On Keystroke Pattern Variability in Virtual Desktop Infrastructure

Ievgeniia Kuzminykh[a,b], Bogdan Ghita[c] and Alexandr Silonosov[d]

[a] *King's College London, WC2R 2ND, UK; ievgeniia.kuzminykh@kcl.ac.uk*
[b] *Kharkiv National University of Radio Electronics, Kharkov, 61000, Ukraine*
[c] *University of Plymouth, PL4 8AA, UK*
[d] *Blekinge Institute of Technology, Karlskrona, SE-371 79 Sweden*

Abstract

The paper investigates the impact of network traffic and network characteristics on the effectiveness of keystroke dynamics for continuous and one-time authentication in the remote desktop applications and virtual desktop infrastructure. The context presented in the paper contributes to the area of biometric authentication systems by identifying virtual desktop environment as a specific application domain that uses a keystroke pattern for user verification and identifying at what extent the context influences on permanence and the immunity of the keystroke data which was never studied before. The results showed that the keystroke pattern is not affected by network latency, but standard deviation, jitter, and packet loss have a significant combined impact onto it. It can also be concluded that RDP packets are not prioritized during transmission over the network, and therefore, we can say that any other competing traffic is likely to render keystroke dynamics unusable for continuous authentication during remote access.

Keywords

Biometric pattern, continuous authentication, Euclidean distance, keystroke dynamics, remote display protocol, RDP

1. Introduction

Information Security represents a key factor to support the critical information infrastructures across all business sectors. While password-based access control of encompassing systems remains the de-facto option for protecting such systems, previous research demonstrated that such an approach is insufficient; in addition, many examples of successful attacks, including fishing, identity theft, brute force, coupled with weak password policies confirmed the inherent weakness of password-based authentication. In order to overcome this weakness and enhance the authentication process, the industry regulators recommend the adoption of Multi Factor Authentication (MFA). On an MFA-based access system, the user is authenticated using two or more methods that combine knowledge-, token-, or biometric-based inputs. While the first two options have been extensively enhanced through security education and respectively hardware hardening, the biometric alternatives are still subject to significant research due to the complexity and variability of the inputs. The two main classes of biometric inputs are physiological (retina, face, fingerprint, or eye scan) and behavioral (gait, voice, signature, typed keystrokes or mouse movements dynamics). Unlike the other options, biometric authentication requires no additional hardware or memorizing of complex patterns, which makes it the preferred choice for additional security provisioning. From an accuracy perspective, physiological authentication is indeed the better option but, given its inherent intrusiveness for sample acquisition makes it less attractive for users. In contrast, behavioral authentication is subject to variability and therefore typically leads to poorer accuracy, but it is ideal for continuous authentication and, as it draws data from the system interaction, it also has a higher user acceptance.

CMIS-2021: The Fourth International Workshop on Computer Modeling and Intelligent Systems, April 27, 2021, Zaporizhzhia, Ukraine
EMAIL: yevheniia.kuzminykh@nure.ua (Ie. Kuzminykh); bogdan.ghita@plymouth.ac.uk (B. Ghita); asilonos@gmail.com (A. Silonosov)
ORCID: 0000-0001-6917-4234 (Ie. Kuzminykh); 0000-0002-1788-547X (B. Ghita)


Given the level and variability of system and applications, the most common interaction option and user data input remains text typing. From an MFA perspective, keystroke dynamics would be the implicit option for continuous authentication, in spite of its inherent variability and attrition, as user behavior may change over time and depends on age, therefore requiring frequent updates of the associated biometric user template.

Biometric authentication has been a highly popular area of research over the past decade; a number of studies demonstrated that keystroke dynamics provides a unique discriminator for individual users through a number of two defining features and their related variables: the duration of a button press and release and the delay between next button press depending on the distance between buttons on a keyboard.

From the intrusiveness perspective, there are two types of user input when performing keystroke dynamics: fixed- and free-text. In the fixed-text authentication, a user needs to type a predefined phrase in order to have their biometric characteristics collected and evaluated, and subsequently be allowed to access system. In free-text authentication, the user may type any text, including command keys, hotkeys, arrows, which makes the method ideal for continuous authentication (CA), to be run in the background, while the user is interacting with the system. Recent studies propose a hybrid approach for improving Free-text approach by using a subset of typed text as input for analysis. Free-text authentication is considered as supplemental security control since it helps to identify the change of legitimate user, particularly when an open session or an unlocked desktop are being intercepted by an intruder. Free-text authentication is reliable since it is hard to forge it. An attacker needs to have access to computer and availability to capture user behavior for a long period to collect data. In this context, one of the factors that further affects the user behavior for a free-text keystroke template is the computer input device, due to its layout and mechanical characteristics. As a result, keystroke biometrics accuracy is affected when collected from different devices and therefore it is preferred in scenarios where the user is regularly performing data input on the same computer, in areas such as healthcare or finance.

