DOI 10.15622/sp.61.6

A.YU. ISKHAKOV, A.O. ISKHAKOVA, R.V. MESHCHERYAKOV,
R. BENDRAOU, O. MELEKHOVA

APPLICATION OF USER BEHAVIOR THERMAL MAPS FOR IDENTIFICATION OF INFORMATION SECURITY INCIDENT

Iskhakov A.Yu., Iskhakova A.O., Meshcheryakov R.V., Bendraou R., Melekhova O. **Application of User Behavior Thermal Maps for Identification of Information Security Incident.**

Abstract. One of the main functions of an information security system is the identification of any access subject to be able to investigate information security incidents. During executing procedures of scanning and vulnerability exploitation, qualified adversaries regularly change identifying features. Such operations can not only obfuscate logging the data in subsystems, thus, complicating the restoring of events chronology for an information security expert but also call into question the irrefutability of the evidence of participation of particular adversary to particular illegal operations.

In the paper analyses of application of modern approaches of adversary identification in web resources, which does not require authentification of main part of users, is given (fingerprinting, analysis of behavioral features).

Along with widely used in web analytics "thermal maps", user adapted profile and computer model of dynamics of "user-mouse" system, authors offer to identify the subjects of information security incident in readily available informational resources of the Internet. The main idea of the prospective approach consists of the following: when a thermal map is built, not only the density of data layout should be considered but also statistical parameters should be defined by an expert (the distance of intensity gradient, distance overlap, etc.). The authors also offer to consider the dynamics of user operations (e.g. calculation of the average duration of data entry into interactive elements). A description of each step of an appropriate technique and also information on its practical implementation are given. Robustness of the given approach is confirmed by a practical experiment. The offered technique is not a universal instrument of adversary identification. Only manual targeted attacks are considered, the cURL tools etc. used by adversaries are not taken into account. Therefore, it is recommended to use this technique exclusively in addition to working protective systems (WAF, IPS, IDS).

Keywords: identification, thermal maps, fingerprinting, biometrics, anonymizing.

1. Introduction.

Today the global Internet is one of the main tools of mass communication. Therefore, its information resources increasingly often become a target of cyber-attacks of malefactors pursuing various aims. In spite of the fact that untargeted hacker attacks dominate the Internet [1], the most serious threat is represented by target hacks.

The popular Internet resources which do not require extra authentification for the main part of users are in the risk zone. Newsfeeds, entertaining portals, Internet shops etc. can be numbered among such resources. In spite of the fact that today the market of information security software vendors provides a large number of various effective solutions for the detection of incidents and neutralization of malicious inquiries, the problem of the imperfection of user identification technologies still remains [2, 3].

Web application security becomes more difficult because of the growing interactivity, increasingly complicated scenarios and support of new protocols. It is not unknown that security of web servers is not anymore limited to the use of classical package OSI filters or stateful firewalls that trace active TCP-sessions. Today the means of traffic filtration of the application level especially focused on web applications (in particular Web Application Firewall) are considered as a traditional and effective approach to security of web resources [4]. The set of WAF functions usually includes machine learning functions and the following security mechanisms:

– protection against SQL-injections and XSS (including proprietary protection);
– signature analysis;
– protocol validation;
– integration with reputation and fraud services;
– possibility of creation of personal security rules;
– integration with other components of complex information security systems.

However, existence of the only WAF — decision isn't sufficient for complex protection of information systems according to various practical researches [3]. Especially it concerns the web-resources which aren't demanding carrying out authentication for the main user audience. The analysis of application of modern approaches to malefactors identification and also the methodical and algorithmic providing, developed by authors, are given further in the paper.

2. Relevance of the study. Web application security is, first of all, a complex of measures which is a part of a system of providing information security of a company as a whole. One of the basic procedures of a security system is the identification of any subject of access for the purpose of investigation of information security incidents. Manufacturers of modern WAF declare the function of calculation of correlations and chains of the attacks. This function allows to group similar operations and to reveal the chain of attack progress — from surveying before the theft of the important data or deployment of bookmarks. As a result, instead of a list of a thousand suspicious events, information security experts receive some tens of really important messages. However, considering a high level of competence and preparation of malefactors during a targeted attack, it is necessary to note that during scanning and vulnerability exploitation the malefactor regularly changes identifying features in order to make the subsequent investigations more complicating. Similar operations not only obfuscate the logging of the data in subsystems, making the restoring of event chronology more complex for an information security expert but also call into question the irrefutabil-

ity of the evidence base to prove the participation of the certain malefactor in certain illegal operations.

Until now widely applied logging methods of users' IP-addresses and methods of storing housekeeping information on the device of a client (Cookie technology) are not effective. When using Cookies, the subject of access possesses the complete control over contents (including legitimate possibilities of destruction and change of data). The given approaches are not capable to resist the use of basic mechanisms of e-mail address broadcasting, Proxy services, anonymizers and dynamic addressing. Besides, it is necessary to consider that even among legitimate and law-abiding visitors of websites, a considerable number of users prefer basic anonymizing resources.

The given condition not only complicates procedures of investigation of incidents but also promotes discrediting of protective mechanisms which automatically add in lists of locking arrays of IP-addresses of services VPN and Proxy, used not only by malefactors but also by quite legitimate users. Thereof, there is an actual necessity of application of such technologies which would allow on the basis of the meta-data gathering to solve the task of classification of user's sessions on real visitors.

3. The analysis of the state-of-the-art investigations in the given area. Many researchers intend to define rational attribute space which provides reliable identification of users by means of indirect characteristics (work environment parameters) or by means of processing of the statistical data on behavioural parameters (methods of dynamic biometric authentication) [6].

Fingerprinting methods have gained wide popularity. Various algorithms, methods, and techniques are actively being developed in order to obtain new results in the given area. For example in [7-9], the questions of user identification of an Internet resource by the basic set of features of the browser are considered. The paper [10] is devoted to the improvement of the reliability of the subject by means of the analysis of auxiliary meta-information on the property array of the user's software. The parameters comprising the most significant attribute space [11] include:

- a list of the installed fonts;
- a set of plug-ins of the browser provided by means of JavaScript;
- the information on OS localisation;
- SuperCookie;
- Canvas fingerprinting etc.

Some examples of the characteristics used in implementations of similar technologies are shown below.

1) Local Shared Objects (LSO) — the type of metadata that is stored as files on each user's computer; today all versions of Flash Player use LSO.

2) HTML5-repositories (localStorage, File API and IndexedDB) are intended for maintenance of constant storage of the arbitrary portions of the binary data corresponding to a specific resource.

3) Isolated Storage — isolated Silverlight storage; as with LSO, from a technical point of view, there are no barriers to storing the session identifiers.

4) The Last-Modified header (date of the cached document version).

5) Cookies — a small data fragment stored on the user's computer.

6) Browser cache objects. This mechanism was not intended to be used as random access storage. But if the service returns a JavaScript to the user document with a unique identifier inside its body and sets the value of headers "Expires / max-age" as distant future, then the identification script will be stored in the browser's cache. After such a manipulation it is possible to access this script from any page in a network, simply requesting the script download from the known URL.

7) Application cache (HTML5) — a set of functions that provides advanced caching of web application resources.

