Bulletin de la Société Royale des Sciences de Liège, Vol. 86, *special edition*, 2017*, p.* 474 - 483

A framework to achieve dynamic model of cyber battlefield

Mohammad SHAKIBAZAD[1]*, AliJabar RASHIDI[2]

[1]Associate Professor, Faculty of electrical engineering, Malek-Ashtar University of Technology, Tehran, Iran

[2]Ph.D. candidate, IT engineering, Security branch, Malek-Ashtar University of Technology, Tehran, Iran

* Corresponding Author's E-mail: Shakibazad@mut.ac.ir

Abstract

With fast growth of cyber space and related network infrastructures, it is important to detect the intrusion and respond to it in a timely manner. Cyber-attacks are in progress and are becoming more complex, as a result, more sensitive and more difficult to defend cyberspace. To determine the best response to cyber-attacks and cyber protection are cyber situation awareness. To achieve this goal, we require a framework to provide the possibility of cyber maneuvers. In this research running cyber maneuvers by simulating the dynamic cyber battlefield. Cyber battlefield contains the information necessary to detect cyber incidents. This paper aims to present a novel method for integrated model of cyber battlefield. It is necessary to execution cyber maneuvers to achieve cyber situation awareness. In this cyber defense model, situation awareness presents useful information (in a real time) to the analyst cyber space. The present study presents a framework of cyber situation awareness for accurate inspection of the current situation of cyber battlefield and cyber maneuvers. this method would be successful in exposing cyber threats for timely response.

Keywords: Cyber situation awareness, Cyber maneuver, Cyber space simulator, Cyber battlefield

1- Introduction

With the progress of cyber infrastructure, cyber-attacks are progressing and getting more complicated. With the extreme complexity of computer networks, the complexity of defense against cyber-attacks is increased and some methods and techniques are proposed against the attacks. To determine the best response to cyber-attack and learning of success and failures in the systems, a framework of cyber situation awareness should exist to detect the target of attack, predict the probable attacks and protect the cyber environment. Situation awareness is a cognitive process including the conditions of environment, understanding their meanings and projecting their future status.

By improvement of cyber situation awareness via information fusion, we can achieve useful information in a real time. Cyber-attacks can create malicious consequences in military systems and non-military network infrastructures (e.g. SCADA systems of electricity network, water utilities and bank systems) [1].

Before performing defensive, reconstructive and retaliatory actions against the cyber-attacks, the managers of network should achieve situation awareness to identify, perceive and predict the continuous varying threats. A comprehensive understanding of systems and their relevant threats to guaranty the security and integrity of operation is a necessity including evaluation of adverse effect of attacks on cyber environment components. As it was said, a situation awareness system presents useful information (in a real time) to the analyst.

The purpose of situation awareness models is presenting situation awareness-based cyber environment defense tools as it leads to true and timely decision making against cyber-attacks. The presented framework consists of an integrated model [2].

situation awareness is being aware of what is occurred in the surrounding network and enviornment. Situation awareness is a cognitive process which can percieve the present situation of network and take a decsion after the perception of their meaning [3][5].

2- Conceptual view of architecture of cyber battlefield

In the conceptual view, the architecture of cyber battlefield (Figure 1) and its relationship with other systems are shown. The relevant subsystems of battlefield include information fusion engine and cyber-attack simulator [4].