Prior studies exhaustively evaluated the strength of keystroke dynamics authentication and proposed a number of improvements focusing on the free-text authentication methods. Given the de-facto description of computer systems, research focused exclusively on system-based, local authentication, while the impact of remote interaction on free-text authentication has not been considered. In this study, we investigate how the variability of network characteristics, delay in particular, influence the calculation of user biometric keystroke dynamics patterns. We will perform an experiment using the most commonly used remote display protocol Microsoft RDP to determine how changes in the network load and resulting congestion influence the keystroke dynamics pattern, in particular, the Euclidean distance value.

Following this introduction, section 2 of the paper provides a brief overview of research on keystroke dynamics authentication system and protocols. Section 3 outlines the methodology for data acquisition and processing. Section 4 provides a comparative analysis and comparison of the results, to benchmark the actual impact of network path changes on the resulting biometric profile. Based on this evaluation, Section 5 draws a discussion and further opportunities for research and Section 6 concludes the paper.

2. Literature review

Review of state-of-the-art in network protocols that implements remote display or so called thin client functionality shows that network latency is one of the key factor characteristic that affects remote display performance. Simoens provided in [1] an in-depth analysis of network latency and its impact of user input events. In [2], the authors show that high network latency affects temporal characteristics of the provided service and thus human perception. Long and Gutwin in their study [3] covers temporal aspect of user input actions in network context and differentiate between local lag versus network lag, which is also exist.

As can be inferred from their required functionality, one of the main performance indicators of remote display infrastructure is their ability to transmit commands and render the screen in a near-real-time fashion; as a result, low latency is critical to their success. A number of studies [4, 5]

benchmarked how network latency impacts on the perceived performance in multiplayer Internet games, more specifically how delays in interaction affect the movement, location, and actions of a player.

Another subject of our research is biometric pattern based on the user keystroke dynamics. In this area slightly more works but any work related to the application of the keystroke for remote access.

In [6] authors acquired keystroke types of the users, built biometric template called enrolment vector, and then tested five matching methods presented by different researchers by comparing enrolment vector with test vector. Experiment included only password typing template, the position of the keys on the keyboard was not taking into account as well as any network or environmental conditions. All results were obtained only by manipulation of the datasets that were collected from users who typed several times password for experiment.

Miguel Lizarraga in [7] collected keystroke dynamics from set of the users, created template for each user and then tested similarity of template and sample. The method of verification of the similarity is developed by authors and based on mean and standard deviation of each feature. The features extracted were three time-features of pressed keys (down-down, down-up, and up-down times). They tested the efficiency of the verification algorithm for different situations: when user is legitimate and when user is impostor.

In this work [8] the timing values from 10 users for typing of the password/username pair were collected and presented. The users should login with the same credentials. The flight and hold time for each user were analysed and showed the difference of the user's biometric behaviour, some users typed text faster, some slower. The further analysis of the obtained data with timing characteristics was not provided.

In [9] the authors investigated the feasibility of using keystrokes for creating cryptography key for files stored remotely in the cloud as alternative to the algorithmic key generation. The key based on the biometry provides both authentication and integrity of data. The work showed the reliability of creating a 256-bit key with biometric pattern. The results showed very low FAR parameter for keystroke-based cryptography key.

Another work devoted to the authentication in the cloud [10] uses keystroke activity as one of the input parameters for creating user template align with other host-based characteristic and network flow-based features. Totally, authors used 36 features to form user profile. But only two features were used to describe keystroke activity of the user: the key press-down time and the time interval between two pressed keys.

Gunetti et.al. [11] and Monrose et.al. [12] analysed non-static biometric technique based on user free-text typing dynamics. It is an attempt to consider using of keystroke dynamics for continuous authentication. The user's typing profiles were obtained using of digraph-specific measures, and in [11] Imposter Pass Rate (IPR) and False Alarm Rates (FAR) have been calculated. This technique provides useful information for user identification and authentication even when a long time has passed since user profiles were formed.

