IMPROVING DISTRIBUTED VULNERABILITY ASSESSMENT MODEL OF CYBERSECURITY

Kálmán Hadarics[1] and Ferenc Leitold[2]

DOI: 10.24989/ocg.v331.32

Abstract
In the digital age more and more services and data are available over the Internet. Companies and public organizations becoming increasingly vulnerable related to hacks and cyberattacks. In order to provide successful online services, effective security initiatives and targeted protections are necessary to mitigate security risks. Effective cybersecurity more than deploying firewalls and other security software (e.g. antivirus, intrusion detection/prevention systems.). Through risk assessment and risk management practices we can identify critical parts of information systems and can transform them into security tactics. Furthermore in the Distributed Vulnerability Assessment (DVA) model three factors are identified: (1) characteristics and prevalence of cyber-threats, (2) vulnerabilities of IT infrastructure and its components and processes, (3) vulnerabilities deriving from users' behavior.

In this paper, we examine and improve our mathematical model of Distributed Vulnerability Assessment. This model can be extended for using additional information and considerations. This paper also presents a practical method which can be applied to eGovernment infrastructure and services also to reduce the impact of malware attacks of the information system.

Keywords: *distributed vulnerability analysis, malware, threat, cybersecurity*

1. Introduction

The recent evolution of information technology caused significant increase in productivity and everyday life. These days using online services is self-evident. Our personal and other specific data are accessible from different devices like computers, tablets, smartphones and other IoT devices. However if our data are available online they are exposed to theft or unwanted manipulation. There are different cyber-threats. With the help of that cyber criminals can steal unauthorized data or other credential information. In the digital age the information security became a crucial point of an information system. If you want to launch a new digital service you have to ensure data security. An unwanted security incident can disrupt our business success, and partners will abandon our service.

If we want to observe the protection level of our IT system and infrastructure we have to consider our data flows and processes. But all systems, networks, applications or other infrastructure element may contain vulnerabilities or just misconfiguration. Newer and newer threats are appearing everyday therefore continuous review of security rules are expected. In order to achieve digital enterprise success, effective security initiatives and targeted protections are necessary to reduce or mitigate security risks.

[1] University of Dunaújváros, H-2400 Dunaújváros, Táncsics M. u. 1/A., hadarics@uniduna.hu
[2] Secudit Ltd., H-8200 Veszprém, Kupa utca 16., fleitold@secudit.com

As a result of our research we have define DVA (Distributed Vulnerability Assessment) model [1].

In this model three distinct but highly interactive sources of vulnerability are considered [2]:

(1) Characteristic and prevalence of harmful cyber-threats

(2) Vulnerabilities of the IT infrastructure and its processes;

(3) Vulnerabilities deriving from users' behavior.

More detailed information about the model is available in [1] and [2].

2. Background and related work

More and more organizations around the world perceived the need of risk assessment in order to enhance information security. Standard organizations e.g. NIST or ISO have published their risk management guides [3],[4]. These are attempts to create a common language and guidance for assessing and mitigating risks related to information security incidents. An information security incident can be a single or a sequence of unexpected or unwanted information security event. New vulnerabilities are discovered on average daily in different software and hardware devices. It makes possible launching new attacks or other types of exploitation.

An infrastructure is as secure as the weakest component in the system. "To succeed, a malware attack directed against a protected target network requires successful execution of the malicious code by the protected IT with sufficient authorized user facilitation to subvert network security." [5] Security metrics generally focus on malicious activity and protected IT. Metrics related to user behavior are less common. The DVA model focus on all of three main factor discussed earlier. Using different mathematical formulas and techniques the risk value for a threat can be estimated.

3. Limits of DVA model

A quantitative risk assessment model provides appropriate results if its input parameters are derived from some irrefutable facts. Certain factors have more impact on overall result. But adding new factors to the model can help to refining and clarifying the issue.

The DVA model has some limitations:

- The probabilities that are used in formulas need to be independent. Otherwise the estimation won't be accurate.
- Detailed unfolding of properties of model elements are necessary for reaching the expected accuracy.
- The model doesn't identify the direct connections between elements.

4. Alternative approach

The starting triangle is very similar to DVA model elements. In the first corner there are the Users. Users are humans, they can do something on computers (devices), and they have activities on IT infrastructure. The second main corner are the devices. They are just physical devices, they have hardware components and they are able to execute programs. The third main corner are the threats [6]. There could be a plenty of possible threat types [7] related to an attacker or any unwanted event that can be occurred.