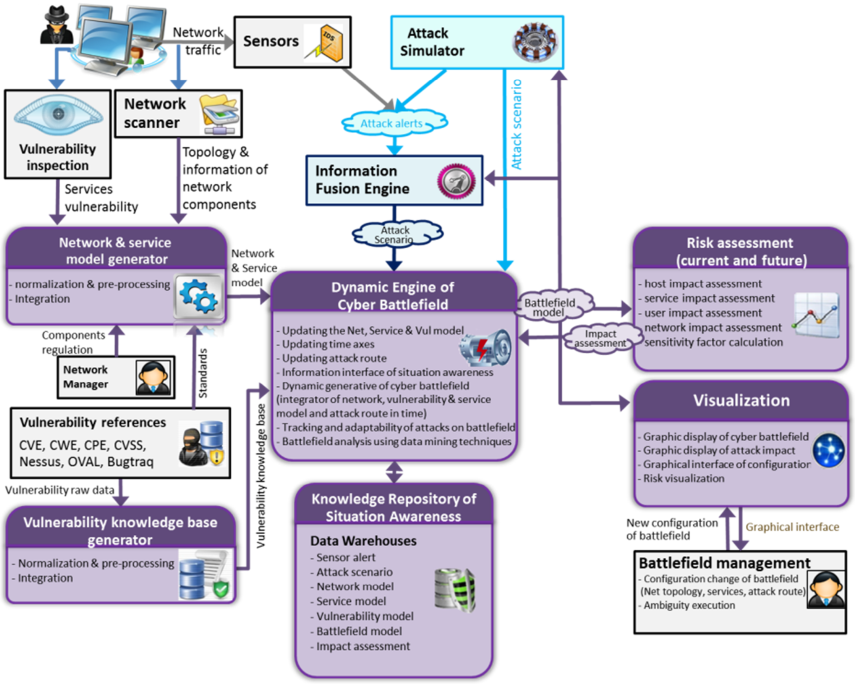

Network traffic
Sensors
IDS
Attack Simulator
Vulnerability inspection
Network scanner
Attack alerts
Attack scenario
Topology & information of network components
Services vulnerability
Information Fusion Engine
Attack Scenario
Network & service model generator
- normalization & pre-processing
- Integration
Network & Service model
Dynamic Engine of Cyber Battlefield
- Updating the Net, Service & Vul model
- Updating time axes
- Updating attack route
- Information interface of situation awareness
- Dynamic generative of cyber battlefield (integrator of network, vulnerability & service model and attack route in time)
- Tracking and adaptability of attacks on battlefield
- Battlefield analysis using data mining techniques
Battlefield model
Impact assessment
Risk assessment (current and future)
- host impact assessment
- service impact assessment
- user impact assessment
network impact assessment
sensitivity factor calculation
Components regulation
Network Manager
Standards
Vulnerability references
CVE, CWE, CPE, CVSS, Nessus, OVAL, Bugtraq
Vulnerability raw data
Vulnerability knowledge base
Vulnerability knowledge base generator
- Normalization & pre-processing
- Integration
Knowledge Repository of Situation Awareness
Data Warehouses
- Sensor alert
- Attack scenario
- Network model
- Service model
- Vulnerability model
- Battlefield model
- Impact assessment
Visualization
- Graphic display of cyber battlefield
- Graphic display of attack impact
- Graphical interface of configuratior
- Risk visualization
New configuration of battlefield
Graphical interface
Battlefield management
- Configuration change of battlefield (Net topology, services, attack route)
- Ambiguity execution

Figure 1: Conceptual view of cyber battlefield (study finding)

3- The network model generator and service

Each environment including cyber environment consists of some components and elements. The elements of cyber battlefield include tangible and intangible components and their relevant relationship. Tangible components include work stations, servers, users, firewalls, routers, detection systems and intrusion prevention which are collected by network scanners and configuration fields from the network environment. The intangible components are service, cluster of host, protocol, vulnerability and attack scenario. The relationship between the battlefield components as access list is between the components and rules of firewall [6].

Pre-processing and integration of the information are performed by this sub-system and then based on standards, information normalization is performed and finally the information of network topology is controlled by the manager.

4- Vulnerability knowledge Base generator

Vulnerability is any weakness or error in the design or implementation and can lead to an unexpected event and this endangers the security and violates the security policies of system, network, software or protocol and intrusion is occurred based on the abuse of these policies. Thus, it is one of the basic data in modeling and simulation of battlefield. The detected vulnerabilities in computer networks are recorded in some main references. Beside these references, some standards are created for classification and scoring of vulnerabilities and this information is required to perceive the current status of the network. Vulnerability knowledge Base generator performs the creation and updating the vulnerability knowledge base by integration, correlation and classification of vulnerabilities. Each work station in the network consists of some active services. These services can include vulnerability. The identification of the network vulnerabilities is performed by the dynamic engine of battlefield.

An example of implementation of vulnerability model in a five-level hierarchy structure is shown in Figure 2. The first level is the general classification of vulnerabilities in 8 parts. Second level is regarding the classification based on CWE standard. Now, there are 1003 CWE records and each one indicates a group of vulnerabilities with common features. Level 3 indicates the list of affected services. Level 4 is about the different versions of each service and level 5 is about the vulnerabilities of a definite version of a special service. Each vulnerability consists of some features as an attacker access level in case of using vulnerability.