In [13] the authors conducted static manipulation with the dataset of collected keystroke dynamics. The time related features were extracted from the dataset, VKF is calculated based on the typing speed. Using Genetic Algorithm and Support Vector Machines (SVM) algorithms the feature subset selection was done from the reduced. Feature reduction rate and FAR were calculated using the MATLAB.

Bajaj et.al. [14] and Yvonne J. et.al. [15] used timing characteristics of the keystroke as pressing time, dwell time and total time of password entering. Then statistical method is used to calculate the mean time. If value is above the threshold value, then access can be grated, otherwise access is denied. In both papers the users were required to enter only password for collecting biometric pattern.

Literature review shows that only few works analysed free-text keystroke dynamics, and there are no studies researching how characteristics of virtual desktop infrastructures affects free-text based authentication. Moreover, most of the researchers used extraction of timing information from the raw data for forming user profile, but some researchers rely only on two parameters, some use 3-4 timing parameters to describe keystroke activity of the user. Only one work proposes using additional parameter of key location on the keyboard for user profile that we will use in our research. The use of four timing features with adjacency class for keys to authenticate users is novel. Therefore, we conduct an experiment to investigate the impact of network and host characteristics on the user

biometric profile based on keystroke dynamics and to derive the threshold for delay variation beyond which the underlying behavioural biometric algorithms become ineffective.

3. Methodology

Null hypothesis is that network latency has no effect on consistency of behaviour pattern that is calculated based on keystroke dynamics of user input. The first part of the methodology is to develop input rendering engine for thin client, then implement algorithms to calculate biometric pattern from real input keystroke dynamics in a VDI session, and then calculate distance for user reference and current biometric pattern. Current biometric pattern will be obtained under different network environmental conditions.

Thin client as part of VDI will capture input events from locally attached keyboard, transfer them to remote desktop over a network protocols such TCP/IP and then replay or render input events on a remote display to simulate, user input. The infrastructure of the remote session is showed in Figure 1.

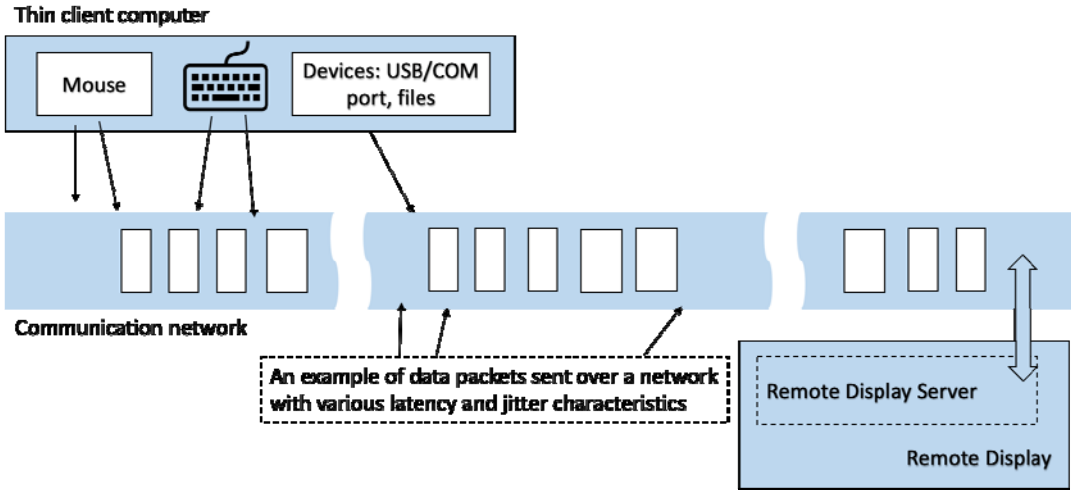

Figure 1: Typed keystrokes, mouse clicks and devices data are sent to Remote Display in a raw format in different TCP packets. Screen image and sound are sent back to thin client

We need to experiment with network protocol, network load, running processes on the remote host and biometric pattern which is calculated from keystroke dynamics by an algorithm. The objective is to study how network and host characteristics affect the keystroke dynamics user pattern.