8) SDHC dictionaries. This method is a compression algorithm developed by Google, which is based on the use of the dictionaries provided by the special server. The client receives a dictionary file containing the lines that may appear in subsequent replies. After that the server can simply refer to these elements inside the dictionary, and the client will independently generate a page on their basis.

9) Abstract identifier ETag (tag of the cached document version);

10) Use of the internal DNS browser cache.

11) Other storage mechanisms (window.name or session.storage) which allow to store and request an unique identifier in such a way that it remains even after deleting all browsing history and site data.

12) Use of the protocol features. Origin Bound Certificates (persistent self-signed certificates that identify the client for an HTTPS server) - as a unique identifier, it’s possible to take a cryptographic certificate hash, provided by the client as part of a legitimate SSL handshake. TLS also has "session identifiers" and "session tickets" mechanisms that allow clients to resume interrupted HTTPS connections without performing a full handshake.

Assimilation of the information set forth above most effectively allows us to generate a unique print of the computer in the identification system database [12]. In 2010 the Electronic Frontier Foundation measured more than 18.1 bits of informational entropy which can be used for fingerprinting. However, this research was before the invention of a digital Canvas fingerprinting which added 5.7 more bits. In 2017 the method of cross-browser fingerprinting [13, 14] was introduced, allowing one to track a user from different browsers on one device.

In spite of the fact that in similar papers it is offered to use a suite of the most significant features for identification according to their authors, there is no unified correlation analysis of all features which would allow to reveal relations between them and to optimize attribute space. Considering that many found informative metrics are defined by the methods which are heavy from the computational point of view, similar approaches do not find a wide circulation in view of the necessity of maintaining a fast response of a web resource.

It is necessary to note that the mentioned techniques are effective only for usual web-browsers which do not declare the providing of user's anonymity. In specialized browsers, such as Tor Browser, the majority of developed estimation methods of the hardware and browser environment features are blocked [15]. And considering that the given research is directed on development of a technique of identification of an exclusively prepared malefactor a priori applying tools for a regular change of browser prints, the fingerprinting technology can be applied only with additional mechanisms of identification.

The identification systems based on the syntactic and morphological analysis of text data indexing messages of users with certain keywords cannot be applied in the investigated objects because of their prominent features (the majority of users do not interact with data transfer forms). The algorithms of subject authentication by keyboard handwriting for the same reason cannot be applied in the selected subject domain.

There are approaches based on the registration of features of the operation with a mouse pointing device for identification of its owner, for example [16-19]. In paper [20], the author identifies the user of a computer game on the basis of a neural network. For data processing, the state machine is used. Both the trajectory and accuracy of clicks are evaluated. The software error is 6-20%. In paper [21] the authors offered to use biometric data obtained from the analysis of the mouse use for constant (periodic) authentication of a user. The biometrics data of mouse movements is represented as a reflexion of psychological and behavioural characteristics of a user. Such data as mood and weariness are selected. In paper [22] the comparative analysis of methods conducted in similar researches (with the accuracy of identification from 84% to 99.7%) is carried out. In 2017 researchers developed a prototype of a system considering the speed of mouse movements and features of scroll wheel movements [23]. Despite a large scientific backlog in the given area, it is necessary to note that all enumerated investigations were carried out on the authentication systems applied to the solution of the "Friend or Foe" problem.

Thus, on the basis of the analysis of state-of-the-art research in the selected area, it is possible to conclude that for today there is no complex solution using modern technologies and means in aggregate, and also satisfying current development of the given problem which lies in the identification of the qualified malefactor of generally available information resource.

4. The use of thermal maps. Thermal maps are often connected to cartograms i.e. a way of the cartographical representation visually showing the intensity of any parameter within the territory on a map [24]. Data can be plotted by hatching of various densities, colouring with a certain degree of saturation, or points. Biological thermal maps are used in molecular biology and medicine for representing of data on expression of a set of genes in the various samples obtained, for example, from different patients or in different conditions from one patient. The main principle which lies in the basis in all spheres of application and construction ways of thermal maps is a representation of various values by means of colour, which provides a high level of visualization and accelerates analysis process. Classical thermal maps were used in those areas of science where input data allowed to define colour easily enough for a particular cell (temperature picture in meteorology, levels of gene expression, exchange indexes).

Today there are many different implementations of analytical maps. Below are some examples:

1) "Map of clicks". It is a tool for measuring and displaying click statistics on your web-site. The map displays clicks on all elements of the page (including those that are not links). In this case, you can see not only the interaction of visitors with one page, but also aggregated statistics on the group of pages of the site. For example, you can get statistics for a particular section (Figure 1).

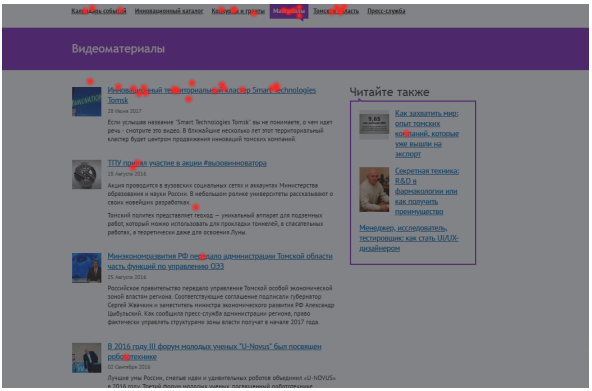


Fig. 1. Map of clicks

Several modes of map display:

– "Heat Map" — warm colours correspond to the frequent clicks, cold colors — rare.

– "Monochrome map" — the density of color corresponds to the frequency of clicks at a given point.

– "Clicks by links and buttons" — the map does not display clicks on items that are not links or buttons.

– "Transparency map" — a click map displays like a "foggy mask": the most clickable elements appear more clearly through the "fog".

– "Map of the elements" — the map displays all the elements of the web-site page.

2) "Map of links" (Figure 2). It is tool for measuring the statistics of the referrals on your site. The links on the map are highlighted in different colours depending on their popularity. When user clicks on a link, the following data is displayed:

– the number of hits by this reference;

– the percentage of following this link on the number of following the other links on web-site.

Fig. 2. Map of links

3) "Scrolling map" (Figure 3) is a tool for analysis how the attention of visitors is distributed to the certain areas of the web-site pages. The map will help to choose the optimal length of the pages and place important information correctly. The map shows the average time and number of views of a specific section of the page if the administrator hover over it. The "scrolling map" can also provide statistics for a group of pages. For example, for a separate directory.

