Iranian Journal of Information Technology & Communication

No.33-34, Vol.9, Fall & Winter 2018
PP: 1-8

Iranian Society of Information Communication Technology

Cyber Threats Foresight Against Iran Based on Attack Vector

[*] Mahdi Omrani [**] Masoud Shafiee [***] Siavash Khorsandi

[*] Department of Management, Science and Technology Amir Kabir University of Technology, Tehran, Iran

[**]Faculty of Electrical Engineering Amir Kabir University of Technology, Tehran, Iran

[***]Associate Professor Faculty of Computer Engineering Amir Kabir University of Technology, Tehran, Iran

Abstract

Cyber threats have been extraordinary increased in recent years. Cyber attackers, including government agencies or hackers, have made significant advances in the use of various tools for attacking target systems in some countries particularly on Islamic republic of Iran. The complexity of cyber threats and the devastating effects of them on critical systems highlights necessity of cyber threats Foresight. This research can prepare the country for countering cyber threats based on existing and potential attack Vectors. First of all, 18 major cyber threats drivers base on attack Vectors through reviewing resources and interviewing with seven experts were identified. We use cross-impact analysis Future studies method to indicate main drivers of future cyber threats such as social engineering, Denial of service, ransomwares, spoofing and fraud and non-state actors. Mic Mac software will be used for this step. Finally, future scenarios for cyber threats were identified by using scenario-based approach. Scenario Wizard software will be used. The results of the research include two strong scenarios and 18 possible scenarios, based on the strongest scenario, ransomware, spoofing, fraud, social engineering and Denial of service are the most likely cyber threats by non-state actors through in a limited level.

Keywords: Foresight, cyber threats; attack Vector; cross-impact analysis;senario

I. Introduction

Today, cyber threats are one of the most serious and ambiguous concerns of many countries in cyberspace. Due to the difference in cyber threats from the perspective of nature, content, multiplicity of actors with traditional and conventional threats, they can no longer be confronted with past strategies and actions. Some threat such as Stuxnet, Doku, Viber, Vana cray against the country highlights the need for cyber threat forecasting and preparedness to deal with these threats.

The emergence of new trends and paradigms of information and communication technology such as service oriented, networking, cloud computing, Internet of things, the fourth industrial revolution had been had Deep effects on the perspectives, orientations, policies, strategies in some organizations and government [1].

The foresight approach used extensively in the formulation of macro documents at the national and international levels is based on a participatory and microfinance approach that encompasses the widespread participation of experts and influential institutions in each field of expertise in developing of strategic documents, prospects, policy making, and the possibility of creating an agreement and consensus among them.

If the trends and key factors of cyber threats and their impact on each other are identified, then we can create future cyber security scenarios and manage the organization's cyber security challenges. Therefore, it is essential that serious measures be taken at the strategic, operational, and technical levels of the various dimensions of cyber threats through future research in our country.

The organization of research is as follows: In the second part, the most important researches on the classification of cyber threats is reviewed. In the third section, the main research approach is expressed. Research methodology and analysis of the results are described in sections 4 and 5. In the sixth section, conclusions and future works will be presented.

II. Related works

There are several ways to categorize cyber threats. The main characteristics for a proper cyber threats classification are acceptability, non-overlapping, comprehensible, complete, comprehensive, clear and repeatable [3].There are some of the most famous cyber threat categories:

Kjaerland, categorized cyber intrusions in 2005 based on four categories; method of operations, impact of the intrusion, source of the intrusion and target. This study examined the likelihood of attacks against different kinds of targets and the likelihood of various kinds of attacks occurring together on a given target. The classification emphasizes the aggressor's motive for the attack and tries to quantitatively analyze the cause of the attack and the location of the attack. The weakness of this classification is that it does not provide enough details regarding the Vectors of identifying the start of the attack and only provides a high-level view of the types of attack Vectors [4].

Hansman and Hunt created a unique taxonomy in 2004 which was designed to be used by information bodies to classify new attacks. This taxonomy was based on four dimensions of attack tools, the target of the attack, the type of vulnerability and the impact of the attack. The various levels of information inside each one are available to defenders for details of the attack. The weakness of the classification is the lack of sufficient information about vulnerabilities, which results in the lack of information needed to protect the system against attacks [5].