3.1. Network generator

For the purpose of experimenting with network load the review of current state-of-art techniques to generate network workload and measure network performance in VDI scenario has been made. Using literature review four methods of network workload generation were identified and presented in Table 1. The table reflects main characteristics of network simulation and tools that were used for traffic generation. Most of the papers run experiments in testbed that includes network environment close to VDI, where client computer accesses a service or data on a server via heterogeneous network. The results showed that the network latency is the most popular parameter for network simulation experiments, and many researchers [18, 20, 22] used D-ITG software to simulate controlled network traffic. Several research [19,22] used OpenFlow protocol to retrieve network latency and loss rate from network equipment. We will use D-ITG tool as traffic generator in our experiment.

3.2. Dataset

The subject is represented by a dataset on natural human-computer interaction [11] that includes keystrokes dynamics of 39 users and three typing patterns of each user resulting into a total of 122 typed keystrokes to be used as input data for creating user profile. This reference profile will be compared with current user profile that is captured under different network and host performance. The dataset contains keystroke-timing information from three different passwords, free-text questions (500 chars) and the transcript of Steve Jobs' Commencement Speech split into two parts. Each user performed the typing test in two separate laboratory sessions, with each session taking about one hour and containing approximately ten thousand keystrokes.

Table 1
Research on using the traffic generator tools

Ref	Latency	Workload	Speed, Mbs	Delay, ms	Packet loss, %	VDI	Year
[17]	DiffProbe	DiffProbe	1-100	-	0.15-1.68	Y	2010
[18]	D-ITG	D-ITG	1	1	1	Y	2012
[19]	OpenFlow	OpenFlow OpenNet-Mon, NetEm	100	10-20	1	Y	2014
[20]	Yaz	D-ITG	7	300-1000	n/a	N	2018
[21]	NorNet	Netem, D-ITG	10-20	25-400	1-5	N	2018
[22]	OpenFlow	D-ITG	30	5-100	n/a	N	2018
[23]	Emulab	D-ITG	4	30	1	N	2019

3.3. Feature Extraction

In order to verify the impact of external impairments on the effectiveness of keystroke authentication, we selected a recognised, successful method and applied it to both the raw initial dataset and the new dataset, based on the received keystroke events. We followed the studies [7,16] and used digraph latency for feature extraction. Features were computed for each key-pair using two main values, specifically the press time (P) and the release time (R) of each key in milliseconds. Four keystroke features were extracted from each key-pair for each user as shown in Figure 2:

1. *Press-Release Time:* Hold time for a key that define the time the key remains pressed.
2. *Press-Press Time:* Time interval between pressing two successive keys.
3. *Release-Release Time:* The interval between releasing two successive keys.
4. *Release-Press Time:* The interval between releasing and pressing two successive keys. This value could be positive or negative according to when keystroke was pressed, before or after previous key was released. That is why we will use absolute value of this feature.

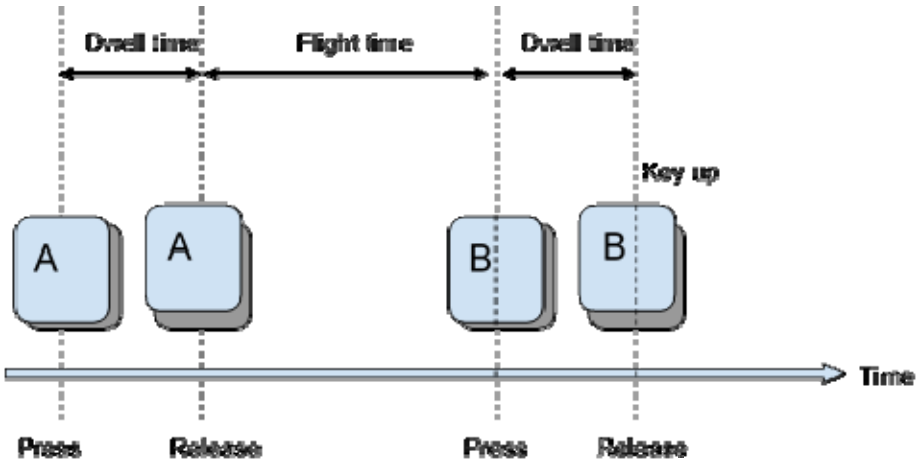

Figure 2: Timing features for the key pair

It is apparent only three of the four parameters are independent but, given there was no post-processing applied to the data, the full set of four was maintained for completeness.