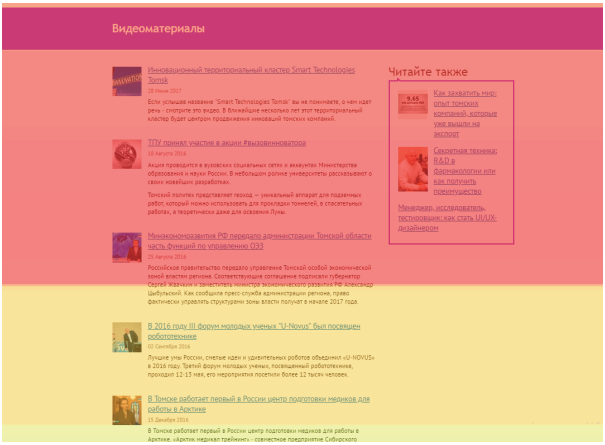
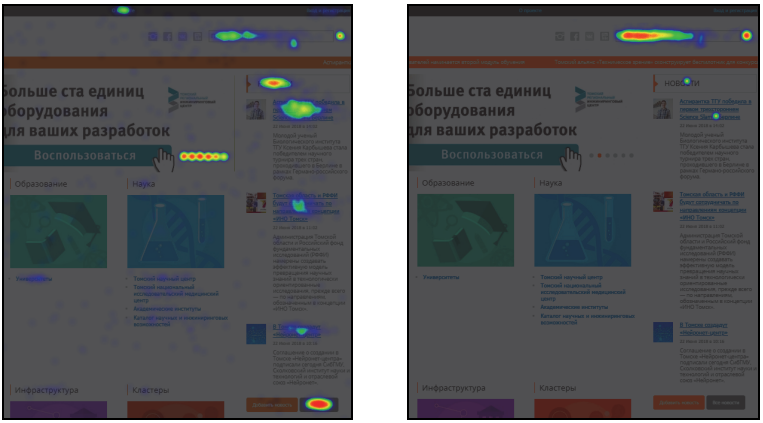


Fig. 3. Scrolling map

In case of application of thermal maps for the task of analytics of user's operations (clicks, motion step of a cursor), it is possible to define the user's activity as a dotted activity. The operations are actually linked to a particular point (pixel) on the screen which seems to be a too small area in comparison with all interface of the system for in-depth study. For the given task, it is necessary to work not with particular points but interactive elements (various data entry forms, which malefactors use for manual exploitation of vulnerabilities). In Figure 4 visualisation of a session of a typical user in comparison with a session of a malefactor is presented.



a) *b)*

Fig. 4. Thermal map *(a)* of a session of a typical user (top).Thermal map *(b)* of a session of a malefactor (bottom)

The number of thermal points and their gradient characterises the purposes and vectors of attacks by the subject of access. The map b on the right shows the interest of the malefactor in interactive elements; this interest stipulated the purpose of vulnerability exploitation in the subsystem of resource security. In this case, it can be clearly seen in the active interaction of the malefactor with the search form on an information portal.

Figures 5-7 show examples of thermal maps of the various user sessions presenting the area of the interactive form allowing users to upload news or to send a press release.

Based on the data about 117 revealed and investigated beforehand incidents of information security (4 large regional news portals) and the subsequent comparison of the facts to visualisation of the events on the data thermal maps, the authors concluded that there are certain prominent features of the use of a mouse pointing device by malefactors during attacks on information resources.

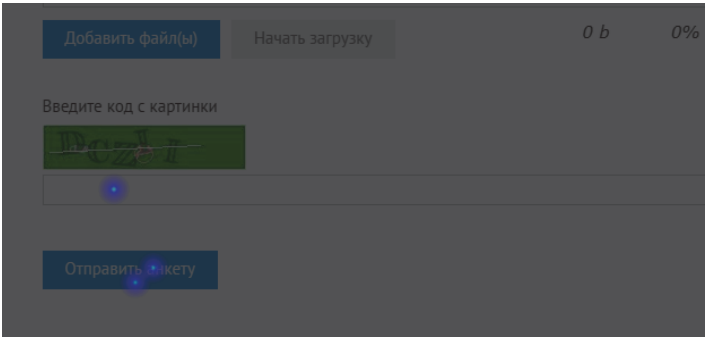


Fig. 5. Thermal map of a session of a legitimate user

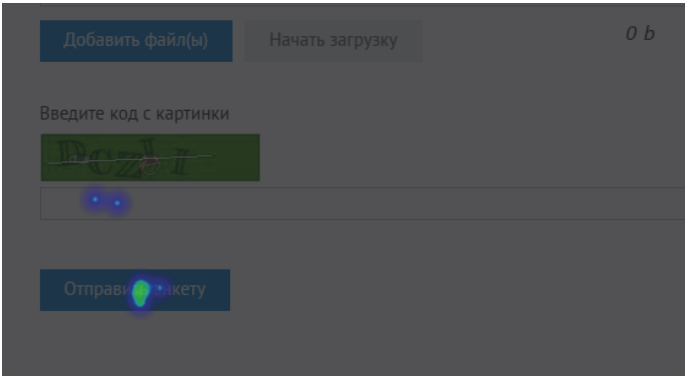


Fig. 6. Thermal map of a session of a legitimate user (some errors are found during the Turing test)

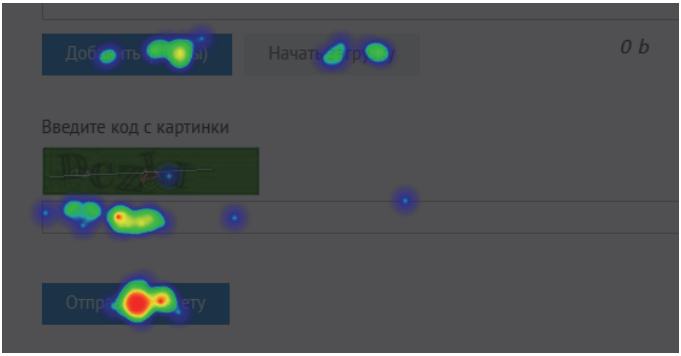


Fig. 7. Thermal map of a session of a user during which the WAF detected attempts of injections and XSS

First, the number of "warm" points in maps of the malefactor is comparable (not more than twice as much) with the number of interactive elements on the page. Under interactive elements, we will understand the data entry forms which are used by the malefactor for sending payload. The maps of sessions of legitimate users are characterised by a wide scatter of clicks on hyperlinks around all perimeter of the screen (tens of times more than the number of interactive elements). Secondly, the data from analytical tool "WebVisor" show that the average time of data entry by the malefactor is several times less than for legitimate filling in the fields with correct data. It is connected to the fact that during the attack malefactors use certain combinations of characters prepared in advance. Besides, one more informative metrics of distinction of the malefactor from the legitimate user can be the number of clicks on interactive elements (which were in advance defined by experts as possible vectors of attacks) in relation to the total number of clicks.

5. Metrics of a user's profile. On the basis of the stated suppositions, the data on functions of "thermal" maps and presumable behaviour of a malefactor, and also with application of the approach and selected in [25] features of user classification according to the pattern "user-mouse", a list of features which will allow to identify the subject of access in the considered task has been adapted.