Mirkovic and Reihner created a comprehensive taxonomy of Distributed Denial of Service Defenses which categorized DDoS, defense mechanisms based on activity level, degree of cooperation and deployment location, source address, the dynamics of the attack rate, the type of victim, and the level of impact. The weakness of classification is that it only emphasizes an attack type [6].

Lough suggested an attack-driven classification called VERDICT that focuses on four main reasons for security errors, such as incorrect validation, inaccurate disclosure, improper randomization, and inappropriate publishing. The weakness of the classification is that it does not take into account the types

of attacks, such as Worms, Viruses and Trojans [3].

Howard delivered a classification of attacks based on events in five dimensions of tools, vulnerabilities, operations, goals, and outcomes. This classification, although providing useful information, lacks details for accurate analysis of attacks [7].

Simmons et al, (2009) suggested a cyber threat taxonomy which called AVOIDIT base on five dimension of Attack Vector, Operational Impact, Defense, Information Impact and Target to help identify and defend against cybercrime attacks. The classification is intended to address shortcomings and deficiencies in previous practices and provides useful information for managing cyber threats. The lack of coverage of physical attack Vectors and new attacks is one of the weaknesses in this classification [8].

One of the most important dimensions of cyber threats in the mentioned categories is Attack Vector, the main approach of the present research is to identify the most popular Vectors of attack and mapping out the future cyber threats based on them.

III. The research main approach

One of the key components of cyber threats is determining of attack vectors. An attack Vector is defined as an attack path through which an attacker can access a system. Starting a successful attack may require several vulnerabilities. Therefore, in order to accurately investigate the Vectors of attack identifying vulnerabilities in the system is essential.

A lot of researches has been done on cybercrime vulnerabilities and there are various databases in this field. CVE (Common Vulnerabilities and Exposure) and NVD (National Vulnerability Database) are two examples of vulnerability-related database. The CVE database, although fully covered by more than 98,000 vulnerabilities, is difficult to use, because it does not provide a specific classification for vulnerabilities [9]. The NVD's database reduces vulnerabilities by using the Common Vulnerability Score System (CVSS), but it is difficult to exploit the vulnerability due to excessive access to vulnerabilities. The attack Vector is one of the key components for quantifying vulnerabilities in this database [10].

The main approach of the present research is to predict the future of cyber threats based on attack Vectors. 11 attack Vectors mentioned in the latest version of the AVOIDIT classification were considered as the basis for research [11]. In addition, more than 20 other attack Vectors were added by reviewing several security sources, such as McAfee's most recent 2017 cyber threat reports and EU Cyber threat reports [12], [13], [14].

IV. Research Methodology

Foresight has more than 39 research Vectors, which is generally done by combining different Vectors. Research has been done by combining Foresight methods such as resource reviews, expert panel, cross-impact analysis, scenario analysis. According to the characteristics of the statistical society (cybersecurity and foresight experts), the research has been done through targeted sampling. The realm of research is ten years from now.

The cross-impact analysis method, as one of the prominent scenario planning Vectors, was first developed by Theodore Gordon and Helmer in 1996. It is a visualization of the interactions between trends and variables, and is based on the question "Can future

predictions be based on the possible effects of future events on each other?" [15].

The steps to do cross-impact analysis are as follows:

A. In the first step, a total of 31 major attack Vectors were identified and provided to seventeen cyber security and Foresight experts. By conducting multiple expert panels, the attack Vectors were examined. Eventually, by elimination less important and the classification of similar attack Vectors, 18 Vectors of attack were identified as cyber threats drivers. They described in Table 1.

B. In the second step, an 18*18 matrix was designed to show the number of cyber threats, and the experts were asked to determine the relationship of 18 major drivers with respect to the range (0 to 3), so that the zero number, Without impact, number of one low impact, number of two intermediate effects and number of three effects of propulsion on each other.

C. In the third step, the main drivers of cyber threats were identified based on the cross-impact analysis Vector and the results of the experts' supplementary questionnaires were analyzed using the Mic Mac software.