Before feature extraction, the dataset was ordered by grouping records from dataset according to the keystroke value ci that first pressed and then released. The adjacency class was introduced as an input to set the level of adjacency between two keys on the keyboard and allows to decrease the deviation of the time values during feature extraction. Each row was labelled by the class parameter that corresponds to one of the five adjacency classes and related to key-pair. This ordered dataset was used for the extraction of the timing features, and the reference profile of a user is created for a particular typing session, consisting of mean time characteristics for 121 digraphs (corresponds to 122 characters).

The difference in the assessment of the two profiles, the reference profile P_{ref} and current P_t is defined in Equation (1) and could be measured using different classification algorithms as statistical algorithms and machine learning algorithms [11, 16, 24-27]. Few of the common statistical measures are k-nearest neighbour, Euclidean distance, Manhattan distance, Mahalanobis distance, Bayesian distance, statistical t-test, and degree of disorder. Among ML algorithms the common algorithms include Neural Networks, SVM, Regression, Decision Tree, Random Forest, KNN, K-Means, Naive Bayes.

$$distance = |P_{ref} - P_t| / P_{ref} \quad (1)$$

There are two approaches to calculate distance with several features for the authentication purpose. First way is to calculate distance for summative vector with all features that corresponds to the user profile, another way is to calculate distance value for each feature separately. The determination of the threshold is an important issue in the methodology. The analysis of the real collected keystroke data needs to be done to determine thresholds. The works [7, 16] showed that a user's feature with a higher variation demands a lower threshold, while a feature with a lower variation demands a higher threshold. So, the threshold for each feature in each account is obtained based on its standard deviation. Decision about an optimal threshold for each feature based on the a priori knowledge of authentication system administrator and usually the task of determination of the threshold is simple linear function maxima problem. In our work we do not consider decision-making part of the matching phase, the user's identification and authentication is out of scope. We only used an Euclidean distance value as indicator for changes that happened with keystroke pattern under certain conditions with variety of network and host characteristics.

3.4. Experiment setup

For the experiment, a network consisting of two routers, two switches and the client and server side was constructed. On the client side:

- Keystroke dynamic was simulated according to one of the profiles
- Remote access to the system was initiated using one of the RD protocols.

Remote server software was installed on the server side, the pattern recognition algorithms program was launched and the received data was compared with the user reference model that was obtained in advance and stored on the server.

The network latency was simulated between the client and the server using the D-ITG traffic generator simulator. We can control and change this variable of latency during an experiment by changing parameter C (intensity of traffic, packets/sec) and c (packet size, bytes) in D-ITG. Since keystroke dynamics is transferred over the network then changing of traffic delays will predetermine the temporal characteristics of the keystroke dynamics and as a result will affect a pattern. The dependent variable is a biometric pattern.

Three types of the experiment were conducted performing the efficiency of keystroke dynamics:

- Under increasing network latency
- During transmission the files from remote desktop to the host
- During watching the video on the remote desktop.

In the first experiment, the transmission channel was loaded with UDP traffic, which was generated using D-ITG, there were two streams of the same intensity, the channel capacity was reduced to 1mbps to obtain high delays in early iterations. To fix the behaviour of the system in the normal state, baseline for the network of characteristics was measured in the absence of load. Further, the network load increased due to an increase in the -C parameter in D-ITG until the packet loss began to exceed 1%.

In the second experiment, the communication channel was not loaded with generated traffic, but the keystroke data prompted for authentication was accompanied by copying the file from remote desktop to the client machine.

In the third experiment, the biometrics authentication process was accompanied by watching a fullHD video on the youtube channel on remote desktop.

4. Results

Process of the performing continuous authentication based on the keystroke dynamics was implemented under different conditions. The difference between reference biometric user profile and current obtained during experiment was estimated by its distance value that shows similarity of two patterns, and summary is showed in the Table 1.