The formed attribute space for the task of identification of the user according to his or her behavioural activity on a web resource:

1) H — the number of "warm" (activated by the user) points (areas);

2) d — the number of clicks on interactive elements in relation to the total number of clicks:

$$d = \frac{D}{N},$$

where D is the number of clicks on interactive elements, N is the total number of clicks;

3) t_{av} — average time of data entry into the interactive input fields:

$$t_{av} = \frac{1}{k}\sum_{j=1}^{k} t_j,$$

where k is the number of the detected facts of data entry into an interactive element of the page, t_j is time of j^{th} data entry in an interactive element of the page;

4) S — the length of the virtual trajectory, i.e. the distance which user's mouse has passed:

$$S = \sum_{i-1}^{n} s_i,$$

where s_i is the distance which has been passed for provisional time step of measurements according to which the trajectory is measured; the authors considered a minimum value for the personal computer Δt = 15 millisecond as a time step, n is the number of time steps (measurements of sections of a trajectory);

$$s_i = \sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2},$$

where x_i, y_i are the manipulator's coordinates on the screen in i^{th} time step, x_0, y_0 are the manipulator coordinates at the initial instant;

5) V_{max} is the maximum speed of passing of a virtual trajectory of the mouse manipulator for all time steps:

$$V_{\max} = \max_i \frac{s_i}{\Delta t},$$

6) t_{stay} is the time from the moment of aiming of the mouse on the point (t_{point}) till the moment of the click on this point (t_{press}):

$$t_{stay} = t_{press} - t_{point},$$

7) t_{hold} is the time of hold of the mouse manipulator during clicking on a point;

8) α — is the angle between the direction of initial motion (from the index point — (x_0, y_0) to the vertex 3 — (x_3, y_3)) and the line connecting the index point — (x_0, y_0) and the finite point (x_n, y_n):

$$\alpha = \operatorname{arctg}\frac{(y_3 - y_0)}{(x_3 - x_0)} - \operatorname{arctg}\frac{(y_n - y_0)}{(x_n - x_0)}.$$

6. Technique of thermal map building. The approach offered by the authors implies visualisation of the calculated characteristics in the form of a thermal map of user's clicks. During the experiment, the authors faced a problem of lack of the literature and engineering specifications on practical implementation of proprietary algorithms for thermal map building. As a result, paper [22] and initial codes of "Heatmap.js" library from the company Yandex was chosen as a basis for the experiment.

The basic idea of the prospective approach consists in the following: when building a thermal map not only density of layout of data but also static parameters defined by the expert (a distance of a gradient of intensity, an overlap distance, etc.) should be considered. Authors offer to consider the dynamics of user's actions (e.g. calculation of average duration of data entry into interactive elements).

According to [22], every element of dotted activity is represented in the form of a circle with a linear-decreasing gradient of colour intensity from centre to edges. The circle radius (intensity area) is defined by the value of the gradient intensity distance and is specified by the expert. Particular colour of each point on a thermal map is defined according to the value of its cumulative intensity, the sum of intensity values of all areas covering this point, and the selected colour scheme (graphic palette). Values of cumulative intensity are normalised within the limits from 0 to 1. The initial value of intensity gradient:

$$I_s = 1 / MQO ,$$

where MQO is the maximum quantity of circles overlapping each other around whole data area. Two or more circles are considered overlapping each other if the distance between them pairwise is less than the distance value of the overlap specified by the expert.

Finite value of the intensity gradient I_k is always equal to 0. Thanks to calculation of I_s on the basis of MQO, the reliability of lost-free visual data is ensured. At high density of dotted data, the greatest intensity is present in the separate areas actually outlined by these points, instead of where maximum cumulative intensity would be generated. For example, in Figure 8 there are shown 2 areas of intensity. The circles on the co-ordinate plane are presented, where the horizontal axis characterises the co-ordinate (position) of a point, and vertical represents its intensity. While the distance between two points is more than a half of the intensity gradient distance, cumulative intensity is less than 1 (one) as the intensity is calculated according to the linear gradient. When the distance becomes less or equal to a half of value of intensity gradient distance, cumulative intensity becomes more or equal to 1 (one) accordingly.

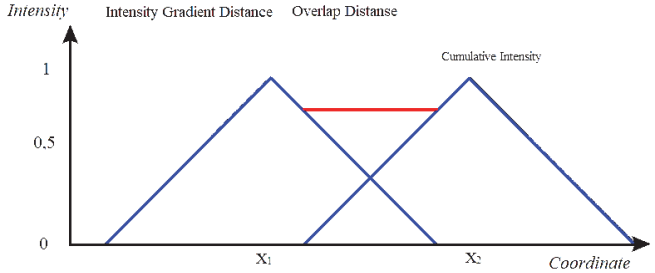


Fig. 8. Intersection of point's intensity regions

Earlier it was noted that in the given task the most interesting is the cumulative intensity of the particular active area of the interface (which, as a rule, interests the malefactor). Therefore, depending on the value of the overlap distance specified by the expert, simplification of visual analytics is up to the point admitted. For example, the clicks on an active element but not on a particular point of this element are important to the expert. If points are on the distance smaller or equal to the value of the overlap distance, there is a recalculation of initial intensity for all points.

Also at the thermal map building, the metrics t_{av} is considered, allowing one to distinguish the border of each interactive element with a characteristic colour from the selected colour graphic palette. It gives the expert an evident picture of objects into which the malefactor inserts various injections.

The method of building the thermal map of user's activity with the above-stated parameters is shown below.

Input data:

– array of dotted clicks of the user's activity (a set of points with the indication of their co-ordinates on a plane);
– distance of intensity gradient;
– overlap distance;
– array of parameters of the colour graphic palette.

Output data:

– The visualised thermal map of user's dotted activity.

Step-by-step description of the method:

Step 1. To receive input data.

The array of dotted clicks of user's activity is generated by means of a specialised script which traces clicks of the mouse on the interface and records the information in a database. The value of the gradient intensity distance, the value of the overlap distance and colour graphic palette are specified by the expert and depend on the nature of the object being analysed.

Step 2. To calculate the *MQO* value.

Step 3. To calculate I_s value according to the formula $I_s = 1 / MQO$.

Step 4. To construct on the map an area of intensity in the form of a circle with centre in the indicated point for each data item of user's activity. In so doing, to define the radius as equal to the value of gradient intensity distance and to construct a linear gradient of intensity value from circle centre to edges. To define the initial value of the gradient as equal to I_s, the finite value as equal to 0 (zero).

Step 4.1. If areas of the intensity of two or more circles are intersected, to calculate cumulative intensity as the sum of values of intensity of all areas covering this point for each point in the field of interception.

Step 4.2. If the value of cumulative intensity is more than 1, to set the value of cumulative intensity as equal to 1 (one).

Step 5. To visualise the thermal map on the basis of values of intensity for each point and the indicated graphic palette.

Step 6. To visualise the thermal map.

7. Experiment description. Yandex and Google web analytics services and the program implementation of the model [25] adapted by authors were installed on one of the popular regional news portals (average attendance more than 50,000 unique users a year). The resource functions on the basis of the "1C-Bitrix: Website management platform". Standard "Proactive Filter" with the configuration of automatic blocking of the source of attack for 30 minutes in the case of detection of suspicious inquiries was used. The imitation of the qualified malefactors' activity was conducted by the representatives of three organizations providing external penetration test of Internet resources. The procedure of testing for penetration was carried out in a stringently certain time period in the mode of greatest possible anonymization.

1) Sessions of bots and vulnerability scanners were eliminated from the access logs (if there are no clicks traced by the specialized script or User Agent null values). After the given operation, a sampling of unique IP-addresses for the reporting period was 79 records.

2) Sessions of conducted attacks (about 70 events of "Security alert" class were recorded) were selected from the WAF register of intrusions. As an automatic blocking was set up in WAF; if the identification of signatures of attacks was regular, the testers' address was added in "Stop list". Penetration testers used a Tor browser and each time when the access was denied, they activated the function of IP-address change.