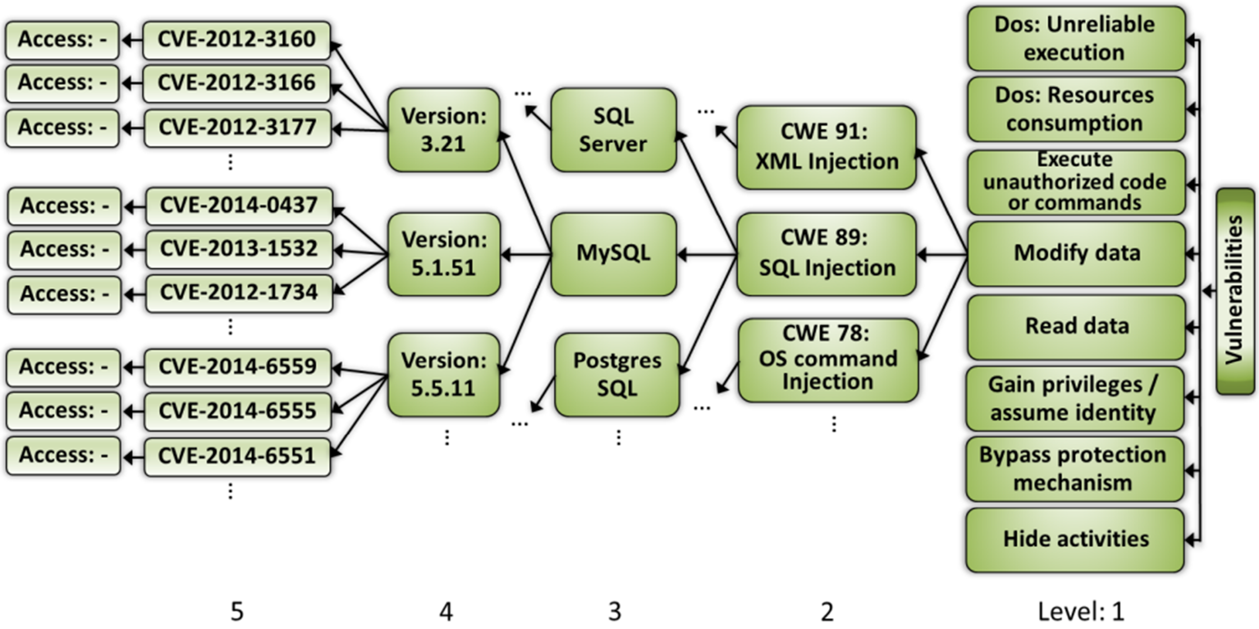


Figure 2: An example of implementation of vulnerability model

5- A dynamic engine of cyber battlefield

This sub-system as the main component of battlefield by receiving information of network model, service model, vulnerability knowledge base and attack scenario of cyber battlefield can perform creation, battlefield dynamic updating, tracking, consistency of attacks and statistical analyses of battlefield and also it acts as information interface of situation awareness for information exchange in a standard format.

6- Impact and risk assessment

The impact assessment defines the attack actions on the battlefield components. To have an accurate impact assessment, we need exact information about the network regulations, executing services, services vulnerability and the importance of each asset. This sub-system performs impact assessment on each of cyber environment components (user, service, host and entire network) by injecting a step of attack into the battlefield. The assessment of total impact of network is computed based on the final damage imposed on the entire component of network.

Risk assessment is used to determine and identify the potential threats and their impact on the assets of battlefield. The output of this process helps the selection of suitable controls to mitigate risk in risk mitigation process. Risk is a function of a threat source based on vulnerability and tis negative impact in the battlefield. Its level is calculated based on the impact on the network mission and the impact on our resources and assets.

7- Visualization

Visualization is used for a graphical display of topology and battlefield components (host, user, service, firewall, physical relationship between the components), real time graphical display of attack tracking, graphical display of the impact of each step of attack on the battlefield components, charts and statistical analyses including the impact assessment and risk assessment, graphical display of components status (active, normal, passive, hacked). Based on the dynamic nature of the battlefield, it is required to update the impact of each change as graphical and real time in the battlefield.