Table 1
Results of the experiment

Experiment	1	2	3	4	5	6	7
C parameter D-ITG [pkts/s	0	10..100	110	110,	115		
Additional actions				Mouse moves on RDP window		Copying file	Watching video
Av. Euclidean distance	1.068	1.07	1.074	1.77	3.2	2.12	3
Av. packet loss, %	0	0	0	0.14	3.6	n/a	n/a
Av.delay, ms	<1	<10	10.5	64	370	n/a	n/a

As shown by the first three experiments, the impact of low or medium congestion is minimal on the resulting keystroke dynamics parameters, as the Euclidian distance of experiments 2 and 3 is comparable to the baseline obtained in experiment 1. In the case of experiment 3, the measured average bitrate was 901 kb/s, which is close to the bottleneck bandwidth for the testbed, still with minimal impact on the Euclidian distance between the original vector and the one collected at the RDP server. Although the channel utilisation was rather high, there was no packet loss recorded and the average delay (10.5ms) and jitter (3.2ms) were also low. In order to see the behaviour of the

channel under heavy congestion, the data flows were further increased to an average bitrate of 916kb/s, leading to a bottleneck link utilisation of 91.7% and subsequently increasing the average delay (370ms); given the additional traffic was CBR, the jitter varied only slightly, increasing to 3.7ms.

The last three experiments involved a combination of RDP-based interaction, RDP-based traffic, and bandwidth limitations. Experiment 5 was similar to the original conditions, running through a limited 1Mbps bandwidth, but included additional activity on the remote display, more specifically random fast window movements for an open application. This affected slightly the average delay, increasing it to 64 ms, but had a slightly more significant impact on jitter (7ms) and packet loss, which increased to 0.14%. While none of the individual parameters increased significantly, the resulting Euclidian distance varied by a significant factor of 1.77. Experiments 6 and 7 also investigated the impact of additional RDP activities onto the keystroke timings but using a non-restricted 100Mbps link. For experiment 6, a text file was transmitted from the remote machine to the client machine via RDP, while experiment 7 generated additional traffic by streaming a video from the remote machine to the thin client. The video chosen for experiment 7 was an HD 1080p video, with bitrate varying between 4000-8000kbps; while this is indeed the bitrate between the YouTube server and the RDP server, optimised for the bandwidth between the two endpoints, not the same can be said about the link between the RDP server and the client, which uses non-optimised video communication between the them. As a result, it is likely that the down-streaming from the server to the client is higher in terms of bitrate.

5. Discussion

The results showed that increasing the channel load with UDP traffic to a certain level does not affect the biometric pattern. This could be explained by the fact that UDP traffic is non-bursty, smooth, and the standard deviation and jitter values are relatively small [28, 29]. But when the channel utilization goes beyond 0.9 (as it is the case for experiments 3-5) the throttling algorithm is starting to work causing a packet loss. This affects the keystroke pattern and the similarity coefficient changes from 1 to 1.7 even with small packet loss values of 0.15-0.5%.

The keystroke dynamics pattern is also affected by the value of standard deviation and jitter, as demonstrated where the transmission of RDP keyboard events is concurrent with events from the VDI. In this case, the average delay was within normal limits but the deviation in delay values was almost two times greater (100 msec). From this, we can conclude that such an effect will be caused by applications running on TCP, since TCP traffic is characterized as bursty, greedy, and is more resistant to delays, but has large jitter values due to its nature [30,31].

When the network load approaches bandwidth the network latency increases to an unacceptable 370msec (ITU-T recommendation for UDP traffic network latency is less than 150ms) and packet loss occurs. This leads to a modification of the timing information required for user current biometric pattern, as a result, the similarity coefficient has a very large distance value which means that the user is most likely not to be identified.

Additional actions such as copying and watching videos on the remote display also significantly affect the keystroke pattern which means that biometrics dynamics are transmitted with the same priority as the rest of the traffic and are served in a queue. From this we can conclude that continuous authentication will be not effective in this situation.

Not prioritizing of RDP messages that carry biometric information can be explained by the fact related to the functioning/processing of keyboard events. Keyboard messages often have a low priority over other operations such as file management [32]. This is evident when typing in a word processor. If there is any disk activity when typing, the text being written is held in a buffer until such time that the processor is free to deal with it (causing the display to pause and then the 7 characters appearing). In order to achieve the high accuracy of timing between keystrokes, the keyboard driver and timing device need a high priority in order not to be affected by other activities.

6. Conclusion

This paper presents assessment of the applicability of keystroke dynamics for continuous and one-time authentication in the remote desktop applications and VDI. The combination of four features (Press-Release, PP, RR, RP times) were collected to form a user profile that was object of the experiments. This profile was compared with the current user profiles obtained during experiments under increasing network latency, during transmission the files from remote desktop to the host and during watching the video on the remote desktop. The similarity of two profiles was assessed using Euclidean distance.