3) The following task consisted in carrying out classification of the sessions of attacks on real users according to paper [26] with adapted features of users' classification. The measurement of numerical values of the selected information features was carried out. 53 sessions of legitimate users and 10 sessions of penetration testers were conducted for this purpose. The results of numerical values of the defined metrics for profiles of 10 users are brought in Tables 1-2.

Table 1. Numerical values of profiles of 10 users (Heat Map)

No	H	d	t_{av}, sec
1	21.035	0.150	4.125
2	30.154	0.161	10.195
3	25.095	0.017	0
4	16.150	0.092	10.500
5	15.986	0.014	5.116
6	19.845	0.061	6.857
7	20.213	0.181	7.500
8	20.836	0.045	0
9	17.741	0.064	0
10	19.098	0.071	5.150

Table 2. Numerical values of profiles of 10 users (Mouse manipulator)

No	S, m (for 600 sec.)	V_{max}, m/s	t_{stay}, sec	t_{hold}, sec	α
1	422.095	80.268	0.410	0.212	180.550
2	736.950	120.111	0.509	0.262	169.153
3	1022.812	196.504	0.211	0.197	144.122
4	636.568	102.870	0.360	0.290	253.689
5	698.911	60.127	0.390	0.110	190.884
6	902.100	30.006	0.543	0.411	99.117
7	1192.325	105.985	0.480	0.274	123.880
8	1011.750	41.560	0.327	0.346	140.890
9	732.890	59.998	0.399	0.281	111.400
10	442.089	56.012	0.370	0.201	150.688

The results of numerical values of the defined metrics for profiles of 10 penetration testers are shown in Tables 3-4.

Table 3. Numerical values of profiles of 10 penetration testers (Heat Map)

No	H	d	t_{av}, sec
1	4.565	0.468	1.060
2	5.965	0.655	3.458
3	4.198	0.653	3.201
4	6.065	0.719	3.787
5	6.854	0.398	2.008
6	5.782	0.687	1.989
7	4.786	0.586	2.168
8	5.865	0.350	1.469
9	5.569	0.366	1.667
10	5.068	0.387	1.318

Table 4. Numerical values of profiles of 10 penetration testers (Mouse manipulator)

No	S, m (for 600 sec.)	V_{max}, m/s	t_{stay}, sec	t_{hold}, sec	α
1	206.881	39.126	0.226	0.111	201.110
2	301.430	31.075	0.310	0.397	99.335
3	336.865	53.500	0.369	0.186	98.152
4	411.068	40.113	0.407	0.195	96.482
5	350.561	59.873	0.365	0.213	198.548
6	346.012	59.451	0.311	0.200	171.009
7	329.890	60.890	0.225	0.240	209.501
8	298.111	41.669	0.302	0.199	174.694
9	306.623	53.548	0.278	0.238	199.697
10	348.778	51.060	0.200	0.297	98.001

Figure 9 presents the numerical results of comparing the listed characteristics on the "box plot" histograms.

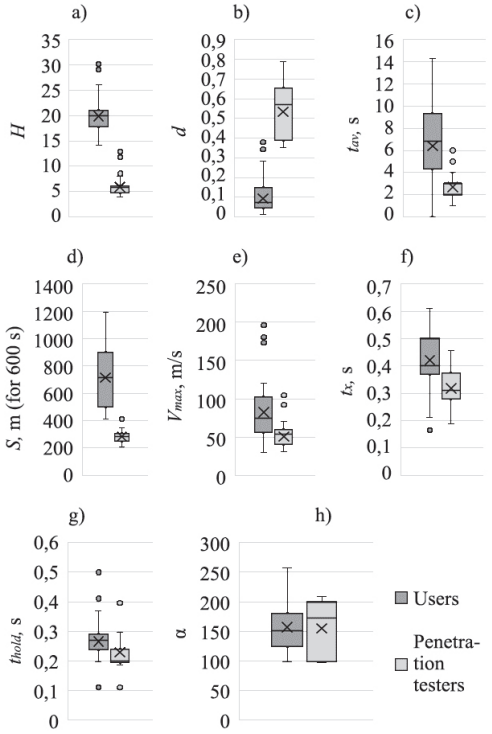


Fig. 9. Histograms (a-h) showing the characteristics numerical differences between the classes of users and penetration testers

The numerical results shown in Tables 1-4 and histograms a-h on Figure 9 allow us to notice that the average quantity of "warm" (made active by the user) areas for the legitimate user fluctuates in the range from 15 to 26, which says that to work with a resource the user uses not less than 15-17 objects in the working area. At the same time, the number of clicks on interactive elements in relation to the total number of clicks is no more than 19%; that is, various links are used, informational tools of the website are researched, and only if necessary the user transmits various interactive inquiries to the resource. Also, the average duration of data entry into interactive input fields considerably differs among certain some users. While analysing numerical parameters in Tables 1-2 as a whole, it is possible to see that deviation of the results from average values is great enough and is up to 50%. The average quantity of the distance passed in 600 seconds (the length of the mouse trajectory) depending on the user's activity fluctuates within 422 to 1192 metres; maximum speed the mouse also considerably varies: from 30 to 197 m/s. The time from the moment of pointing of the mouse on a certain point of a working area till the moment of the mouse click onto this point (object) on the average is equal to 0.399 seconds; time of the mouse button hold during a click is 0.258 seconds.

At the same time, the results of the feature values for malefactor's behaviour (simulated by a penetration tester conducting the test for penetration) have other specific mature. The average quantity of "warm" areas (made active by the malefactor) does not exceed 7; that is, during a session on the average only from 4 to 7 objects of the resource are used and not less than 35% of them are interactive. The given fact says that when searching of weak spots interactive forms for data exchange with the re-source and the analysis of the received results are used more often. The average time of data entry into interactive input fields is on average from 1 to 4 seconds, which speaks about fast data entry owing to available skills of such operations and, probably, applied automation tools for the given process. Deviation of numerical values in Tables 3, 4 from the corresponding average (on columns) is much lower than for values in Tables 1, 2 and is about 30-40%. The distance passed by penetration testers during 600 seconds vary from 206 to 351 metres that is much less than the length of the legitimate users' trajectory. The maximum speed of the mouse was from 31 to 61 m\s, which means that when simulating the actions of the malefactor — purposeful search for vulnerabilities, analysis of objects, and work with interactive fields — there are not any sharp mouse motions, a search of elements in the working area and similar actions. The period from the moment of pointing of the mouse on the object of a resource till the moment of the mouse click by penetration testers is on the average 0.299 seconds, which is lower than the corresponding parameter of legitimate users by 25%; whereas the time of the mouse button hold during a click is comparable with the results in Table 2 and is 0.228 seconds.

The obtained numerical values allow us to preliminary conclude without a special mathematical apparatus the following:

1) average values of feature H naturally differ for different user groups, for legitimate ones the value several times exceeds the value of the malefactor profile;

2) the number of click on interactive elements (input fields, fields of data sending) is significantly higher for malefactors;

3) average time of data entry also differs between user groups;

4) the vector of features for identification of a unique user according to mouse motion (S, V_{max}, t_{stay}, $t_{y\partial}$, α) shows comprehensible results according to research [26]; efficiency of the received values for identification of users should be defined additionally on the basis of the selected mathematical apparatus.

