National taxonomy for computer-security incidents

Version 1

June 2018

Co-financed by the European Union
Connecting Europe Facility

The project is co-financed through Connecting Europe Facility (CEF) program of the European Commision, Agreement number: INEA/CEF/ICT/A2016/1334308 (Action No: 2016-HR-IA-0085)

Publicity Disclaimer

The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained therein.

Content

Glossary

Key concepts related to cyber security issues, i.e. threats for information systems that arise from cyber space are defined and clarified bellow.

Cyber space – space within which communication between information systems takes place. In the context of the National Cyber Security Strategy of the Republic of Croatia, Internet and all its related systems are included.

Cyber security – includes activities and measures required to achieve confidentiality, completeness and availability of data and systems in the cyber space.

Cyber attack – malicious impact on information systems, computer networks and other electronic resources that occurs in a cyber space in order to compromise the confidentiality, completeness and availability of data generated, processed, stored and transmitted by those systems, networks and resources.

Cyber event – every occurrence in a computer network or information system that can be perceived.

Threat – a potential source of unwanted events.

Computer-security incident – one or more computer-security events that have compromised or are compromising the security of an information system or computer network and compromise the confidentiality, completeness and availability of information that is generated, processed, stored or transmitted using an information system or a computer network.

Cyber crisis – event or series of events in the cyber space that may cause or have already caused a greater disruption in the social, political and economic life of the Republic of Croatia. Ultimately, such a situation may affect the security of people, the democratic system, political stability, the economy, the environment and other national values, namely the national security and defense of the state in general.

Taxonomy – science, technique or method of classification.

Attack Vector – defines a path that the attacker uses to gain access to the system.

Major incident – a computer-security incident that affects critical data (unclassified and classified) and/or information systems and computer networks in the public and private sector, especially systems that are part of the critical national infrastructure, where these data are processed and transmitted, and which can achieve and/or have a negative impact on the everyday life of a large number of citizens, national economy and national security as a whole.

Introduction

National taxonomy for computer-security incidents is based on the Action plan for the implementation of the National Cyber Security Strategy[1] (further in the text, Action plan). Chapter G of Action plan refers to technical coordination in the processing of computer-security incidents, and the G1 objective states: „*Continuously improve existing systems for collection, analysis and storage of data related to computer-security incidents and ensure update of other data important for rapid and efficient handling of such incidents*".

The first step in carrying out this objective is to define the term of computer-security incidents and its classification at the national level.

In order to have uniformed criteria of event classification in information systems and computer networks of all stakeholders in the area of information and cyber security at the national level, and to successfully generate and share information about these events, it is necessary to establish a „common language" – taxonomy.

Therefore, the first measure of the G1 objective (measure G.1.1.) in the Action plan is dedicated to this task, „*defining taxonomy, including the term of a major incident*".

After accepting and adopting the National taxonomy for computer-security incidents (later in text the Taxonomy), all bodies and institutions will be able to exchange information on computer-security events to inform all participants about the context and details of a particular event or incident.

Furthermore, by accepting this Taxonomy, it will be possible to start work on other parts of Measure G.1.1 that include „*defining protocols for the exchange of anonymous data about significant security incidents and establishing a platform or technology for data exchange*". Without an accepted national classification system, platform or technology development for data exchange is not possible.

[1] National Cyber Security Strategy and Action plan for the implementation of the National Cyber Security Strategy http://narodne-novine.nn.hr/clanci/sluzbeni/2015_10_108_2106.html

Taxonomy of computer-security incidents

Considering a number of stakeholders who can have a different view of cyber events and computer-security incidents in cyber space, successful classification of computer-security incidents is a complex procedure. For example, although CERT (Computer Emergency Response Team) and LEA (Law enforcement agency) have a common goal, they have a different approach in solving and investigating incidents. LEA collects information that can be used during an investigation to determine the evidence of a criminal offense or identify an attacker, while CERTs are primarily focused on gathering information on current threats and attack vectors with the aim of eliminating them and further enhancing of prevention within the cyber space.

