Information security aspects of virtual museums in Russia

D A Mityushin

Institute of Information Science and Safety Technologies of Russian State University for the Humanities, Miusskaya sq. 6, Moscow, GSP-3, 125993, Russia

E-mail: dalexx@inbox.ru

Abstract. Information technologies are entering the life of modern society by leaps and bounds, sometimes radically changing its image. The influence of information technologies on changing the cultural and spiritual space of many countries is perceptible too. A new phenomenon of modern culture has gone into society – the virtual museum, which has faced completely new problems that real museums have not experienced before. These problems are associated with ensuring the cyber security of virtual museums. The article discusses the features of virtual museums, their advantages and disadvantages compared with real ones. Special attention is given to the information security of virtual museums. The author has found a large number of research and publications deals with virtual museums. However, they practically do not touch on issues related to the cyber security of the object under study. Threats of virtual museums and attacks against ones are analyzed in the article. Security variants against threats are offered.

1. Statement of the problem

In a post-industrial society, not only the principle of production is changing, but also way of life in whole. Information technologies (IT) permeates all areas of life. The information technologies evolvement didn’t skirt cultural space. In connection with this a new phenomenon of modern culture – the Virtual Museum (VM) – occurs increasingly frequently. For example, the Google search engine results 328,000,000 for "Virtual Museum". Thus, today the Museum is a dynamic cultural institution that is rapidly mastering the virtual space.

A VM is an information system (IS), and, like any IS, it has vulnerabilities and is subject to information security threats. The problem of ensuring the VMs security emerges full blown.

The article purpose is to formulate the main threats to virtual museums and to suggest ways to neutralize them.

2. Concept and features of virtual museums

The first full-fledged VM appeared in 1994. In the same year, French student Nicolas Pioche opened the Online Louvre and was immediately chronicled by CERN as the "Site of the year" in the nomination "For the best use of multimedia" [1].

Encyclopaedia Britannica [2] defines the VM as a collection of digitally recorded images, sound files, text documents, and other data of historical, scientific, or cultural interest that are accessed through electronic media.

However, the concept of VM in the Russian-speaking community is not fully defined, and it differs from the one adopted in the English-speaking community.
For example, Maksimova T E [3] understands by VM a digital information resource that is freely available on the web allows you to study cultural and historical material and has certain communication options: e-mail, user feedback, etc. This author emphasizes that museologists are inclined to consider a VM as a representative body of traditional museum on the Internet or as digital collections of real museums. Researchers associated with computer technology consider a VM just as a type of website or a type of digital creation.

Russian museum encyclopedia [4] gives two definitions of VM:

- VM is a computer model of an invented (marked by the author) museum that exists exclusively in virtual space. It reproduces some components of a real museum: catalogues of "collections", "exposition", etc. As a rule, it differs in the possibility of feedback with site visitors, widely presented reproductions of "museum objects", 3D "virtual expositions" those allow making a virtual tour through the "exposition" and even its independent modeling.
- VMs are electronic publications of artifact collections. These collections are grouped by a thematic, regional, problematic or other principle, but they are actually located in different places and do not constitute collections. For the man in the street the site of a real museum designates often as a VM.

At the same time, the Technical recommendations for creating virtual museums of the Ministry of Culture of Russia define VM as an interactive multimedia software product that presents museum collections in electronic form. The recommendations emphasize that the VM, which is accessed via the official website of the real museum, via the portal https://www.culture.ru, is not part of the official website of the museum or the portal https://www.culture.ru. It is a self-dependent application.

In this article, therefore, we will regard VM in the wide and narrow sense. In the wide sense a VM is an IS that belongs to a namesake cultural establishment. In the narrow sense a VM is a web platform that provides access to content, including multimedia technologies and related services.

VMs have a huge quantity of varieties. They are created by members of real museums, as well as not existing in reality museums, for ex., a Virtual museum of things Thngs.co. There are museums of educational institutions and administrative divisions (for example, universities, theaters, kindergartens, villages, etc.). VMs can also be created by individuals. Despite the fact that the VM does not exist in the real world, but it is based on real museum pieces.