The task of identification of resource users can be presented in the form of mapping $X \rightarrow Y$ where X is a certain image of the user according to models offered in [26], i.e. a set of values of the selected features, and Y is the solution which identifies and-or characterises the user.

To test the efficiency of the offered approach, i.e. implementation of the function displaying the vector of features on an element of a set of known users and characteristics of its behaviour, an artificial neural network was applied. The application of neural networks is for today a widespread tool to make decisions of various types in the automated mode, including for problem-solving, adjacent with the solved one. Neural network learning was carried out on the basis of 75% received designed data (144 000 elementary vector sets).

Parameters of errors of the first and second type, taking into account the recognition of the identity of a user and also his or her behavioural features (detection of ill-intentioned activity) are brought in Table 5.

Table 5. Parameters of errors of the 1st and 2nd type

Task	Errors of the 1st type	Errors of the 2nd type
Recognition of identity of a user	0.079	0.023
Detection of ill-intentioned activities	0.143	0.019

Errors of the 1st type in experiments on recognition of the identity of a user are understood as an amount of cases when the neural network made the decision that the user is not detected, though he or she was in the learning array, errors of the 2nd type are the cases when the user was falsely identified. When detecting a malefactor, the errors of the 1st type are understood as cases of mistaking of the malefactor for the legitimate user; the errors of the 2nd type are understood as mistaking of a legitimate user for a malefactor. Parameters of errors of the first and second type, taking into account the recognition of

the identity of a user and also his or her behavioural features (detection of ill-intentioned activity) are brought in Table 5.

Experimental calculations showed that the user's profile adapted with the application of thermal maps applied in the model “computer-mouse” within the limits of determination of ill-intentioned operations and identification of the subject in the web medium is an effective solution of the relevant scientific task formed above. Undoubtedly, the given method is not a universal tool of malefactor identification — only targeted manual attacks were considered, without consideration of the use cURL tools etc. by malefactors. Therefore, is recommended to use it exclusively in addition to functioning protective systems (Web Application Firewall, Intrusion Prevention System, Intrusion Detection System).

Adaptation of attribute space for the purpose of the solution of adjacent tasks can expand the sphere of "computer-mouse" application. Computing load allowed us to integrate the program implementation directly into the web application in the form of an additional unit-script. Further research has some vectors of development, including the increase of efficiency of determination of required characteristics of a web resource user, simplification of calculations, the increase the number of analysed phenomena, the extension of the spectrum of tasks being solved.

8. Conclusion. The objective opinion on the modern automated systems allows us to talk about the imperfection of existing approaches and technologies of identification of users of the freely available resources selected by malefactors as a target.

The presented method does not allow one to identify absolutely precisely and authentically a particular user but gives a chance to increase the probability of his or her detection in the combination with other indirect methods of identification which allow us with a certain probability to compare the user applying various anonymization means. In the conditions of proceeding development of the information field, the development of similar technologies can become one of priority research directions in questions of counteraction against illegal activity on the Internet.

References

1. Gerasyukova M. [The goal is captured: the most dangerous hacker attacks. Why is target hacker attacks dangerous and how to protect them]. Available at: https://www.gazeta.ru/tech/2018/02/25/11659579/targeted_attack.shtml (accessed: 20.06.2018). (In Russ.).
2. Iskhakov S.Yu., Shelupanov A.A., Mescheryakov R.V. Assessment of security systems complex networks security. Dynamics of Systems, Mechanisms and Machines (Dynamics). 2014. pp. 1–4.
3. Yankovskaya A.E., Shelupanov A.A., Hodashinsky I.A., Gorbunov I.V. Development of hybrid intelligent system of express-diagnostics for detection potential attacker. 9th International Conference on Application of Information and Communication Technologies (AICT). 2015. pp. 183–187.

4. Iskhakov A., Meshcheryakov R., Ekhlakov Yu. The Internet of Things in the security industry. Interactive Systems: Problems of Human-Computer Interaction (collection of scientific papers). 2017. pp. 161–168.
5. Romashev A. [Web Application Firewall Effectiveness Testing and Comparing]. Available at: https://www.anti-malware.ru/compare/web-application-firewall#part4 (accessed: 20.06.2018). (In Russ.).
6. Iskhakov A., Meshcheryakov R., Iskhakov S., Krainov A. Increase in security of authentication services through additional identification using optimal feature space. Proceedings of the IV International research conference “Information technologies in Science, Management, Social sphere and Medicine” (ITSMSSM). 2017. pp. 443–446.
7. Eckersley P. How Unique Is Your Web Browser? Proceedings of the 10th Privacy Enhancing Technologies Symposium (PETS). 2010. pp. 1–18.
8. Alnaami K. et al. Thuraisingham B. P2V: Effective Website Fingerprinting Using Vector Space Representations. IEEE Symposium Series on Computational Intelligence. 2015. pp. 59–66.
9. Iskhakova A., Meshcheryakov R. Automatic search of the malicious messages in the internet of things systems on the example of an intelligent detection of the unnatural agents requests. International Conference on Information Science and Communications Technologies (ICISCT). 2017. pp. 1–4.
10. Bessonova E.E., Zikratov I.A., Kolesnikov Yu.L., Roskov V.Yu. [Method of user identification in the Internet]. *Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki – Scientific and Technical Journal of Information Technologies, Mechanics and Optics*. 2012. vol. 3. pp. 133–137. (In Russ.).
11. Usmonov B. et al. The cybersecurity in development of IoT embedded technologies. International Conference on Information Science and Communications Technologies (ICISCT). 2017. pp. 1–5.
12. Iskhakov A.Y., Iskhakov S.Y., Meshcheryakov R.V [Increase the security of authentication services by performing additional authentication using the optimal feature space]. *Informacionnye tehnologii v nauke, upravlenii, social'noj sfere i medicine. Sbornik nauchnyh trudov – Information technologies in science, management, social sphere and medicine.* 2017. pp. 117–122. (In Russ.).
13. Abouollo A., Almuhammadi S. Detecting malicious user accounts using Canvas Fingerprint. The 8th International Conference on Information and Communication Systems (ICICS). 2017. pp. 358–361.
14. Daud N.I., Haron G.R., Othman S.S.S. Adaptive authentication: Implementing random canvas fingerprinting as user attributes factor. IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). 2017. pp. 152–156.
15. Sistema upravlenija proektami Trac. [Project Management System Trac]. Available at: https://trac.torproject.org/projects/tor/query?status=accepted&status=assigned&status=needs_review&status=needs_revision&status=new&status=reopened&order=priority&col=id&col=summary&col=keywords&col=status&col=owner&col=type&col=priority&keywords=tbb-fingerprinting (accessed: 20.06.2018). (In Russ.).
16. Didenko S.M. [Investigation of the dynamics of the user's information handwriting model parameters]. *Vestnik Tjumenskogo gosudarstvennogo universiteta – Bulletin of the Tyumen State University*. 2006. vol. 5. pp. 170–174. (In Russ.).
17. Pilankar P.S., Padiya P. Multi-phase mouse dynamics authentication system using behavioural biometrics. International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES). 2016. pp. 1947–1950.
18. Hu S. et al. Deceive Mouse-Dynamics-Based Authentication Model via Movement Simulation. The 10th International Symposium on Computational Intelligence and Design (ISCID). 2017. vol. 1. pp. 482–485.
19. Chen X. et al. A practical real-time authentication system with Identity Tracking based on mouse dynamics. IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2014. pp. 121–122.

