UDC 681.13 (043.2)

B.Y. Korniyenko Dts, L.P. Galata
(*National Aviation University, Ukraine*)

Analyzing information risks of the simulation polygon for protection of the critical information resources

In this article, the research of information system protection by analyzing the risks for identifying threats for information security is considered. A quantitative method iRisk for security estimation is used. The known vulnerabilities of used software and hardware are considered and the stability of the built simulation polygon for the protection of critical information resources to specific threats is calculated.

Based on the fact that quantitative methods in conducting a risk analysis at software and technical protection level and if not take into account organizational and technical component, are more effective, it should choose a quantitative evaluation method of protection. Among the main quantitative methods for analyzing information risks RiskWatch, Digital Security, ISRAM and iRisk, the iRisk method is more acceptable [1].

IRisk method

The iRisk method is formally one of the simplest estimates of information security quantitative risks for automated system. In general, it is calculated by the following equation:

$$\text{iRisk} = (\text{Vulnerability} \cdot \text{Threat}) - \text{Controls} \quad (1)$$

First of all, we have calculated Vulnerability, by using the standard CVSS v3 [2]. The standard includes three groups of metrics required for calculation: base, temporal and environmental. The value of the metric is accepted as a pair of vector (specific values of individual indicators) and a numerical value, which is calculated basing on all indicators and using the formula defined in the standard.

The threat is calculated by the formula 2, where Likelihood (correlation from table ARO [2]). If the threat is on a scale from 100 to 50 - the level of risk is high, from 50 to 10 – medium, from 1 to 10 - low.

$$\text{Threat} = \text{Impact} * \text{Likelihood} \quad (2)$$

Formally, the calculation is not a complicated equation, but this methodology contains a general CVSS vulnerability assessment system, which is supported by market leaders in the field of information security in practice, that allows you to use constantly relevant coefficients for calculating vulnerabilities, and also have a list of all the major vulnerabilities associated with all modern software products that can be used in an automated system.

Software and hardware vulnerabilities

The designed simulation cybersecurity polygon hasn't so many vulnerabilities due to the high-quality equipment, the access control, and the network settings, that limit access to the network from the outside [3]. And still, the vulnerabilities remain on the software and hardware level. Next, we will look at some of them, the calculation of the security of the polygon for the protection of critical information resources will be done using iRisk.

Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384)

We will calculate the base, temporal and environmental metric for Vulnerability calculation, according to the security of the cybersecurity polygon.

Base Score Metrics {Attack Complexity = Low; Privileges Required = Low; User Interaction = None; Scope= Unchanged; Confidentiality Impact = High; Integrity Impact = High; Availability Impact = High}

Temporal Score Metrics Score Metrics {Exploitability = Functional exploit exist}

Environmental Score Metrics {Base Modifiers {Attack Vector = Local; Attack Complexity = Low; Privileges Required = Low; User Interaction = None} {Scope = Unchanged} {Impact Metrics {Confidentiality Impact = Low; Integrity Impact = Low; Availability Impact = High}} {Impact Subscore Modifiers {Confidentiality Requirement = Low; Integrity Requirement = Low; Availability Requirement = Low}}}

The resulting calculation of the base level Vulnerability assessment equal 7.8 out of 10, which is shown in Fig. 1

Fig. 1 The Base CVE-2012-0384 vulnerability metric for the cybersecurity polygon

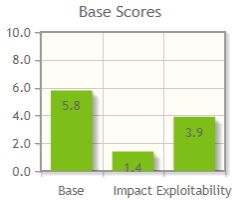

Fig. 2 The Base CVE-2012-1342 vulnerability metric for the cybersecurity polygon

Taking into account that the threat should be realized from inside and first of all is oriented to a normal user without administrator rights and the expected number of threats is estimated as high, then from the ARO table we choose the correlation value *Impact* = 0.9. So, according to the Eq. (2): $Threat = 0.9 \cdot 100 = 90$.

As described in [2], the value *Controls* is estimated at *650*, which will mean - the tool continues to improve.

That is, the value $iRisk = (7.8 \cdot 90) - 650 = 50$ for Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384).

Cisco Access Control Bypass Vulnerability (CVE-2012-1342)

In the same way as for the CVE-2012-0384 vulnerability, we will calculate the *iRisk* value.

Base Score Metrics {Attack Vector = Network; Attack Complexity = Low; Privileges Required = None; User Interaction = None; Scope= Changed; Confidentiality Impact = None; Integrity Impact = Low; Availability Impact = Impact None}

The value *Vulnerability* = 5.8, by the CVSS v3.0 calculator (Fig. 2).

The calculation of the value $Threat = 1.4 \cdot 0.72 \cdot 100 = 108$, so the value $iRisk = (5.8 \cdot 108) - 610 = 16.4$, which means that the vulnerability will be approximately equal to zero, that is we can conclude that this vulnerability can be exploited by an attacker with little probability.

EternalBlue vulnerability (CVE-2017-0144)

Calculate the iRisk value for CVE-2017-0144 EternalBlue vulnerability.