8- Knowledge repository of situation awareness

As it was said, cyber environment consists of tangible and intangible components and their relevant relationship. The information should be integrated, pre-processed, normalized, integrated and finally stored in knowledge repository of situation awareness to use the battlefield and algorithms. Each subsystem generates knowledge in the situation awareness system. These data are converted in a standard form by cyber battlefield generator and are stored in knowledge repository. The subsystems need the generated knowledge in the past and the current situation to perform their mission. By extraction of knowledge form repository, cyber battlefield presents this information to other sub-systems. Thus, battlefield acts as the information interface of situation awareness.

It is possible to store information of different scenes and their combined application. This data warehouse consist of vulnerability models, integrated models of cyber battlefield, service models, network models, attack scenarios, scores of cyber-attack impact and components risk scores.

9- The cyber battlefield algorithms

Cyber battlefield is a platform to perform security analyses. Here, we express the required algorithms of battlefield.

- Sensitivity factor calculation’s algorithm: It is used to determine the sensitivity factor of an element in cyber environment in impact and risk assessment.
- Risk assessment algorithm: It is applied to identify the potential threats and their impact on the environment components.
- Routing algorithm: It is required to rout the packets in the network.
- Logical assessment algorithms of attack: When an attack scenario is injected to the battlefield, the analyst should know whether each step of attack is performed successfully or not? If the attack is not successful, we can assume the attack is not a direct threat for integration or mission of the network but it shows a potential threat in the network.
- Impact assessment of attack algorithm on battlefield components: The impact assessment is used to determine the host of adverse impact of attack on the network components. The effective

factors on determining the impact of each step of attack include active services and its vulnerability, vulnerability sensitivity factor, service, host, user and type of attack step.

- Reference impact scoring algorithm: To have a comparison basis and calculation of damage, we need reference scoring for each impact score. The reference scoring is equal to the highest impact scoring of the component.
- Threshold scoring algorithm: When the impact score is higher than the threshold value, it shows abnormal status in which the manager alert should identify the reason of occurrence of this situation.
- Identification of similar vulnerable systems: in case of occurrence of any attack on the battlefield, at least an intrusion route into the network is identified. Thus, if there is the same vulnerability in other areas of network, the attacker by executing similar scenario can attack the hosts with similar configuration. The identification of these potential threats is performed by this algorithm.

Some analyses are performed before the attack occurrence such as risk assessment, calculation of sensitivity factor, routing and other algorithms during and after attack injection into the battlefield. Some examples are logical assessment of attack, attack impact assessment on the components of battlefield and identification of similar vulnerable systems and these algorithms are performed in the simulator of cyber battlefield.

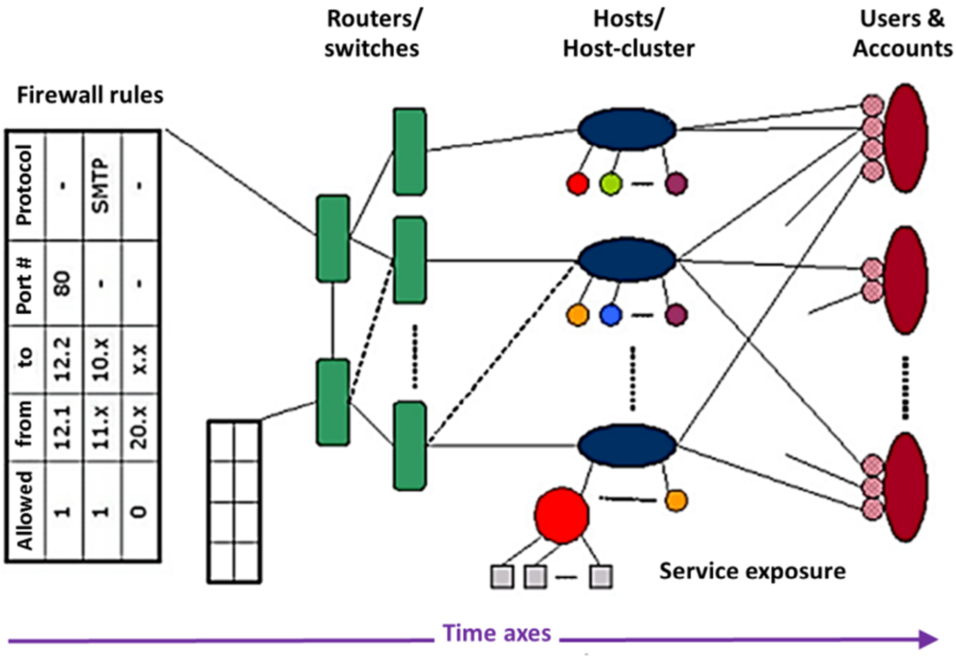
10- The modeling method of cyber battlefield