The three main corners represent the corners of our triunal model, they are the main actors in any security issue.

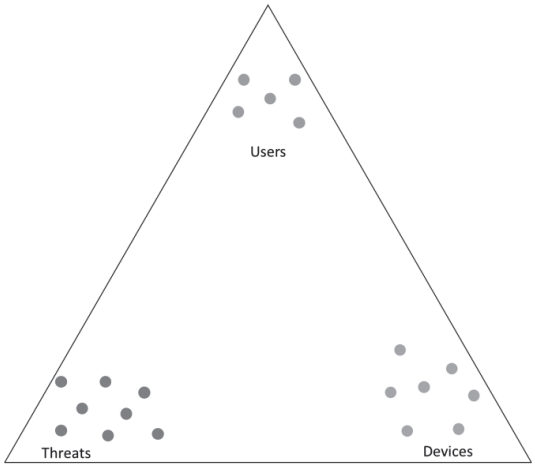

Figure 1: Main actors of the cybersecurity vulnerability assessment

A set of points inside the triangle contains the actors that have impact on information security and they belong together based on some attribute.

Beyond the main actors we can define other influential set of points. These are

- User tricks
- Credentials/access rights
- HW/SW elements
- Cloud services
- Vulnerabilities
- Protections.

In the model we can define connections between set of points. These connections generally link together points from different sets. Later we will define the exact meaning of a connection that is exists between different set of points. It can be said generally if there is connection in the pattern that belongs to a specific threat it carries a security hazard.

We have hardware and software elements as well. Of course two devices have different HW/SW elements, they can be similar. So this set of light green points represent different instances of HW/SW components. E.g. Windows 7 on device 1, Internet Explorer on device 2, Google Chrome on device 1, Microsoft Word on device 2. A line between a device and a HW/SW element indicates that the particular device has that component.

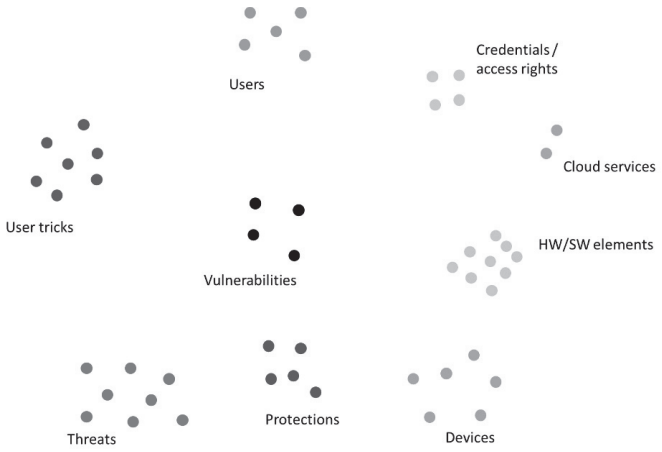

Figure 2: The influential actors of the cybersecurity vulnerability assessment

The next set of defined points are very similar to the HW/SW elements. They are cloud services. The cloud services can be assigned to the devices as well, if we define the connection between a device and a cloud service if the device is able to use the cloud service. E.g. if the Dropbox is installed or if there is an internet browser and the device has internet connection (in this case most of cloud services can work).

Users are the humans that use computers (devices). In fact they can access to one or more HW/SW components only. Now we assume that they do not make any physical changes in the machine. So they need credentials/access rights to HW/SW components and they may have credentials/access rights to one or more cloud services. So, a line between a user and a credential/access right indicate that the particular user has that credential/access right. And there could be a line between a credential/access right and a HW/SW element or a cloud service indicating which component can be accessed. Please note, that if a user has an administrator right to a computer then this user has credential/access right to all of its HW/SW components. But it can be limited by settings and/or policies. Users have their own behavior as they are humans. [8] There are user tricks that can be used by threats. The line between a user and a user trick indicates that there is a possibility that using the particular user trick the user will make what the threat requests/expects. The line between a threat and a user trick indicates that there is a possibility that the threat uses the particular user trick.

Each point in the protection group represents a SET of protections can protect a SET of HW/SW elements or cloud services. E.g. a firewall and an antivirus together.

A line between a threat and a protection indicates that there is a possibility that the protection does NOT block the particular threat.
A line between the protection and a HW/SW element or a point of cloud service indicates that the protection is installed to protect that HW/SW element or the cloud service.

There are vulnerabilities in the HW/SW elements and they can be in cloud services as well. Vulnerabilities are used by threats.