The base EternalBlue vulnerability metric will have the following parameters. The result is shown in Fig. 3

Base Score Metrics {Attack Vector = Network; Attack Complexity = High; Privileges Required = None; User Interaction = None; Scope= Unhanged; Confidentiality Impact = High; Integrity Impact = High; Availability Impact = High}

Since the attack is conducted from the outside and its' probability is very high, the attacker should be an hacking expert, according to the iRisk method in this case, the value *Impact = 100*, and the value *Likelihood = 0.7* and the value *Threat =70*,

So, you can calculate the *iRisk* value for CVE-2017-0144, without the security patch from March 14, 2017.

iRisk = (8.1 × 70) - 0 = 567.

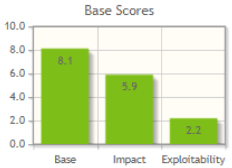

Fig. 3 The Base CVE-2017-0144 EternalBlue vulnerability metric for the cybersecurity polygon

Fig. 4 The Base CVE-2017-5754 Meltdown vulnerability metric for the cybersecurity polygon

Meltdown vulnerability (CVE-2017-5754)

Calculate the *iRisk* value for a cybersecurity polygon, without KAISER patch.

Calculate the base metric for Meltdown vulnerability (CVE-2017-5754), the result is shown in Fig. 4.

Base Score Metrics {Attack Vector = Local; Attack Complexity = High; Privileges Required = Low; User Interaction = None; Scope= Changed; Confidentiality Impact = High; Integrity Impact = None; Availability Impact = Impact None}

Taking into account that the attacker can act both from the outside and inside and the attack can be executed frequently, and the attacker can have just an advanced level of skills and the attack code is shown in large numbers of articles, all of this will give: correlation value of *Impact = 0.9;* the value of *Threat* will be equal to *100 · 0.9 = 90.*

The resulting value of *iRisk* for Meltdown (CVE-2017-5754) will be equal to *iRisk = (5.6 · 90) -0 = 504*, because without the KAISER patch this Vulnerability doesn't show itself, and is included in the architecture of most modern processors.

SPECTRE vulnerability (CVE-2017-5753, CVE-2017-5715)

Calculate the *iRisk* value for the Specter vulnerability. The base metric in both versions of the vulnerabilities implementation is the same, the results of the calculation are presented in Fig. 5.

Base Score Metrics {Attack Vector = Local; Attack Complexity = High; Privileges Required = Low; User Interaction = None; Scope= Changed; Confidentiality Impact = High; Integrity Impact = None; Availability Impact = Impact None}

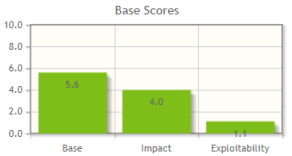

Fig. 5 The Base Spectre CVE-2017-5753 i CVE-2017-5715 vulnerability metric for the cybersecurity polygon

Calculate the *iRisk* value for CVE-2017-5715, given the complexity of the exact implementation and the impact only on the information confidentiality. So the value of *Impact = 50* (including financial, reputational and strategic impact). Given that the vulnerability will be try to use mainly from the outside and the attacker must have advanced technical skills, the correlation value *Likelihood = 0.64*. These parameters are typical for both CVE-2017-5753 and CVE-2017-5715.

However, the *Controls* parameters in this case need to be evaluated in different ways. There are patches for CVE-2017-5715 vulnerability, which partially solve this problem only in some cases, so value *Controls* can be considered *Initial/Ad-Hoc = 100,* but it's provides only some protection value. As to CVE-2017-5753 vulnerability, value *Controls* can be considered as *0*, as this problem is not resolved at this time.

So, for CVE-2017-5715 $iRisk = (5.6 \cdot 50 \cdot 0.64) - 100 = 79.2$.

For CVE-2017-5753 $iRisk = (5.6 \cdot 50 \cdot 0.64) - 0 = 179.2$

Conclusions

The iRisk method was chosen for the research, first of all because this technique is free, enough informative, includes another CVSS v3 vulnerability assessment method, which is actively supported by the National Institute of Standards and Technology. Automated system has been tested for the main known vulnerabilities. Conclusions have been shown about the stability of the designed network to specific threats by the iRisk method. It uses the values from 0 to 1000 scope, where 0 corresponds to automated system, in which it is possible to neglect this vulnerability, whereas at the maximum value, if it exceeds 100, it is necessary to solve this vulnerability. The higher the value iRisk the vulnerability is the more critical and has a higher priority for automated system protection.

References

1. Корниенко Б.Я. Информационная безопасность и технологии компьютерных сетей : монография // ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. − 2016. – 102 с.
2. Common Vulnerability Scoring System v3.0: User Guide
3. L. Galata, B. Korniyenko, A. Yudin. Research of the simulation polygon for the protection of critical information resources//Информационные технологии и безопасность. Материалы XVII Международной научно-практической конференции ИТБ-2017. – К.: ООО "Инжиниринг", 2017. – С. 35-51. ISBN 978-966-2344-59-2