An object oriented technique is used to model physical, non-physical components, relationship and processes. An example of process in cyber environment is cyber-attack to the victim host. Object oriented method can model the phenomena of real world. Indeed, it shows cyber environment as a set of objects, attributes, behavior, processes, relationship and their data interaction in the real world. Some of the features of object oriented technique are structural, solidarity and re-usability of components in the systems creation. By this technique, we can focus on the behavior and information of the system. Thus, we can create the systems as be flexible against the information and behavioral changes.

11- Modeling cyber battlefield

The model is a simplified abstraction of reality. The environment consists of entity and relations of definition and processing the model situation with the necessary information to find about the past situation of environment and what is occurred in the future. Thus, we can say the most important and complex factor in high level fusion is environment. The methodology of cyber environment modeling is presented as an alternative of physical platform of cyber environment including computer networks. The main inputs of correlated alerts of sensors are the information of environment components (host, service, router, firewall and users) and vulnerabilities information.

The conceptual model of cyber battlefield is shown in Figure 3. In the right side, the users of network are modeled. For each user, there is one or some user accounts. Each user account is connected to a host or host cluster. Each host or host cluster consists of one or some services. Each service includes some service vulnerabilities. The relationship between hosts is established by router or switch. Each of routers consists of access list as shown firewall rules. The rules of firewall indicate the authorized or non-authorized of this relationship.



Allowed	from	to	Port #	Protocol
1	12.1	12.2	80	-
1	11.x	10.x	-	SMTP
0	20.x	x.x	-	-

Figure 3: Conceptual model of cyber battlefield

The cyber battlefield engine by integration of the network model, vulnerability model, service model and attack route in time axes generates cyber battlefield. The cyber battlefield is flexible and generalizable. In case of not having complete knowledge of the entire configuration of the network by the user or want generating the topology configuration as randomly, the battlefield simulator by pre-defined models can propose a sample configuration to the user. Each node as work station has the features of cyber-attack scenarios as IP address, access list, active services, detection intrusion system or/and prevention intrusion system, internet access, status in time axes, current status, operating system, sensitivity factor, etc. In this method, the user determines a set of network services with IP ranges and then simulator generates a suitable model of network for simulation purposes.

12- Model assessment method

For evaluation and verification of modeling and its accuracy, qualitative research method of focus group. Based on the lack of suitable data resources and shortage of review of literature in this field and the high significance of assessment of the relevant results including modeling and battlefield algorithms, in this study, at first for the evaluation of documents, the experiences performed via internet paper bases were used to build a conceptual model and then to respond the questions, a focus group was formed consisting of cyber and network security experts with at least MA degree, experience of 5 years and they were also familiar with cyber security literature. If we need qualitative data detailed regarding the opinion of people about a phenomenon, we can use focus group approach. In other words, the purpose of this method is group interview and achieving opinion of people to the study subject. The researchers who use descriptive-survey method, after collection of quantitative data apply this method to interpret the results of data. This can be done conversely [7]. The questions in focus group are as follows:

Modeling assessment and evaluation of accuracy

- Is the modeling a good model for cyber space with security analysis purpose?
- Is the created model suitable to create the simulator of cyber battlefield?

The assessment of model comprehensiveness

- Are the components of network model, service model, vulnerability model and cyber battlefield model include the required elements of cyber environment and have adequate comprehensiveness?
- Does the model cover the cyber environment components comprehensively for the purposes of this study?
- Are the elements of security analyses (business intelligence, data mining, impact assessment and risk assessment) suitable?

Evaluation of extensibility and minimization of battlefield

- Based on the nature of cyber space, extensibility feature is one of the requirements of this study and extensibility and minimization of battlefield are considered. Are extensibility and minimization (addition and elimination of components from the environment and making changes on the features of components) designed and modeled accurately?
- Are revisions of access permission between hosts, access rules on firewall, revision of services of each host and revision of the hosts of battlefield designed and modeled accurately?