For this very reason, there is currently no standardized, internationally recognized taxonomy of cyber events to enable a successful and standardized information exchange. Numerous scientific papers are devoted to this issue, therefore, today there are numerous proposed taxonomies that are exclusively used in individual organizations or countries or they are focused on a particular type of threat (for example, taxonomy of DoS attacks).

There are three important features of taxonomy according to ENISA[2]:

- Classification scheme – the ability to associate related events into groups.
- Dictionary – important for the description of knowledge and entities. This feature is especially important in the Croatian language, since a large part of the concepts in the cyber security domain can not be accurately labeled.
- Knowledge map – provides the ability for users to understand, in short term, the overall structure of a computer security incident processed by the taxonomy.

Creating a national taxonomy has been guided to meet all three of the above-mentioned features and to be adapted to the widest range of future users in the Republic of Croatia.

[2] https://www.enisa.europa.eu/

Information exchange

Information exchange is one of the key mechanisms of successful defense against cyber attacks. Since there are no physical barriers to restrict the cyber space, it allows attackers to carry out attacks regardless of geographical distance, which simultaneously enables attacks on multiple targets.

After being shown as successful, a large number of cyber attacks is being used for years and eventually becomes more sophisticated. Considering mentioned, it is clear that the information exchange related to cyber attacks and defense methods represents an important part of cyber threats defense mechanism.

The basic characteristics of successful information exchange are:

- Timeliness – information is timely (received on time)
- Accuracy – information contains accurate data
- Authenticity – information credibility is not questionable (information source is reliable).

The complexity of the information exchange rises in situation when information are not presented in standardized form, while on the other side, rapid exchange and prompt action upon receipt of information is required. Precisely, exchange speed and prompt action are basic features of each information exchange system. The need for a standardized form of presentation and information exchange imposes itself as the first step in building an information exchange system.

The National taxonomy of the Republic of Croatia (VOUND)

The National taxonomy of the Republic of Croatia was developed by using a model of public released AVOIDIT taxonomy (Attack Vector, Operational Impact, Defense, Information Impact, and Target), developed at the Department of Computer Science at the University of Memphis, USA with appreciation of experience and specificities in the processing of computer-security incidents in the Republic of Croatia. The basic feature of the AVOID taxonomy is that a computer event and/or incident is classified by using multiple attributes. Using this method enables precise definition and differentiation between individual events and incidents.

The National taxonomy is based on the use of attributes that should provide a comprehensive description of all computer-security incidents and events on a national level, which removal requires the information exchange and timely responses of the relevant CERT teams.

In accordance with the mentioned AVOIDIT taxonomy, the National taxonomy of computer-security incidents will use the acronym VOUND obtained by using initial keywords of five attributes proposed for the description of computer-security incidents in the Republic of Croatia (Image 1):

- Attack Vector *(cro. **V**ektor napada)*
- Operational Impact *(cro. **O**perativni učinak napada)*
- Informational Impact *(cro. **U**činak napada na informacije)*
- Attack Target *(cro. Objekt **N**apada)*
- Phase Of The Attack *(cro. **D**osegnuta faza napada).*

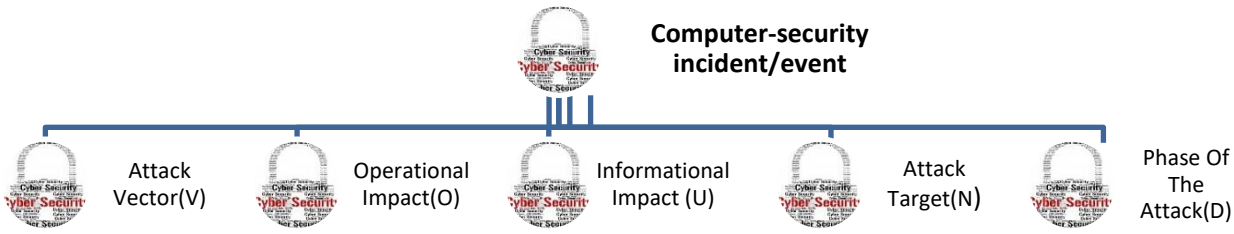

Image 1 Attributes for computer-security incidents description

A taxonomy using the above attributes does not imply that in each case it is possible to describe a single event or incident with a unique value for each individual attribute. For example, a cyber attack can use multiple attack vectors at the same time, and by using the proposed methodology, it is possible to select multiple values of individual attribute for a particular event.