The line between a threat and a vulnerability means that the particular threat uses that vulnerability. The line between a vulnerability and a HW/SW element or a cloud service means that there is a possibility that the usage of the particular vulnerability against the HW/SW element or the cloud service is successful.

The line between a vulnerability and a credential/access right means that there is a possibility that the usage of the particular vulnerability against the credential/access right is successful. For example if the malicious activity tries to figure out the user name and the password.

In this model we represent a factor as a point of a set. With the help of defined connection we are able to find the concerning elements. We defined this representation the constellation model of vulnerability assessment.

5. Practical usage

The threat type is exploit. Exploits use vulnerabilities of HW/SW elements to execute their code on the device.

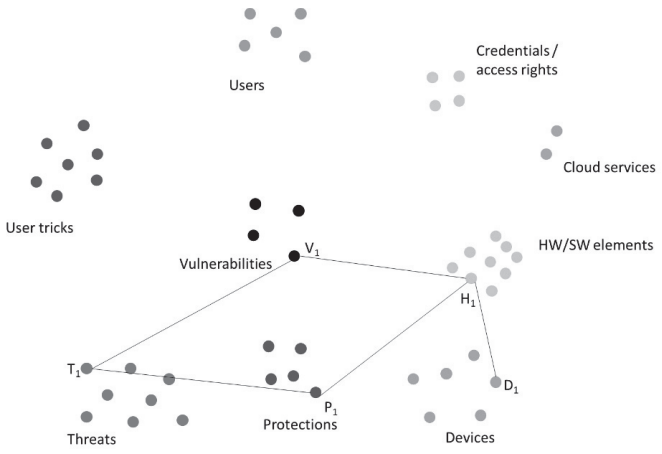

Figure 3: Representation of "Exploit" type threat

Successful operation requires the followings:

- Threat T_1 has to use vulnerability V_1.
- Vulnerability V_1 has to be related to HW/SW element H_1.
- For protecting operation of H_1, the P_1 set of protections (it can be empty set) exists and it is unable to block all of Threat T_1 executions against the HW/SW element H_1.
- And finally there should be the device D_1 which has the HW/SW element H_1.

Please note that all of the five lines indicates a probability or a relative frequency related to the operation.

T – V: How often use Threat T_1 the Vulnerability V_1.

V – H: How often successful the Vulnerability V_1 against HW/SW element H_1.

T – P: The blocking rate of threat T_1 by the protection (set) P_1.

P – H: The availability of Protection P_1.

H – D: How often the HW/SW element is working on device D_1.

In the next example the threat type is eavesdropping. During this an attacker attempts to obtain authentication information for a cloud service.

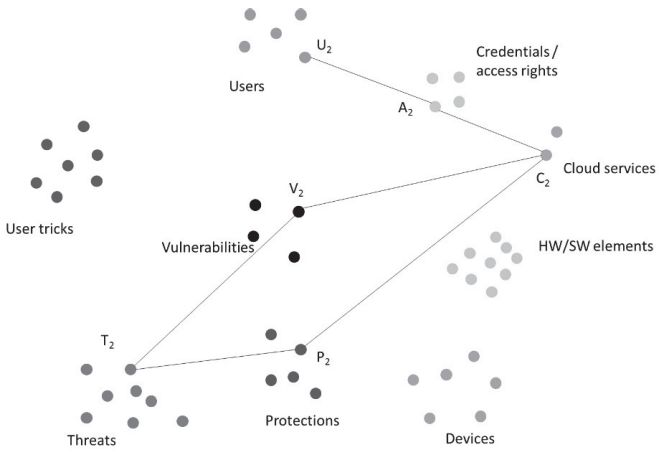

Figure 4: Representation of an Eavesdropping

Successful operation requires the followings:

- Threat T_2 has to use vulnerability V_2.
- Vulnerability V_2 has to be related to cloud service C_2.
- For protecting operation of C_2, the P_2 set of protections (it can be empty set) exists and it is unable to block all of Threat T_2 executions against the cloud service C_2.
- And finally there should be a user U_2 who has an access A_2 for cloud service C_2.

All of the six lines indicates a probability or a relative frequency related to the operation.

T – V: How often use Threat T_2 the Vulnerability V_2.

V – C: How often successful the Vulnerability V_2 against cloud service C_2.

T – P: The blocking rate of threat T_2 by the protection (set) P_2.

P – C: The availability of Protection P_2.

U – A: How often the User U_2 is using cloud service C_2.

A – C: How often the access rights A_2 are in use accessing cloud service C_2.