Virtual museums have a wide range of advantages of real ones:

- VM is some kind of "personalized museum" for the visitor, according to his preferences and interests, in contrast to the real one, where "personalization" of the exposition is a too seldom event [5];
- as a rule, a real museum cannot display all its pieces simultaneously because of a lack of rooms or space, while the VM "area" is limited only by the servers memory;
- increased protection of real exhibits from theft and deliberate damage;
- digitizing of priceless rarities allows showing them a large number of visitors, while real exhibits may require serious attention to both storage and exhibition conditions;
- the museum pieces digitizing will allow visitors to "see" them in more detail (for example, stamps) or to study them better, if this is about, for example, an ancient multi-page tome;
- the user is able to visit any VM in the world from anywhere in the world only by having Internet access;
- VMs more promote the restriction of illegal trade in cultural property [6];
- the museum pieces digitizing allows to keep an idea of ones, in case of its theft, destruction from time or deliberate destruction (one can remember the destruction of architectural monuments and looting of museums by DAESH militant in Syria and Iraq).

Of course, VMs have shortcomings. One can mark out two ones:
• lack of museum atmosphere, "feeling of antiquity", a touch of a long-gone era;
• the appearance of new threats that real museums did not have to face.

3. Research and publication analysis
Analysis of research and publications on the article topic shows the VM security issue is not sufficiently studied.

For example, the scientific electronic library eLIBRARY results 1044 publications (September 2020) for the request "virtual museum". Of these only two articles [7, 8] are devoted to VM security, while the second work is mainly devoted to augmented reality museums.

Search queries in Yandex and Google for the phrases "cyber security of virtual museums" and "cyber-attacks against (aimed at, on) virtual museums" was given too few information.

Two articles were found in the English-speaking Internet segment.

The representative of the Australian Museum Victoria Wendy Pryor [9] focuses on the IS of the real museum. This system is related to the data processing of the business activities of real museums (selling tickets and products via the Internet, collecting and updating participant data, sending electronic newsletters, registering donations, providing employees with access to software for cataloging collections or negotiating agreements with commercial partners).

Another article narrates about the attack on the Asian Art Museum website of San Francisco [10]. Hackers attacked the museum after transferring money from sponsors and benefactors. The Museum refused to pay the required ransom in accordance with official city policy.

No information was found about attacks on Russian VMs, but in a private conversation representative of the Museum of the Russian icon reported attacks on this Museum and other VMs occur constantly. But museums don't talk about it.

As previously unsolved problems, we can mark out main threats, possible goals and motives of intruders.

4. Virtual museum information security threats
An information security threat (hereinafter referred to as a threat) is a set of conditions and factors those create a potential or actual risk of information security violations.

Most VMs, especially large ones, are distributed information systems. To classify threats, one can use the Basic threat model of the FSTEC Russia, describing possible personal data security threats.

When considering a VM in the wide sense, the following threats can be implemented:

1) Threats of information leakage via technical channels:

   • acoustic (speech) information leakage channel;
   • image information leakage channel;
   • information leakage via the compromising emanation (TEMPEST).

2) Threats of unauthorized access (hereinafter – UNA) to information processed at the automated workplace (AWP):

   • threats that are implemented during the booting of the operating system (hereinafter – OS) and are aimed at passwords or IDs intercepting, BIOS modifying, and boot management intercepting;
   • threats that are implemented after the OS loading and aimed at UNA performance using standard OS functions (destruction, copying, moving, formatting media, etc.) or any application program (for example, a database management system), or using programs specially created for UNA performance (programs for viewing and modifying the registry, searching for texts in text files, etc.);
   • malware introduction threats.
3) Threats that are implemented using internet protocol from external networks:

- network traffic analysis with interception of information transmitted from the IS and received in the IS from external networks;
- scanning threats aimed at identifying used operating systems types, network addresses of workstations, network topology, open ports and services, open connections, etc.;
- introducing a false object both in the IS and in external networks;
- trusted object substitution;
- foisting a false route by unauthorized changes of route and address data both within the network and in external networks;
- password detection threats;
- denial of service (DoS) threats;
- remote app launch threats;
- malware introduction threats via the network.