Use of the National taxonomy

The accepted Taxonomy will be used at the national level by companies from different sectors, government bodies and other legal entities and physical persons. The model will serve to allow collection and information exchange among all stakeholders that will use the proposed Taxonomy, regardless of the level of knowledge about the computer-security incidents, and to allow adequate classification of events/incidents. According to the eCSIRT.net[3], the incident classification is defined by minimum set of information (attribute the operating effect of the attack, which describes the direct impact of an attack on an information system or its parts) that should be collected for each event/incident. Therefore, the following criteria are taken into consideration:

1. Easy to use in everyday work
2. Unique classification of a computer-security incident
3. Interpretation of classified computer-security incidents

Along with the minimum set of information that is necessary for the basic classification of events/incidents, VOUND taxonomy allows users to accurately define and mutually differentiate individual events and incidents, depending on their level of knowledge and available information about computer-security event/incident. The description of the event/incident by using all five attributes from the Taxonomy, enables development of more precise statistical models, and potentially the development of models for the early detection and prevention of malicious campaigns, as described in the following chapter Possibilities of further development and implementation in future.

Attack Vector (V)

An Attack Vector is used as an attribute of computer-security incident description in order to define a path that the attacker uses to gain the initial access to the system. The attribute Attack Vector identification can be challenging, especially if the attack is classified as a high level complexity attack where the attackers give extreme attention to hide every step of their attack. Therefore, Attack Vector is in many cases perceived like a legitimate or ordinary course of events.

During the attack, it is not out of ordinary for attackers to use several available vectors, depending on the existing target vulnerabilities, so this attribute does not represent a "unique key" in attack identification. Identifying and understanding the attribute Attack Vector can often be one of the key steps in attack attribution.

This attribute can have various values:

[3] https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

Mark	Value	Description
(V1)	Portable media / devices	The attack was performed using a portable media or a peripheral device. Example: • Malicious code spread through infected USB or CD / DVD.
(V2)	Attack on web technologies	The attack was performed using methods related to web technologies and vulnerabilities of web applications. This attack vector among others, includes: • XSS • SQL Injection • DNS Hijacking • Brute force attacks towards web applications authentication mechanisms, passwords, CAPTCHA protection and digital signatures • Attack on internet browsers in the user environment.
(V3)	Attack on available network and computer equipment	An attack that exploits vulnerabilities in computer networks, network devices, publicly available servers, or computers. This attack vector among others, includes: • (D)DoS • Man-In-The-Middle • Public available resources scanning • False wireless access points • The Impact on the open ports of the public available servers.
(V4)	Physical Attack	Loss or theft of equipment, computers or data storage media. Intentional or unintentional physical action on the equipment, computers or media. This attack vector among others, includes: • Theft and installation of malicious code on notebooks, mobile phones, etc. • Installation of malicious code or device on public available devices such as ATMs, POS terminals, etc. • Installation of malicious code or malicious components of operation system on computer components in manufacturing process or during delivery to customers.
(V5)	Social Engineering	The attack vector that relies on human interaction and mostly involves referring people to violation of common security procedures. This attack vector among other, includes: • Attempt to disclose confidential information by false presentation • Phishing – sending e-mails or SMS with malicious documents or links to malicious web sites • Persuasion to download malicious content, mobile applications, etc.
(V6)	Attack from the internal environment	An attack that includes information, access data and resources available only to the legitimate user who uses these resources for malicious purposes or contrary to internal policies and standards.
(V7)	Unknown	Early phase of incidents identification in which attack vector is unknown.

Operational Impact (O)

Attacks classification according to the operational performance, represents an attribute which describes direct impact of an attack on information system or its parts.

Attribute Operational Impact is defined as a basic set of information that needs to be collected because it answers what actually happened with an affected information system or network. Identification of attribute Operational Impact partly corresponds to the question of attackers motivation and the ultimate goal of attack conduction.