In the third example there is an e-mail client (H_3) which has a vulnerability (V_3). H_4 is the operating system which executes the attachment when the User (U_3) clicks. D3 is the device that executes H_3 and H_4. C_3 denotes the user's credentials to the e-mail client, C_4 to the used operating system. The applied User trick (scam) is represented by S_3. P_3 is the set of e-mail protections, P_4 is the set of endpoint protections.

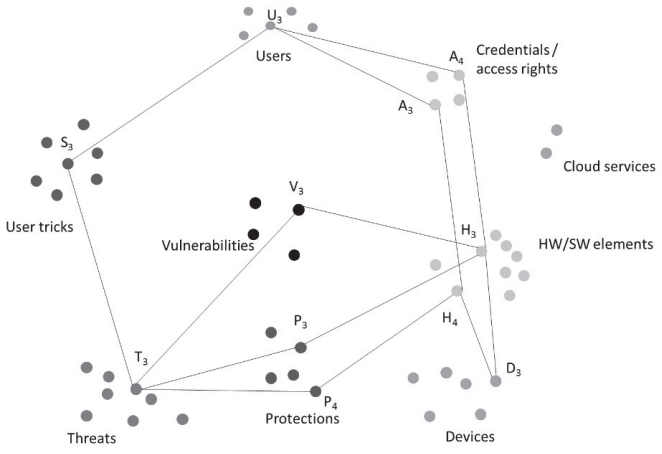

Figure 5: Representation of an e-mail related threat

All of the fourteen lines indicates a probability or a relative frequency related to the operation.

T – V: How often use Threat T_3 the Vulnerability V_3.

T – P: The blocking rate of threat T_2 by the protection (set) P_3 and P_4.

T – S: How often use Threat T_3 the User trick S_3.

S – U: How often user U_3 can be deceived by user trick S_3.

U – A: How often the User U_3 use the access to A_3 and A_4.

A – H: How often the access rights A_3 and A_4 are used to access HW/SW elements H_3 and H_4.

P – H: The availability of Protection P_3 and P_4.

H – D: How often the HW/SW element is working on device D_3.

6. Conclusion

In this paper we demonstrate our improved model of cybersecurity vulnerability. All important aspect of cybersecurity vulnerability are considered. There are a lot of possible threat types. If we put the actors onto the table, all of threat types can be characterized using the “connection graph”. If all of the influencers are drawn, then these factors influence the vulnerability of the single threat on a single device using a single user.

7. References

[1] HADARICS, K., K. Győrffy, B. Nagy, L. Bognár. A. Arrott. F. Leitold (2017): Mathematical Model of Distributed Vulnerability Assessment, 9th International Scientific Conference, Security and Protection of Information, 2017, Brno, Czech Republic

[2] LEITOLD, F., A. Arrott, K. Hadarics: Quantifying cyber-threat vulnerability by combining threat intelligence, IT infrastructure weakness, and user susceptibility 24th Annual EICAR Conference, Nuremberg, Germany, 2016

[3] International Organization for Standardization (ISO), ISO/IEC 27005: Information technology – Security techniques – Information security risk management (2008)

[4] National Institute of Standards and Technology (NIST), Special Publication 800-30r1: Guide for Conducting Risk Assessments (2012), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[5] LEITOLD, F., A. Arrott, and K. Hadarics, "Automating visibility into user behavior vulnerabilities to malware attack" Proceedings of the 26th Virus Bulletin International Conference (VB2016), pp. 16-24, Denver, USA, 2016.

[6] ENISA: Ad-hoc & sensor networking for M2M Communications - Threat Landscape and Good Practice Guide 2017 https://www.enisa.europa.eu/publications/m2m-communications-threat-landscape/at_download/fullReport

[7] VAVOULAS, N., Xenakis C. (2011) A Quantitative Risk Analysis Approach for Deliberate Threats. In: Xenakis C., Wolthusen S. (eds) Critical Information Infrastructures Security. CRITIS 2010. Lecture Notes in Computer Science, vol 6712. Springer, Berlin, Heidelberg

[8] ONWUBIKO, C. (2016) Understanding Cyber Situation Awareness, *International Journal on Cyber Situational Awareness*

[9] LEITOLD, F. and Hadarics, K., "Measuring security risk in the cloud-enabled enterprise." Malicious and Unwanted Software (MALWARE), 7th International Conference on Malicious and Unwanted Software, pp: 62-66, ISBN: 978-1-4673-4880-5. 2012.