Considering a VM as a web platform, we can identify the main threats and vulnerabilities are typical for web platforms. These are [11]:

- All kinds of injections, including SQL, LDAP, etc.
- Cross-Site Scripting (XSS).
- Broken Authentication and Session Management.
- Insecure Direct Object References.
- Cross Site Request Forgery (CSRF).
- Security Misconfiguration.
- Failure to Restrict URL Access.
- Unvalidated Redirects and Forwards.
- Insecure Cryptographic Storage.
- Insufficient Transport Layer Protection.

The most often used attack is SQL injection. For example, according to the Akamai Intelligent Edge Platform, only in the day of September 6, 2020 were detected 71,717,000 attacks on web resources, and they were distributed as:

- SQL Injection 64,851,530 90.43%
- Cross-Site Scripting 3,719,830 5.19%
- Remote File Inclusion 3,107,860 4.33%
- PHP Injection 24,820 0.03%
- Command Injection 12,960 0.02%

Now it is necessary to define the possible goals and motives of the intruders. For this purpose does not matter their kind, i.e. external or internal intruder. What matters is their potential, i.e. their ability to implement threats. We note only that the Basic threat model of the FSTEC Russia sorts external intruders:

- intelligence services of states;
- criminal structures;
- competitors (competing organizations);
- unfair partners;
- individuals.

The potential goals and motives of intruders, along with the "classic" ones – revenge, profit, hooliganism – include the following.
• Theft of master copies of digital museum items available on VM servers for the purpose of making physical counterfeit based on them.

• The study of the real museum for the implementation of criminal intentions. Many VMs have 3D panoramas of the physical museum. Using this panorama an intruder planning to commit a real crime (for example, stealing the original exhibit) will be able to study in detail the map of the museum's halls, determine the location of cameras, motion sensors, and so on. This will allow him to carefully plan his action that can be succeed.

• Theft and other manipulation with personal data of visitors, sponsors, founders, benefactors and museum employees. Since one of the directions of information security defined by the Information Security Doctrine of the Russian Federation is to ensure the protection of citizens from information threats by forming a culture of personal information security, the author considers necessary to draw attention to this type of threat.

• Placement of phishing links and links to illegal content on site sections that may not be seriously monitored by security service employees or IT specialists (for example, parts of 3D panoramas where there are no exhibits).

• Using such at first sight a "harmless" and "accessible" site of a VM for training novice hackers for acquirement of experience.

• Falsification or substitution of documents and other exhibits in order to "rewrite" the history of both the Russia and the world in whole, to change the attitude to the Russia’s foreign policy activities. For example, the intruders could avail themselves of the exhibition "Munich-38. On the threshold of catastrophe" (2018/09/20) if the documents presented for the first time on it would be part of the VM exhibition. In the event of a cyber-attack, the intruders could distort the facts of the USSR's participation in those historical events. This could create an erroneous negative perception of the General public about the real causes of the beginning of World War II and the real victims, as well as the accomplices of Nazi Germany [7]. This is also stated in the Information Security Doctrine of the Russian Federation, thus showing that the country's leadership pays serious attention to this threat.

• Destructive psychological influence of private VMs operating outside of state doctrines in the field of protection of cultural and spiritual heritage on society.

Both virtual and real museums can hardly be classified as objects of critical information infrastructure. However, unauthorized influence on the information circulating in the museum's IS, especially its distortion, can have although remote, but very serious consequences.

Based on the listed goals and motives of intruders, VM threats can be divided into three levels [7].

The first level of threats is the implementation of cyber-crimes. It base on the first five points of the goals and motives of the intruders.

The second level of threats is the implementation of internal political and geopolitical conflict potential. It base on the sixth point of the goals and motives of the intruders.

The third level of threats is the antisocial psychological influence. It base on the seventh point of the goals and motives of the intruders.

5. Providing protection against VM threats

Comprehensive measures must be taken to protect virtual museums from threats.

Since a VM in the narrow sense is a web application, it is necessary to understand how these attacks can be carried out. First of all, the intruder will be forced to obtain access to the server where the website's program code is stored in order to cause a destructive influence. As an object of attack, one can also specify the storage of graphic images, including master copies of exhibits. Threats can be implemented using well-known technologies applicable to any IS, such as DNS tunneling, Port Scanning, TOR, I2P, VPN, proxy, etc. [7].