Table1: Most Important Attack Vectors

Row	Attack Vector	Symbol
1	Misconfiguration	MC
2	Kernel Flaws	KL
3	Design Flaws	DF
4	Buffer Overflow	BO
5	Insufficient Input Validation	IV
6	Insufficient Authentication Validation	AV
7	Symbolic Link	SC
8	File Descriptor Attack	FD
9	Race Condition	RC
10	Social Engineering	SE
11	Ransomwares	RM
12	Denial Of Service	DS
13	Installed Malware	IM
14	Rootkit & Botnet	RB
15	Known Vulnerability	KV
16	Spoofing	SP
17	Organized Actors	OA
18	Non-Organized Actors	NA

V. Analysis of research findings

Mic Mac software, determines the extent of the influence and impact of their variables and their space by identifying low-impact and removable variables, objective and effective variables, and identifies the most important variables as main drivers [15]. The results of the complete of experts in the Mic Mac software supplementary questionnaire are as follows:

The degree of maturity filling is 94.44%, which indicates that the factors selected affect more than 94% of the cases. Generally, 324 relationships that can be evaluated, the number of eighteen relationships is zero; these factors do not affect each other and do not affect each other. The matrix is based on statistical indicators with two data rotations of desirability and optimization of 100%, which shows the high validity of the questionnaire.

In Table 2, the sum of the numbers of the rows of each variables, as the effect of the numbers and the sum of the columns of each variable, shows the effect of the other variables in two stages of repetition.

Table 2: cross impact matrix main keys

	1 : MC	2 : KL	3 : DF	4 : BO	5 : IV	6 : AV	7 : SC	8 : FD	9 : RC	10 : SE	11 : RM	12 : DS	13 : IM	14 : RB	15 : KV	16 : SP	17 : OA	18 : NA
1 : MC	706	1003	804	828	1002	938	867	778	734	1066	999	977	935	883	959	916	965	878
2 : KL	815	1161	913	949	1131	1083	987	893	841	1212	1150	1094	1081	1006	1113	1045	1119	1015
3 : DF	772	1073	859	900	1077	1030	923	842	788	1159	1070	1040	1003	956	1048	985	1047	952
4 : BO	823	1175	933	960	1153	1107	998	905	869	1228	1166	1129	1092	1015	1131	1055	1138	1036
5 : IV	760	1070	864	880	1069	1018	920	835	795	1137	1064	1047	996	944	1040	978	1037	953
6 : AV	807	1136	905	953	1135	1079	980	884	836	1219	1140	1102	1061	1001	1104	1034	1110	995
7 : SC	692	965	778	798	969	911	840	747	713	1035	960	938	899	854	938	889	933	856
8 : FD	710	1001	803	821	1000	926	874	778	735	1054	1003	970	940	881	962	923	966	885
9 : RC	625	893	713	734	881	840	764	687	655	943	892	860	828	776	859	804	863	777
10 : SE	1229	1768	1413	1423	1725	1654	1492	1363	1299	1827	1751	1703	1643	1523	1690	1593	1693	1555
11 : RM	1207	1693	1346	1400	1688	1584	1460	1307	1236	1805	1666	1635	1581	1495	1635	1556	1634	1498
12 : DS	1195	1666	1330	1397	1671	1598	1425	1293	1224	1796	1654	1615	1558	1477	1628	1532	1624	1472
13 : IM	714	1000	798	831	1003	932	876	770	733	1070	998	964	933	881	966	917	967	881
14 : RB	936	1317	1059	1082	1302	1237	1143	1022	971	1397	1331	1256	1218	1144	1275	1181	1279	1161
15 : KV	831	1188	942	985	1179	1111	1024	906	864	1263	1181	1131	1100	1042	1135	1068	1149	1029
16 : SP	1022	1433	1148	1197	1449	1356	1253	1112	1055	1549	1425	1389	1331	1277	1380	1308	1393	1266
17 : OA	756	1072	855	883	1063	996	928	831	785	1137	1068	1041	1001	940	1031	978	1037	937
18 : NA	1193	1685	1353	1395	1691	1568	1478	1306	1233	1789	1697	1634	1582	1495	1620	1558	1626	1472

A. The axis of influence and the impact of variables

The most important outputs of the Mic Mac software are the presentation of the variables in the form of the axis of influence and the impact of variables, as shown in Figure 1.

