scenario and calculating the values of return on attack, the risks of specific attack before and after the implementation of defense actions can be compared quantitatively. The paper also suggests that the defender should take defense measures as soon as possible once the detection of attacks. In addition, taking specific countermeasures may possibly deter attackers as a result of the increase of attack costs and decline in return. In the future work, optimal strategy will be studied instead of the just given statics. Besides, attackers are assumed to be rational to choose the least cost route in this paper. Behaviors of irrational attackers and specific scenarios will also be studied in the future work to extend the proposed framework.

Acknowledgments. This work was partially supported by the National Natural Science Foundation of China (61572521).

References

1. Bencsáth, B., Pék, G., Buttyán, L., Felegyhazi, M.: The cousins of stuxnet: Duqu, flame, and gauss. Future Internet **4**(4), 971–1003 (2012)
2. Virvilis, N., Gritzalis, D.: The big four-what we did wrong in advanced persistent threat detection? In: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), pp. 248–254. IEEE, September 2013
3. Laszka, A., Johnson, B., Grossklags, J.: Mitigating covert compromises. In: International Conference on Web and Internet Economics, pp. 319–332. Springer, Heidelberg, December 2013
4. Kordy, B., Kordy, P., Mauw, S., Schweitzer, P.: ADTool: security analysis with attack–defense trees. In: International Conference on Quantitative Evaluation of Systems, pp. 173–176. Springer, Heidelberg, August 2013
5. Gadyatskaya, O., Jhawar, R., Kordy, P., Lounis, K., Mauw, S., Trujillo-Rasua, R.: Attack trees for practical security assessment: ranking of attack scenarios with ADTool 2.0. In: International Conference on Quantitative Evaluation of Systems, pp. 159–162. Springer International Publishing, August 2016

6. Schneier, B.: Attack trees. Dobb's J. **24**(12), 21–29 (1999)
7. Moore, A.P., Ellison, R.J., Linger, R.C.: Attack modeling for information security and survivability. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst (No. CMU-SEI-2001-TN-001) (2001)
8. Edge, K.S., Dalton, G.C., Raines, R.A., Mills, R.F.: Using attack and protection trees to analyze threats and defenses to homeland security. In: IEEE Military Communications Conference, MILCOM 2006, pp. 1–7. IEEE, October 2006
9. Bistarelli, S., Fioravanti, F., Peretti, P.: Defense trees for economic evaluation of security investments. In: The First International Conference on Availability, Reliability and Security, 2006, ARES 2006, pp. 8–pp. IEEE, April 2006
10. Roy, A., Kim, D.S., Trivedi, K.S.: Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees. Secur. Commun. Netw. **5**(8), 929–943 (2012)
11. Kordy, B., Mauw, S., Radomirović, S., Schweitzer, P.: Foundations of attack–defense trees. In: International Workshop on Formal Aspects in Security and Trust, pp. 80–95. Springer, Heidelberg, September 2010
12. Kordy, B., Mauw, S., Radomirović, S., Schweitzer, P.: Attack–defense trees. J. Logic Comput. **24**, 55–87 (2012). exs029
13. Du, S., Li, X., Du, J., Zhu, H.: An attack-and-defence game for security assessment in vehicular ad hoc networks. Peer-to-peer Netw. Appl. **7**(3), 215–228 (2014)
14. Ji, X., Yu, H., Fan, G., Fu, W.: Attack-defense trees based cyber security analysis for CPSs. In: 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pp. 693–698. IEEE, May 2016
15. Wueest, C.: Targeted Attacks Against the Energy Sector. Symantec Security Response, Mountain View (2014)