20. Kaminsky R., Enev M., Andersen E. Identifying Game Players with Mouse Biometrics. University of Washington. Technical Report. 2008. 12 p.
21. Feher C. et al. User Identity Verification via Mouse Dynamic**s**. *Information Sciences*. 2012. vol. 201. pp. 19–36.
22. Stanic M. Continuous user verification based on behavioral biometrics using mouse dynamics. The 35th International Conference on Information Technology Interfaces. 2013. pp. 251–256.
23. Identifikacija pol'zovatelej Tor Browser cherez analiz osobennostej raboty s mysh'ju. [The Tor Browser users identification through the analysis of the mouse features]. Available at: https://www.opennet.ru/opennews/art.shtml?num=44027 (accessed: 20.06.2018). (In Russ.).
24. Danilov N., Shulga T. [Constructing a heat map based on the point of the application user's activity]. *Prikladnaja informatika – Applied informatics*. 2015. vol. 2(56). pp. 49–58. (In Russ.).
25. Didenko S.M. [Development of the mathematical model of the user's information handwriting]. *Matematicheskoe i informacionnoe modelirovanie: sbornik nauchnyh trudov – Mathematical and information modelling: collection of scientific threads*. 2006. pp. 68–73. (In Russ.).
26. Shaptsev V.A., Didenko S.M. *Razrabotka i issledovanie komp'yuternoj modeli dinamiki sistemy «pol'zovatel'-mysh'»* [Development and research of the «user-mouse» system model]. Ph.D. thesis. 2007. 95 p. (In Russ.).

Iskhakov Andrey Yunusovich — Ph.D., senior researcher of cyber-physical, systems laboratory, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. Research interests: methods of information protection, theoretical foundations of computer security, identification and authentication systems development. The number of publications — 25. iskhakovandrey@gmail.com; 65, Profsoyuznaya str., Moscow, 117997, Russia; office phone: +7 495 336-71-05.

Iskhakova Anastasia Olegovna — Ph.D., senior researcher of cyber-physical, systems laboratory, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, junior researcher of Internet of Things Security laboratory of information systems security department, Tomsk State University of Control Systems and Radioelectronics (TUSUR). Research interests: methods of information protection, big data processing, artificial intelligence. The number of publications — 15. shumskaya.ao@gmail.com; 65, Profsoyuznaya str., Moscow, 117997, Russia; office phone: +7 495 336-71-05.

Meshcheryakov Roman Valerievich — Ph.D., Dr. Sci., professor, head of cyber-physical, systems laboratory, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. Research interests: system analysis, information processing, cyber-physical systems, information security. The number of publications — 240. mrv@ieee.org; 65, Profsoyuznaya str., Moscow, 117997, Russia; office phone: 7 495 336-71-05, Fax: +7 495 334-93-40.

Bendraou Reda — Ph.D., Dr. Sci., professor, Paris Nanterre University. Research interests: model driven engineering, meta-modeling, model transformations, model execution, DSL specification and code generation. The number of publications — 51. bendraou@mail.ru; 4, Place Jussieu, Paris, 75252, France; office phone: +33 1 44 27 88 6.

Melekhova Olga — Ph.D., associate professor, Paris Nanterre University. Research interests: autonomic systems. The number of publications — 33. melekhova.o@list.ru; 4, Place Jussieu, Paris, 75252, France; office phone: +33 1 44 27 88 6.

Acknowledgements. The work was partially supported by the Russian Federation President Grant for the Lead-ing Scientific Schools (grant NSh. 3070.2018.8) and the Russian Federation President Grant for the Young Russian Scientists – PhD (grant MK-6802.2018.8).

УДК 004.9 **DOI** 10.15622/sp.61.6

А.Ю. Исхаков, А.О. Исхакова, Р.В. Мещеряков, Р. Бендрау, О. Мелехова

ИСПОЛЬЗОВАНИЕ ТЕПЛОВОЙ КАРТЫ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ В ЗАДАЧЕ ИДЕНТИФИКАЦИИ СУБЪЕКТА ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Исхаков А.Ю., Исхакова А.О., Мещеряков Р.В., Бендрау Р., Мелехова О. **Использование тепловой карты поведения пользователя в задаче идентификации субъекта инцидента информационной безопасности.**

Аннотация. Одной из основных функций системы защиты информации является идентификация любого субъекта доступа с целью возможности расследования инцидентов информационной безопасности (ИБ). В ходе выполнения процедур сканирования и эксплуатации уязвимостей квалифицированные злоумышленники регулярно производят смену идентифицирующих признаков. Подобные действия не только обфусцируют данные в подсистемах аудита, затрудняя возможность восстановления хронологии событий эксперту ИБ, но и ставят под сомнение неопровержимость доказательной базы причастности конкретного злоумышленника к конкретным противоправным действиям. В статье приводится анализ применения современных подходов идентификации злоумышленников в веб-ресурсах, не требующих проведения аутентификации для основной пользовательской аудитории (методы fingerprinting, анализ поведенческих признаков). Рассмотрены признаки пользователя, которые могут быть использованы для решения задачи его последующей идентификации.

С использованием широко применяемых в задачах веб-аналитики «тепловых карт», адаптированного профиля пользователя и компьютерной модели динамики системы «пользователь-мышь» предлагается проводить идентификацию субъектов инцидента ИБ в общедоступных информационных ресурсах сети Интернет. Основная идея предполагаемого подхода заключается в том, что при построении тепловой карты должны учитываться не только плотность расположения данных, а также определяемые экспертом статистические параметры (дистанция градиента интенсивности, дистанция перекрытия и т.д.). Предлагается учитывать и динамику действий пользователя (например, вычисление среднего времени ввода данных в интерактивные элементы). Представлено подробное описание каждого шага соответствующей методики, а также информация по ее практической реализации. Робастность данного подхода подтверждается практическим экспериментом. Предложенная методика не является универсальным средством идентификации злоумышленника — во внимание принимаются только ручные таргетированные атаки, не учитывается использование злоумышленниками cURL инструментов и так далее. Поэтому рекомендуется использовать его исключительно в дополнение к действующим системам защиты (WAF, IPS, IDS).

Ключевые слова: идентификация, тепловые карты, fingerprinting, биометрия, анонимизация.

Исхаков Андрей Юнусович — к-т техн. наук, старший научный сотрудник лаборатории киберфизических систем, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук. Область научных интересов: методы защиты информации, теоретические основы компьютерной безопасности, развитие систем идентификации и аутентификации. Число научных публикаций — 25. iskhakovandrey@gmail.com; ул. Профсоюзная, 65, Москва, 117997; р.т.: +7 495 336-71-05.