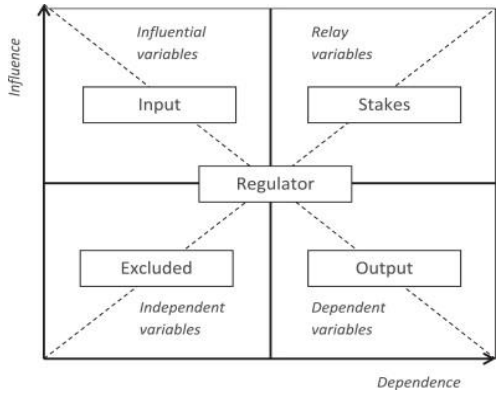

Figure1: Axis of Influence and Impact

In the above axis, the system variables in five domains are most influential, two-way variables (Risk and purpose); influenced (dependent); independent and regulated.

The most influential variables: they have most influential and least impact and are located in the northwest.

Two-way variables (risk and purpose): they act simultaneously as influential and impact, and are located in the northeast.

Effective variables (result): they have a very low impact and a very high influential and are located in the southeast.

Independent variables: they have a low impact and are located in the southwestern part.

Regulator variables: they have the ability to become other variables and are located in the center of gravity.

When the influence and impact of a variable is high, it will be placed in the risk area and the target variables; therefore, it can be considered as a key factor in success.

One of the most important outputs of Mic Mac software is direct and indirect effects of variables. Table 3 shows the direct and indirect effects base on their priority.

B. Analyzing the direct effects of variables

Figure 2 illustrates the dispersion map of variables and their position in the axis of influence and the impact of variables, directly. The Variable of non-governmental actors is there in the area of effective variables. Variables like social engineering, denial of services, ransomware, spoofing and fraud are there in the area of double-headed variable. The variables like known vulnerability, Insufficient Input Validation, Kernel Flaws, Insufficient Authentication Validation, and Installed Malware are there in the affected area. The Variables like buffer overflow, design error, file descriptor, incorrect configuration, competition status, and symbolic links in the region of independent and variables like rootkit and botnet are in the area Regulated.

Table 3: Direct and Indirect Effects

Rank	Label	Direct influence	Direct dependence	Indirect influence	Indirect dependence
1	SE	783	659	784	655
2	DS	762	618	759	617
3	RM	742	618	757	615
4	NA	742	618	751	614
5	SP	639	597	646	597
6	RB	577	597	590	595
7	BO	536	597	529	595
8	KV	536	577	523	580
9	KL	515	577	515	575
10	AV	515	556	511	562
11	DF	494	536	485	543
12	IV	494	536	481	542
13	OA	474	536	480	532
14	MC	453	515	449	509
15	FD	453	494	449	493
16	IM	453	474	449	477
17	SC	432	453	435	453
18	RC	391	432	398	437

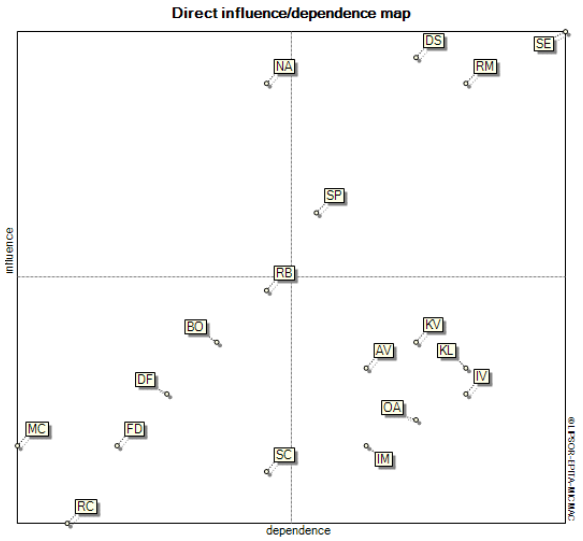

Figure 2: Direct influence/dependence map

Figure 3 shows the graph of the direct relationships of the variables.