Values that this attribute can have are listed in the table below. During a specific attack, the Operational Impact attribute can have various values, depending on the phase of the attack. In accordance with that, for example, "Information Gathering" value in later stage of attack transforms into the value "Compromise" or "Unauthorized Access Attempt". Therefore, it is often impossible to unambiguously identify the value of this attribute.

Mark	Value	Mark	Subcategories	Description
(01)	Compromise	(011)	Malware URL	Malware URL implies compromised web server with malicious code.
		(012)	Phishing URL	Phishing URL implies compromised web server with fake web page which purpose is stealing data.
		(013)	Spam URL	Spam URL implies compromised web server with unauthorized advertising content.
		(014)	Web Defacement	Web Defacement implies compromised web server with modified layout and content of the web page.
		(015)	System infected with malicious code	Implies that computer or some other device is compromised by malicious code. Bots, i.e. computers under the attackers control are part of this category.
		(016)	C&C	C&C implies a control server for controlling and managing computers that are part of a botnet.
		(017)	User account	User account implies that user account is compromised.
(02)	Collecting information	(021)	Scanning	Scanning implies unauthorized automated gathering of information related to computer networks and systems.
		(022)	Phishing	Persuading users to provide data via various communication channels (usually e-mail).
		(023)	Sniffing	Sniffing implies unauthorized network traffic interception.
(03)	Unauthorized Access Attempt	(031)	Password guessing	Password guessing implies unauthorized attempt to access into computer system by multiple password guesses.

		(032)	Vulnerabilities Exploitation Attempt	Vulnerabilities exploitation attempt implies an attempt to exploit vulnerabilities on a computer system in order to gain an unauthorized access that impact on data confidentiality or integrity.
(04)	Denial of Service	(041)	Volumetric attack	Volumetric attack implies attack with sending numerous IP packages to congestion network bandwidth.
		(042)	Application layer attack	Application layer attack implies sending numerous requests to a computer system in order to exploit system resources or to exploit a security vulnerability that leads to the end of the application.
(05)	Unsolicited electronic messages, offensive content, harassment, disinformation	(051)	Spam	Spam refers to unsolicited e-mails with advertising content.
		(052)	Hoax	Hoax implies e-mail with disinformation content sent to intimidate or disinform the recipient.
(06)	Advanced persistent threat (APT)			APT implies targeted attack on a specific victim with the use of numerous advanced techniques and technologies.
(07)	Frauds			This class of events includes events that can be categorized as cybercrime, and involves various types of internet fraud, from false presentation to e-commerce frauds, etc. this class of events does not include financial fraud involving the installation of malicious code.
(08)	Other			It implies any events that can not be described by attributes mentioned above, and which are considered as computer security incidents from user perspective.

Informational Impact (U)

The ultimate goal of any cyber attack is to realize effect on data/information in terms of disruption of one of the three basic information security principles: confidentiality, completeness and data availability.

Impact of the attack on the protected information is classified by the attribute Informational Impact, which also clarifies the criteria for selecting a particular attribute value.

Mark	Value	Description
(U1)	Modification/Distort	Breaking the information integrity, usually resulting in a change or "distortion" of the data during the attack.
(U2)	Disruption (Access denial etc.)	Denial of a service availability that provides access to information, usually due to (D)DoS attacks.

(U3)	Destruction	Destruction of information usually occurs when the attack for the ultimate goal is to delete data or remove access rights.
(U4)	Disclosure	Disclosure of information implies a situation in which an attacker achieves "insight" into information to which in normal circumstances would not have an access.
(U5)	Unknown	Early detection phase of an incident in which the impact of information attacks is unknown yet.

Attack Target (N)

Type of informational infrastructure that is target of cyber attack is classified through attribute Attack Target. By correct attribute classification, it is possible to draw conclusions about the attacker's motives and to predict the incident spread in the future.

Similar to the attribute Operational Impact, this attribute also changes its value depending on the phase of the attack, during attacker's lateral "movement" upon his successful unauthorized access to the original attack object. Therefore, it is often impossible to unambiguously identify the value of this attribute. This attribute can especially be ambiguous during the (D)DoS attack when is not entirely clear whether the object of the attack is a computer network or application system.