We found that the pattern is not affected by network latency that approved our null hypothesis; but by the values of its standard deviation, jitter, and packet loss. This means that working with applications that require TCP transmission on the remote desktop will have a greater effect on the pattern than UDP based ones. It can also be concluded that data transmitted via RDP is not priority traffic which means that as of today, it is impossible to use keystroke dynamic based pattern for continuous authentication for remote access. For one-time authentication at the beginning of the session it is possible to use keystroke pattern when there is no other running application or open windows that can affect the pattern.

But for future, that needs to be reconsidered and modified the RDP protocol in order to take into account the prioritizing of the traffic that is necessary for transmission of biometric information. It is very important in the situation we are faced now, during coronavirus, caused social isolation and needs to work remotely. The biometric identification and authentication based on the keystroke dynamics could be great solution for control the remote access.

7. References

[1] P. Simoens, B. Vankeirsbilck, L. Deboosere, F. A. Ali, F. D. Turck, B. Dhoedt, and P. Demeester, Upstream bandwidth optimization of thin client protocols through latency-aware adaptive user event buffering, Int. J. Communication Systems 24 (2011): 666–690.

[2] Md Liakat Ali, John V Monaco, Charles C Tappert, and Meikang Qiu, Keystroke biometric systems for user authentication, Journal of Signal Processing Systems, 86(2-3):175–190, 2017

[3] M. Long and C. Gutwin, Characterizing and modeling the effects of local latency on game performance and experience, in: Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play, 2018, pp. 285–297.

[4] D. Stuckel, C. Gutwin, The effects of local lag on tightly-coupled interaction in distributed groupware, in: Proceedings of ACM conference on Computer, CSCW '08, 2008, pp. 447–456.

[5] K. Almeroth, J. Nelson, On the impact of delay on real-time multiplayer games, in: Proceedings of 12th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV'02), 2002, pp. 23-29.

[6] R. Giot, M. El-Abed and C. Rosenberger, Keystroke dynamics authentication for collaborative systems, in Proceedings of 2009 International Symposium on Collaborative Technologies and Systems, 2009, pp. 172-179.

[7] Livia C. F. Araújo, Luiz H. R. Sucupira Jr., Miguel G. Lizárraga, Lee L. Ling, Andjoão B. T. Yabu-Uti, “User Authentication Through Typing Biometrics Features," IEEE Transactions on Signal Processing 53(2) (2005): 851-855.

[8] P. V. Pawar, Static User Authentication through Typing Behavior, International Journal of Latest Trends in Engineering and Technology 4(1) (2014): 144-148.

[9] L. Abed, N. Clarke, B. Ghita, A. Alruban, Securing Cloud Storage by Transparent Biometric Cryptography, in: J.L. Lanet, C. Toma (Eds.), Innovative Security Solutions for Information Technology and Communications, volume 11359 of LNCS, Springer, Cham, 2018, pp.97-108. doi: 10.1007/978-3-030-12942-2_9.

[10] W. Liu, A. S. Uluagac and R. Beyah, MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data, in Proceedings of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2014, pp. 518-523.