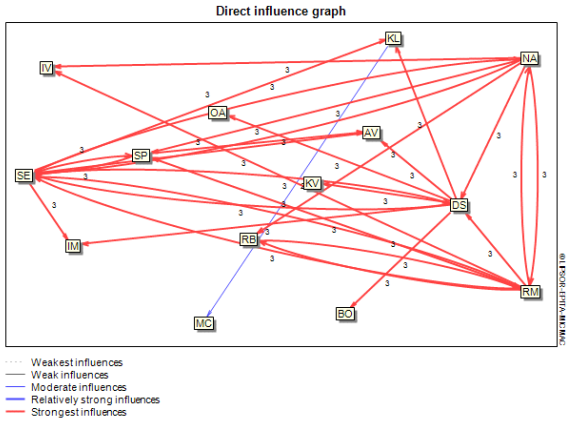

Figure3: Direct influence graph

C. Analyzing indirect effects of variables

Mic Mac software can calculate the indirect effects of variables on each other through potentials 2, 3, or 4. Figure 4 illustrates the dispersion map of variables and their position in the axis of influence and the impact of variables, indirectly.

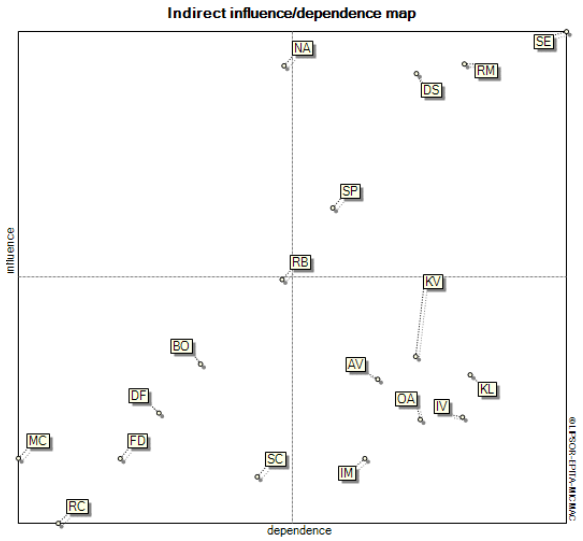

Figure 4: Indirect influence/dependence map

Figure 5 shows the graph of indirect relationships between variables.

Comparing two direct and indirect Vectors indicates a lack of change in the prioritization of key predictors. The final output of the Mic Mac software outlines five main drivers of cyber threats based on attack Vectors. It will form the basis for future scenarios for cyber threats.

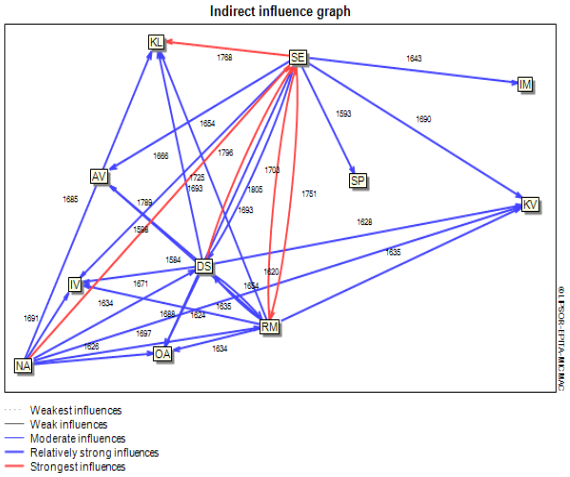

Figure5: Indirect influence graph

D.Compilation of cyber threat scenarios

After identifying the five main drivers,with the consideration of the experts, 15 possible situations were described in Table 4.