Исхакова Анастасия Олеговна — к-т техн. наук, старший научный сотрудник лаборатории киберфизических систем, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук, младший научный сотрудник лаборатории безопасности интернета вещей кафедры безопасности информационных систем (БИС), Томский государственный университет систем управления и радиоэлектроники (ТУСУР). Область научных интересов: методы защиты информации, обработка больших данных, искусственный интеллект. Число научных публикаций — 15. shumskaya.ao@gmail.com; ул. Профсоюзная, 65, Москва, 117997; р.т.: +7 495 336-71-05.

Мещеряков Роман Валерьевич — д-р техн. наук, профессор, профессор РАН, заведующий лабораторией киберфизических систем, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук. Область научных интересов: системный анализ, анализ и синтез речи, информационная безопасность, обработка информации в интеллектуальных системах. Число научных публикаций — 240. mrv@ieee.org; Профсоюзная, 65, Москва, 117997; р.т.: 7 495 336-71-05, Факс: +7 495 334-93-40.

Бендрау Реда — д-р техн. наук, профессор, Университет Париж X – Нантер. Область научных интересов: моделирование, метамоделирование, преобразование моделей, исполнение моделей, спецификация DSL, генерация кода. Число научных публикаций — 51. bendraou@mail.ru; Площадь Юссие, 4, Париж, 75252; р.т.: +33 1 44 27 88 6.

Мелехова Ольга — доцент, Университет Париж X – Нантер. Область научных интересов: автономные системы. Число научных публикаций — 33. melekhova.o@list.ru; Площадь Юссие, 4, Париж, 75252; р.т.: +33 1 44 27 88 6.

Поддержка исследований. Работа выполнена при поддержке Министерства образования и науки Российской Федерации в рамках проектной части государственного задания на 2017–2019 гг. (проект № 2.3583.2017/4.6).

Литература

1. *Герасюкова М.* Цель захвачена: самые опасные хакерские атаки. Чем опасны целевые хакерские атаки и как от них защититься. URL: https://www.gazeta.ru/tech/2018/02/25/11659579/targeted_attack.shtml (дата обращения: 20.06.2018).
2. *Iskhakov S.Yu., Shelupanov A.A., Mescheryakov R.V.* Assessment of security systems complex networks security // Dynamics of Systems, Mechanisms and Machines (Dynamics). 2014. pp. 1–4.
3. *Yankovskaya A.E., Shelupanov A.A., Hodashinsky I.A., Gorbunov I.V.* Development of hybrid intelligent system of express-diagnostics for detection potential attacker // The 9th International Conference on Application of Information and Communication Technologies (AICT). 2015. pp. 183–187.
4. *Iskhakov A., Meshcheryakov R., Ekhlakov Yu.* The Internet of Things in the security industry // Interactive Systems: Problems of Human-Computer Interaction (collection of scientific papers). 2017. pp. 161–168.
5. *Ромашев А.* Тест и сравнение эффективности WAF (Web Application Firewall). URL: https://www.anti-malware.ru/compare/web-application-firewall#part4 (дата обращения: 20.06.2018).
6. *Iskhakov A., Meshcheryakov R., Iskhakov S., Krainov A.* Increase in security of authentication services through additional identification using optimal feature space

// Proceedings of the IV International research conference “Information technologies in Science, Management, Social sphere and Medicine” (ITSMSSM). 2017. pp. 443–446.

7. *Eckersley P.* How Unique Is Your Web Browser? // Proceedings of the 10th Privacy Enhancing Technologies Symposium (PETS). 2010. pp. 1–18.
8. *Alnaami K. et al.* P2V: Effective Website Fingerprinting Using Vector Space Representations // IEEE Symposium Series on Computational Intelligence. 2015. pp. 59–66.
9. *Iskhakova A., Meshcheryakov R.* Automatic search of the malicious messages in the internet of things systems on the example of an intelligent detection of the unnatural agents requests // International Conference on Information Science and Communications Technologies (ICISCT). 2017. pp. 1–4.
10. *Бессонова Е.Е., Зикратов И.А., Колесников Ю.Л., Росков В.Ю.* Способ идентификации пользователя в сети Интернет // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 3. С. 133–137.
11. *Usmonov B. et al.* The cybersecurity in development of IoT embedded technologies // International Conference on Information Science and Communications Technologies (ICISCT). 2017. pp. 1–5.
12. *Исхаков А.Ю., Исхаков С.Ю., Мещеряков Р.В.* Повышение защищенности сервисов аутентификации путем проведения дополнительной идентификации с использованием оптимального признакового пространства // Информационные технологии в науке, управлении, социальной сфере и медицине: сборник научных трудов. 2017. С. 117–122.
13. *Abouollo A., Almuhammadi S.* Detecting malicious user accounts using Canvas Fingerprint // The 8th International Conference on Information and Communication Systems (ICICS). 2017. pp. 358–361.
14. *Daud N.I., Haron G.R., Othman S.S.S.* Adaptive authentication: Implementing random canvas fingerprinting as user attributes factor // IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). 2017. pp. 152–156.
15. Система управления проектами Trac. URL: https://trac.torproject.org/projects/tor/query?status=accepted&status=assigned&status=needs_review&status=needs_revision&status=new&status=reopened&order=priority&col=id&col=summary&col=keywords&col=status&col=owner&col=type&col=priority&keywords=tbb-fingerprinting (дата обращения 20.06.2018).
16. *Диденко С.М.* Исследование модели динамики параметров информационного почерка пользователя // Вестник Тюменского государственного университета. 2006. № 5. С. 170–174.
17. *Pilankar P.S., Padiya P.* Multi-phase mouse dynamics authentication system using behavioural biometrics // International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES). 2016. pp. 1947–1950.
18. *Hu S. et al.* Deceive Mouse-Dynamics-Based Authentication Model via Movement Simulation // The 10th International Symposium on Computational Intelligence and Design (ISCID). 2017. vol. 1. pp. 482–485.
19. *Chen X. et al.* A practical real-time authentication system with Identity Tracking based on mouse dynamics // IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2014. pp. 121–122.
20. *Kaminsky R., Enev M., Andersen E.* Identifying Game Players with Mouse Biometrics // University of Washington. Technical Report. 2008. 12 p.
21. *Feher C. et al.* User Identity Verification via Mouse Dynamics // Information Sciences. 2012. vol. 201. pp. 19–36.

22. *Stanić M.* Continuous user verification based on behavioral biometrics using mouse dynamics // Proceedings of the ITI 2013 35th International Conference on Information Technology Interfaces. 2013. pp. 251–256.
23. Идентификация пользователей Tor Browser через анализ особенностей работы с мышью. URL: https://www.opennet.ru/opennews/art.shtml?num=44027 (дата обращения: 20.06.2018).
24. *Данилов Н.А., Шульга Т.Э.* Построение тепловой карты на основе точечных данных об активности пользователя приложения // Прикладная информатика. 2015. № 2(56). С. 49–58.
25. *Диденко С.М.* Развитие математической модели информационного почерка пользователя // Математическое и информационное моделирование: сборник научных трудов. 2006. С. 68–73.
26. *Шапцев В.А., Диденко С.М.* Разработка и исследование компьютерной модели динамики системы «пользователь-мышь» // Диссертация на соискание степени кандидата технических наук. 2007. 95 с.