Mark	Value	Description
(N1)	Operating infrastructure	Attack on the critical system components that manage information system activities and resources (e.g. Active Directory).
(N2)	Computer network	Attack on the network infrastructure.
(N3)	Local computer	Attack which goal is to compromise a local computer (individual user).
(N4)	User	The goal of the user attack o is to collect user's personal information.
(N5)	Application	Attack on the application is attack focused on a specific application or some application component in order to deny availability, compromise data or further spread the scope of the attack.
(N6)	Other	The attack target that is not described by predefined values.

Phase Of The Attack (D)

Current phase of cyber attack is identified by the attribute Phase Of The Attack. Although, in real-life situations, cyber attacks phases exchange in very short intervals, it is possible to identify in which stage the malicious attackers and campaign are located.

With the correct and timely classification of this attribute, it is possible to make decisions on defense strategies that can prevent the attacker from going into further phases of the attack, upon which defensive action can have a significantly narrowed set of possibilities.

Mark	Value	Description
(D1)	Scouting	Phase of the attack in which attacker collects information about the target and prepares attack strategy depending on the detected vulnerabilities. This phase includes scanning with automated tools, collection of email contacts for potential use of social engineering mechanisms, etc.
(D2)	Delivery	Phase of the attack in which an attacker activates cyber attack mechanisms. This phase typically refers on emails with malicious content in case of cyber attack that uses a malicious code or launching a malicious code generation tool in case of DoS attack.
(D3)	Access Granting	Phase of the attack in which an attacker exploits system vulnerabilities and achieves access to a targeted system. At this phase, an attacker usually installs a malicious code, maximizes escalation of privileges, and depending on the scope extends the scope of attacks by expanding to related systems and computers.
(D4)	Complete compromise	Final phase of the attack from the perspective of the attacker. In this phase, attacker achieves goals and motivation for the attack. This phase typically involves exfiltration, destruction or modification of data, denial of services, launch of new attacks using compromised system resources, etc.
(D5)	Persistence	Phase of the attack in which attackers achieve a permanent presence in a compromised system with activated capabilities of detection prevention.
(D6)	Unknown	Phase of the attack is not possible to be determined.

Possibilities of further development and implementation in future

The accepted Taxonomy should be used as a tool that will allow efficient exchange of information and that will enable faster detection and prevention of computer-security incidents. The National taxonomy of computer-security incidents:

1. Allows quick identification, description of computer-security incidents and events through five attributes that are characteristic for every cyber attack (examples in Appendix 1).
2. Opens space for additional upgrade of attributes in cases of new threats (e.g. new type of vector attack).
3. By using five attributes described, enables the creation of detailed statistical reports within individual organization or at a national level, in order to monitor trends and the success of defense mechanisms used.
4. Enables tracking the attack or campaign flow, along with ability to quickly predict the next attacker's step by using Attack target and Phase Of The Attack attributes (examples in Appendix 2).

There are directions that are not primarily within the scope of the original goal of establishing information exchange system and the National taxonomy of computer-security incidents development, but they could be considered as upgrades and future directions of development.

1. Planning of a national system for cyber attacks risk assessment based on the proposed taxonomy – by correct identification of taxonomy attributes and correlation with "the value" and the significance of a specific target, it is possible to assess the risk of a particular computer-security incident. Furthermore, it is possible to implement integration with incident/event classification system, Traffic Light Protocol (TLP)[4]. TLP provides a simple and intuitive classification scheme that indicates the conditions under which sensitive information can be shared.

2. Automation – with the potential automation of the incident recognition process and with classification through the proposed taxonomy, it is possible to build an appropriate strategy system and a defense mechanism at the early stage of a cyber attack. Once when the information exchange system, based on the proposed taxonomy, becomes more widely accepted and a larger number of events and incidents are processed through it, it will be possible to use the collected knowledge and to make certain conclusions on the actors promptly after reporting the event or incident. Also, collected knowledge could be used to define the defense strategy and to assess the impact on the overall level of security.