[11] D. Gunetti, C. Picardi, and G. Ruffo, Keystroke Analysis of Different Languages: A Case Study, in: A.F. Famili, J.N. Kok, J.M. Peña, A. Siebes, A. Feelders (Eds.), Advances in Intelligent Data Analysis, volume 3646 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2005, pp. 133-144. doi:10.1007/11552253_13.
[12] F. Monrose, A. Rubin, Keystroke dynamics as a biometric for authentication, Future Generation Computer Systems 16 (2000): 351-359.
[13] K. Senathipathi, K. Batri, Keystroke Dynamics Based on Human Authentication System using Genetic Algorithm, European Journal of Scientific Research 82(3) (2012): 446-459.
[14] S. Bajaj, S. Kaur, Typing Speed Analysis of Human for Password Protection (Based on Keystrokes Dynamics), International Journal of Innovative Technology and Exploring Engineering 3 (2) (2013): 88-91.
[15] Y.J. Stark, M.R. Kellas-Dicks. Incorporating False Reject Data into Templates for User Authentication. US Patent US8533486B1, 2013.
[16] A. Alsultan, K. Warwick, H. Wei, Improving the Performance of Free-text Keystroke Dynamics Authentication by Fusion, Applied Soft Computing, 70 (2018): 1024-1033.
[17] K. Partha, and C. Dovrolis, Diffprobe: detecting ISP service discrimination, in: Proceedings of IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 1-9, doi: 10.1109/INFCOM.2010.5461983.
[18] A. Botta, A. Dainotti, A. Pescapè, A tool for the generation of realistic network workload for emerging networking scenarios, Computer Networks (Elsevier) 56 (15) (2012): 3531-3547.
[19] N. L. M. van Adrichem, C. Doerr and F. A. Kuipers, Opennetmon: Network monitoring in openflow software-defined networks, in IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 2014, pp. 1-8, doi: 10.1109/NOMS.2014.6838228.
[20] G. Aceto, F. Palumbo, V. Persico and A. Pescape, Available Bandwidth vs. Achievable Throughput Measurements in 4G Mobile Networks, in: 14th International Conference on Network and Service Management (CNSM), Rome, Italy, 2018, pp. 125-133.
[21] S. Ferlin, S. Kucera, H. Claussen and Ö. Alay, MPTCP Meets FEC: Supporting Latency-Sensitive Applications Over Heterogeneous Networks, IEEE/ACM Transactions on Networking, 26 (5) (2018): 2005-2018, doi: 10.1109/TNET.2018.2864192.
[22] H. Tahaei, R. B. Salleh, M. F. Ab Razak, K. Ko and N. B. Anuar, "Cost effective network flow measurement for software defined networks: A distributed controller scenario." IEEE Access 6 (2018): 5182-5198.
[23] V. Vu Anh, and B. Walker, Redundant Multipath-TCP Scheduling with Desired Packet Latency, in: Proceedings of the 14th Workshop on Challenged Networks, Oct 2019, pp. 7-19.
[24] P. Kang, S. Cho, Keystroke dynamics-based user authentication using long and free text strings from various input devices, Inf. Sci., 308 (2015): 72-93.
[25] J. Huang, D. Hou, S. Schuckers, T. Law and A. Sherwin, Benchmarking keystroke authentication algorithms, in: IEEE Workshop on Information Forensics and Security (WIFS), Rennes, France, 2017, pp. 1-6, doi: 10.1109/WIFS.2017.8267670.
[26] A. Carlsson, I. Kuzminykh, R. Franksson, A. Liljegren, Measuring a LoRa Network: Performance, Possibilities and Limitations, in: O.Galinina, S.Andreev, S. Balandin, Y. Koucheryavy (Eds.), Internet of Things, Smart Spaces, and Next Generation Networks and Systems, volume 11118 of LNCS, Springer, Cham, 2018.
[27] I. Kuzminykh, D. Shevchuk, S.Shiaeles, B. Ghita, Audio Interval Retrieval Using Convolutional Neural Networks. In: O. Galinina, S. Andreev, S. Balandin, Y. Koucheryavy (Eds.), Internet of Things, Smart Spaces, and Next Generation Networks and Systems, NEW2AN 2020, ruSMART 2020, volume 12525 of LNCS, Springer, Cham, 2020.
[28] T. Bakhshi and B. Ghita, Traffic Profiling: Evaluating Stability in Multi-device User Environments, in: Proccedings of 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Crans-Montana, Switzerland, 2016, pp. 731-736, doi: 10.1109/WAINA.2016.8.

[29] T. Lebedenko, M. Ievdokymenko, A.S. Ali, Research of Influence Flow Characteristics to Network Routers Queues Utilization, in: Proceedings of 1st International Conference Advanced Information and Communication Technologies, Lviv, Ukraine, 2016, pp.111-112.
[30] H.Oudah, B.Ghita, T. Bakhshi, A Novel Features Set for Internet Traffic Classification using Burstiness, in: Proceedings of the 5th International Conference on Information Systems Security and Privacy, Prague, Czech Republic, 2019, pp. 397-404, doi:10.5220/0007384203970404.
[31] I. Kuzminykh, B. Ghita, A. Silonosov, Impact of Network and Host Characteristics on the Keystroke Pattern in Remote Desktop Sessions, arXiv preprint arXiv:2012.03577, 2020.
[32] R. Shorrock, D. J. Atkinson, S. S. Dlay, Biometric verification of computer users with probabilistic and cascade forward neural networks, URL: https://pdfs.semanticscholar.org/9825/90e785721f5dae5e53183b97c028a996544e.pdf.