13- The comparison of cyber battlefield with the similar models

In the network security field, the conducted relevant researches are attack graph and vulnerable tree models. The common challenge of all models is incomplete information feeding in the model and this leads to false analysis. In this comparison, it is assumed the information in models is fed accurately. In the majority of implementations, each graph can model only one target but some of them as [8] can model some targets in a graph. In the graph, the nodes show the steps of an attack but the arcs show the possible transition between the steps. One of the reasons of failure of attack graphs is assuming a static relationship between the nodes. As different traffics can between two authorized or unauthorized hosts, based on the firewalls and routers, such assumption is not true. In cyber battlefield, firewall rules and list of accesses are considered and there is required information for detection of authorization of traffic. As a vulnerability tree is used to achieve a unified target, for some targets, some vulnerability trees are defined. This method makes the definition of vulnerability tree for a huge network difficult as we need to define many great and complex vulnerability trees but cyber battlefield implicitly can model all defined attacks and targets in a unified model [9][10][11][12][13].

14- Conclusion

One of the most important components of cyber command and control is cyber situation awareness. A comprehensive understanding of systems and their relevant threats to guaranty the security and integrity of operation is a necessity including evaluation of adverse effect of attacks on cyber environment components. The presented framework consists of an integrated model of cyber battlefield, situation awareness knowledge base, risk assessment; attacks impact assessment, vulnerability knowledge Base generator, attack simulator and cyber information fusion engine. To achieve cyber situation awareness, we need an accurate inspection and execution of cyber maneuvers. The present study presents a framework of cyber situation awareness for accurate inspection of the current situation of cyber battlefield and cyber maneuvers. The battlefield engine creates the knowledge repository of situation awareness and provides the required information for security analyses including the complete features of recognized vulnerabilities in cyber space, attacks scenario, service model, network model and cyber battlefield model. Dynamic updating, tracking, consistency of attacks, statistical analyses and situation awareness interface are other duties of battlefield engine. Focus groups as a qualitative research method are selected to evaluate the modeling. To evaluate assessment and performance of the presented model, a research contract is concluded with the Iran fuel smart card system. The implementation of model and algorithms is associated to cyber battlefield simulator.

Acknowledgement

My gratitude goes to Dr. Rashidi for his effective supports and guidance and also I am grateful of Oil Company for collaboration in implementation and evaluation of plan in the Iran fuel smart card system.

References

[1] "United States Air Force Cyber Vision 2025," United States Air Force, Washington, 2012.

[2] Rashidi, AliJabar; Shakibzad, Mohammad. Dynamic modelling of cyber battlefield. The 4th conference of computer engineering and processing of signal. Tehran. 2016.

[3] MR Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995.

[4] Shakibzad, Mohammad; Rashidi, AliJabar. A framework to achieve dynamic cyber battlefield simulation. The 4th International conference on electrical and computer engineering. Tehran. 2017.

[5] D.L. Hall and J. Llinas, "An Introduction to Multi-Sensor Data Fusion," *IEEE*, pp. 537-540, 1998.

[6] Rashidi, AliJabar; Shakibazad, Mohammad. Cyber battlefield: Simulation of computer network for security assessment. Malek Ashtar Univeristy. Tehran. 2014.

[7] Bazargan, Abbas. An introduction to qualitative and mix research methods. Conventional approaches in behavorial science. Terhan. Nashr Didar. 2008.

[8] Peng Ning and Dingbang Xu, "Learning attack strategies from intrusion alerts," in *ACM, Proceedings of the 10th ACM conference on Computer and communications security*, 2003.

[9] C. Phillips and L. P. Swiler, "A graph-based system for network vulnerability analysis system," in *In Proceedings of the 1998 workshop for new security paradigms*, New York, 1998.

[10] S. Jajodia, S. Noel, and B. O'Berry, "Topological analysis of network attack vulnerability," in *Managing Cyber Threats: Issues, Approaches, and Challenges*, 2003.

[11] R. Lippman and K. Ingols, "An annotated review of past papers on attack graphs," Lexington, 2005.

[12] S Vidalis and A Jones, "Using vulnerability trees for decision making in threat assessment," in *ECIW Proceedings of the 2nd European Conference on Information Warfare and Security*, UK, 2003, p. 329.

[13] Bruce Schneier, "Attack trees," *Dr. Dobb's journal*, vol. 24, no. 12, pp. 21--29, 1999.