[4] Traffic Light Protocol (TLP) - implies the way of informing the recipients about restrictions in further information sharing. More about TLP on this link https://www.first.org/tlp/

Attachment 1 – Identification of known computer-security incidents by applying Operational Impact attribute

Threat type	Value	Subcategory
Ransomware – data encryption	Compromise	System infected with malicious code
Web Defacement	Compromise	Web Defacement
Network scanning with the nmap tool	Collecting information	Scan
Phishing page	Compromise	Phishing URL
Zeus Control Server	Compromise	C&C
Phishing campaign	Collecting information	Phishing
Spam campaign	Unsolicited electronic messages, offensive content, harassment, disinformation	Spam
A compromised Gmail account	Compromise	User account
SYN flood	Denial of service	Volumetric attack
Brute force	Unauthorized access attempt	Guessing passwords
Mirai bot	Compromise	System infected with malicious code

Attachment 2 – Identification of known computer-security incidents using five attributes of VOUND taxonomy

Zeus campaign

Attack Vector (V)	Operational Impact (O)	Informational Impact (U)	Attack Target (N)	Phase Of The Attack (D)
Social Engineering (5)	Compromise/ System infected with malicious code (1/5)	Disclosure (4)	User (4)	Compromise (4)

V5_O15_U4_N4_D4

Ransomware – data encryption

Attack Vector (V)	Operational Impact (O)	Informational Impact (U)	Attack Target (N)	Phase Of The Attack (D)
Social Engineering (5)	Compromise/ System infected with malicious code (1/5)	Destruct (3)	Local computer (3)	Compromise (4)

V5_O15_U3_N3_D4

Ransomware – configuration files encryption

Attack Vector (V)	Operational Impact (O)	Informational Impact (U)	Attack Target (N)	Phase Of The Attack (D)
Social Engineering (5)	Compromise/ System infected with malicious code (1/5)	Disrupt (2)	Operating Infrastructure (1)	Compromise (4)

V5_O15_U2_N1_D4

Web Defacement

Attack Vector (V)	Operational Impact (O)	Informational Impact (U)	Attack Target (N)	Phase Of The Attack (D)
Attack on web technologies (2)	Compromise / Web Defacement (1/4)	Distort (1)	Application (5)	Compromise (4)

V2_O14_U1_N5_D4

Scan

Attack Vector (V)	Operational Impact (O)	Informational Impact (U)	Attack Target (N)	Phase Of The Attack (D)
Attack on network equipment (3)	Collecting information/Scan (2/1)	Disclosure (4)	Network (2)	Scouting (1)

V3_O21_U4_N2_D1

DDoS – SYN flood

Attack Vector (V)	Operational Impact (O)	Informational Impact (U)	Attack Target (N)	Phase Of The Attack (D)
Attack on network equipment (3)	Denial of service/ Volumetric attack (4/1)	Disrupt (2)	Network (2)	Compromise (4)

V3_O41_U2_N2_D4

Attachment 3 – Tracking the attack progress and predicting the next attacker steps using five attributes of VOUND taxonomy

Example – Spyware campaign flow

The start of an attack is marked by a computer compromise that does not necessarily have to be the ultimate goal of the attack.

Attack Vector (V)	Operational Impact (O)	Informational Impact (U)	Attack Target (N)	Phase Of The Attack (D)
Social Engineering (5)	Compromise/ System infected with malicious code (1/5)	Disclosure (4)	Local computer (3)	Compromise (4)

V5_O15_U4_N3_D4

In the next phase of the attack, attackers are attempting to expand on the network and compromise the Operating infrastructure so that the attribute Attack Target changes value to "Operating Infrastructure".

Attack Vector (V)	Operational Impact (O)	Informational Impact (U)	Attack Target (N)	Phase Of The Attack (D)
Social Engineering (5)	Compromise/ System infected with malicious code (1/5)	Disclosure (4)	Operating Infrastructure (1)	Compromise (4)

V5_O15_U4_N1_D4

In case of successful identification and classification of the attack, and with the summed knowledge and experience of previous attacks and campaigns, it is possible to define and implement the defense strategy and/or further activities before proceeding from Phase 1 to Phase 2.

Phase 1 V4_O1_U4_**N3**_D4

Defense strategy:

Remove a compromised computer from the network

Phase 2 V4_O1_U4_**N1**_D4

By using this principle, it is possible to recognize and identify relationships (parent-child) between events and to better understand the dynamics of an attack or campaign.