As a protection against these threats, we can suggest a more thorough approach of developers to the organization of VLANs, demilitarized zones, and the creation of access control lists. Special attention should be paid to authorization when writing, modifying, and implementing software codes that directly
implement a web application as a VM. This approach will considerably reduce the risk of implementing first-level cyber threats (1st, 3rd, 4th, and 5th positions of goals and motives of the intruders). To neutralize the second position of the goals and motives of intruders, the authors [7] believe appropriate reasonable to "erase" images of security equipment (video cameras, motion sensors, security posts, etc.) from VM panoramas, and to change the geometry of the displayed halls within certain limits when creating a panoramic 3D exposition.

To protect against a second-level threats it is necessary to study the information published on the VM in detail. This issue is debatable, but it has a serious basis, which in case of illegal actions can endanger the national security of the state in the sphere of spiritual and cultural heritage.

In order to neutralize the third-level threat, it is proposed to regularly monitor web resources, even remotely resembling VMs, and analyze their content.

When considering a VM in the wide sense, it is necessary use properly configured DLP and SIEM systems, as well as systems for detecting and preventing attacks. Do not forget the possible use of social engineering methods by intruders.

6. Conclusion
The formed at the end of the last century virtual museum phenomenon is becoming more and more part of the cultural life of both Russia and the world. Cyber threats to the VM are threats that have not yet fully manifested themselves and have not received a broad scientific understanding. They require an assessment of the risks caused by rapid scientific and technological development, and an understanding of the human-machine systems development processes.

In this paper, we considered the classification of the VM cyber threats and cyber attacks, analyze the goals and motives of the intruder, and how he can implement threats against the VM. This will allow us to move forward in the direction of a comprehensive solution for the problems of providing information security for domestic museums, including their virtual implementation.

References
[1] Veteranova D S 2018 Virtual Museum: Concept, Features and Opportunities Information and Computer Technologies in the Economy Education and Social Sphere 4(22) 142-7
[2] The Editors of Encyclopaedia Britannica 1998 Virtual museum https://www.britannica.com/topic/virtual-museum
[3] Maksimova T E 2015 Virtual Museums: An Analytical Review of Foreign Publications The Bulletin of Moscow State University of Culture and Arts 4(66) 79-84
[4] Russian Museum encyclopedia. Dictionary of Museum terms http://museum.ru/rme/dictionary.asp
[5] Ivarsson Elin 2009 Definition and prospects of the virtual museum (Uppsala Universitet. Department of ALM Museum and Heritage Studies) p 63 http://www.elinivarsson.com/docs/virtual_museums.pdf
[6] Maksimova T E 2013 Virtual Museums: Resistance to Cultural Values Illicit Traffic Historical Philosophical Political and Legal Sciences Culturology and Art History 5-1(31) 125-8
[7] Alakina-Kaminskaya A I and Kazarin O V 2019 Int. Hum. Sci. For. Humanitarian readings of RSUH-2019 "Continuity and gaps: social and humanitarian dimensions" round table topic: "Information security of the cultural and spiritual space of Russia. Countering the destructive influence on young people in social networks" (Moscow: Janus-K Publishing House) p 11-7
[8] Varfolomeeva V V, Kazarin O V, Klimov A A and Lisnyak E O 2019 Int. Sci. and Pract. Conf. Information Security: Yesterday, Today, Tomorrow ed. N V Grishina (Moscow: Russian State University for the Humanities) p 160-8
[9] Wendy Pryor 2017 Staying safe: cybersecurity in modern museums (Museums Victoria, Australia) https://mw17.mwconf.org/paper/staying-safe-cybersecurity-in-modern-museums-internal-external-and-hidden-threats-with-a-focus-on-cryptography-to-maintain-data-security/
[10] Sarah Cascone 2019 Hackers Saw the Asian Art Museum of San Francisco as Ripe for a Ransom Attack. Are Other Cultural Institutions Next? https://news.artnet.com/market/hackers-attack-asian-art-museum-san-francisco-1604188

[11] Budnikov E A and Borisova S N 2015 Web Applications Vulnerability *International Student Scientific Bulletin* **3-2** 267-8