Table 4: Statues of Main Drivers

Driver	Tag	Status	Effect
Social Engineering	SE	SE1	Very low
		SE2	intermediate
		SE3	Very high
Denial of service	DS	DS1	Very low
		DS2	intermediate
		DS3	Very high
Ransomware	RM	RM1	Very low
		RM2	intermediate
		RM3	Very high
Spoofing and Fraud	SP	SP1	Very low
		SP2	intermediate
		SP3	Very high
Non-state actors	NO	NO1	Very low
		NO2	intermediate
		NO3	Very high

These conditions are favorable to the undesirable conditions. By designing a 15*15 matrix, a detailed workbook questionnaire was provided to experts, and they answered by the question, "If any of the 15 situations does, what effect does it have on the occurrence or non-occurrence of other situations have?" The magnitude of the impact of each situation, with a score of between -3 and 3, was determined. Data collection is entered in the Scenario wizard software. The scenario wizard software provides complex and very heavy computing, the ability to extract scenarios with high probability, scenarios with a low probability, and scenarios with the possibility of compatibility and high compliance [16].

The results of using the Scenario wizard software are as follows:

•Strong or probable scenarios: two scenarios

•Highly Compatible Scenarios: 18 scenarios

•Poor scenarios: 0 scenarios

Table 5 shows the status of two strong scenarios for future cyber threats.

Table 5: Strongest Scenarios

Driver	First senario	Second senario
social engineering	SE1	SE2
Denial of service	DS3	DS2
Ransomware	RM3	RM3
Spoofing and Fraud	SP3	SP3
Non-state actors	NO2	NO2

VI.**Conclusion**

In the present era, the threats facing many countries have been challenged. Therefore, it is necessary to conduct future studies researches to predict and prepare the organizations of the country with regard to major trends and threats.

In the present research, at first the most important cyber threats in the form of 18 attack Vectors were identified by reviewing the cyber threat categories and analysis of cybersecurity trends. Then, using the Expert Panel and the Mic Mac Analysis Tools, from among the identified Vectors of attack, five Vectors of social engineering attack, denial of

service, ransomware, spoofing and fraud and non-state actors as The main cyber threats drivers were identified.

Finally, future scenarios for cyber threats based on major drivers were identified using the scenario wizard software. Based on the strongest scenario, the country's most cyber threats will occur by non-state actors, with large-scale ransomware, spoofing and fraud attacks and social engineering attacks and denial of service in limited level.

REFRENCES

[1] B.Dupont, "The Cyber Security Environment to2022:Trends, Drivers and Implications" ssrn Electron.j. jan.2012.

[2] Raford, Noah, Online foresight platforms:Evidence for their impact on scenario planning & strategic foresight, Technological Foresight & Social Change, In press, Available online, 2014.

[3] Lough, Daniel. "A Taxonomy of Computer Attacks with Applications to Wireless Networks," PhD thesis, Virginia Polytechnic Institute and State University, 2001.

[4] Kjaerland, M., "A taxonomy and comparison of computer Security incidents from the commercial and government sectors".Computers and Security, 25:522–538, October 2005.

[5] Hansman, S., Hunt R., "A taxonomy of network and computer attacks". Computer attacks".Computer and Security (2005).

[6] Mirkovic, J., and Reiher, P. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. In ACM CCR ,April 2004.

[7] Howard, John D. and Longstaff, Taxonomy A. "A Common Language for Computer Security Incidents," Technical report, Sandia National Laboratories, 1998.

[8] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, AVOIDIT: A Cyber Attack Taxonomy, This work is supported by the Office of Naval Research ,2014.

[9] https://cve.mitre.org

[10] https://nvd.nist.gov

[11] R. Koch1, M. Golling1 , G. Rodosek, A Revised Attack Taxonomy for a New Generation of Smart Attacks,2014.

[12] Rp-Mcaffee-Quarterly-Threats-Mar-2017

[13] ENISA Threat Landscape Report 2017 15 Top Cyber-Threats and Trends. 2018

[14] Reference Incident Classification Taxonomy ,Task Force Status and Way Forward , 2018

[15] Asan, seyda serdar, Umut asan, Qualitative cross-impact analysis with time consideration, Technological forecasting and social change, vol74, 2007.

[16] Godet, Michel, Creating Futures: Scenario Planning as a Strategic Management Tool, France, Economica publish,2006.

[17]

The development of scenarios based on other Foresight methods such as game theory and other dimensions of the classification of threats such as the sources and objectives of threats, the type of actors