AUTENTIFICARE SECURIZATĂ FOLOSIND METODE BIOMETRICE - STUDIU DE CAZ TypingDNA

Antonio COHAL antonio.cohal@rotld.ro

Carmen ROTUNĂ carmen.rotuna@rotld.ro

Institutul Național de Cercetare-Dezvoltare în Informatică - ICI Bucureşti

Rezumat: În ultimii ani, securitatea internetului şi a comunicațiilor electronice reprezintă factori cheie pentru economie şi pentru societate în general, întrucât observăm o creştere a numărului de incidente majore în materie de securitate cibernetică, datorată unor factori variați. Incidentele de securitate pot afecta utilizatorii individuali, organizațiile, operatorii economici, guvernele şi societatea în general. Un număr foarte mare de incidente sunt cauzate de utilizarea parolelor slabe, furate sau implicite. Această lucrare oferă o perspectivă asupra metodelor puternice de autentificare, cum ar fi autentificarea folosind metode biometrice precum Keystroke Dynamics sau TypingDNA. Implementarea metodelor biometrice a devenit din ce în ce mai folosită în ultimul timp, grație beneficiilor interacțiunii utilizatorilor. TypingDNA este un nou model de autentificare prin recunoaşterea utilizatorului pe baza unui text tastat anterior. În acest fel, dacă se pierde o parolă, recuperarea se va face prin recunoaşterea utilizatorului în mod automat de către aplicație, bazat pe modul de scriere a textului dat. Prin urmare, scopul acestei cercetări este de a oferi părților interesate, dezvoltatorilor de software şi organizațiilor, o analiză comparativă a unor tehnici de autentificare cu un grad ridicat de securitate.

Cuvinte cheie: autentificare, metode biometrice, Keystroke Dynamics, TypingDNA, autentificare securizată, securitate cibernetică.

Abstract: In recent years secure internet and electronic communications are key drivers to economy and society in general as we can notice an increase in the number of major cyber security incidents due to various factors. Security incidents can affect individual users, organizations, economic operators, governments and society in general. An overwhelming number of incidents are caused by leveraging weak, stolen or default passwords. This paper provides an insight on strong authentication methods such as biometric authentication methods like Keystroke Dynamics or TypingDNA. Implementation of typing biometrics has become increasingly used lately, due to the benefits of user interaction. TypingDNA is a new authentication model by recognizing the user based on a previously written text. In this way, if a password is lost the recovery will be done by recognizing the user based on of text writing mode automatically by the application, the user only having to write a provided text. Therefore, the purpose of this research is to provide stakeholders (software developers and organizations) a comparative analysis of authentication techniques with a high degree of security.

Keywords: authentication, biometric methods, Keystroke Dynamics TypingDNA, secure authentication, cyber security.

1. Introducere

În contextul creşterii exponențiale a atacurilor cibernetice este evidentă necesitatea utilizării unor noi mecanisme pentru creşterea nivelului de securitate la nivel de aplicație. Un studiu realizat de compania de cercetare Gartner arată că 95% din atacurile aplicațiilor Web fac uz de parole furate. [13]

În iunie 2012, parolele SHA-1 a 6,5 milioane de utilizatori, utilizate pe o rețea de socializare de mari dimensiuni, au fost dezvăluite pe forumuri publice de hackeri. Impactul atacului nu este pe deplin cunoscut, dar milioane de utilizatori au fost îndemnați să îşi schimbe parolele, întrucât datele lor personale puteau fi în pericol [14].

Parolele devin din ce în ce mai puțin fiabile în protejarea datelor şi a identităților utilizatorilor, gestionarea, protecția şi memorarea lor devin din ce în ce mai problematice, iar persoanele neautorizate au nenumărate modalități de a le fura sau compromite.

Mecanismele de autentificare multi-factor au fost de mult cunoscute ca o soluție, dar datorită complexității în implementare şi costurilor ridicate, acestea nu sunt încă utilizate la scară largă [9]. Parolele continuă să rămână principala metodă de autentificare datorită simplității lor. Un număr mare de atacuri asupra sistemelor informatice se datorează utilizării acestora ca metodă de autentificare.

Există şi alte metode de verificare a autentificării cum ar fi:

- Email;
- SMS;
- Token.

Aceste metode sunt folosite la o scară foarte largă, însă prezintă anumite dezavantaje. Pentru verificarea autentificării prin sms este

necesară deținerea unui telefon în permanență şi cu toate acestea nu este sigură în totalitate deoarece sistemele de operare ale telefoanelor mobile au vulnerabilități care pot fi exploatate.

Metoda de autentificare cu token necesită deținerea în permanență a unui dispozitiv de generare al token-ului care şi acesta la rândul lui poate fi vulnerabil din punct de vedere al securității. Metoda de autentificare prin email este un pic anevoioasă deoarece necesită o autentificare în prealabil în contul de email.

Utilizatorii nu îşi amintesc întotdeauna parolele de la diferite conturi. O metodă folosită de utilizatori pentru a contracara acest lucru este de a folosi aceeaşi parolă pentru toate conturile ceea ce face mult mai nesigură autentificarea, iar riscul de a expune toate conturile creşte considerabil.

Există păreri care afirmă că autentificarea utilizatorilor ar trebui să se facă şi cu parole incomplete. La fel cum semnăturile de pe documente nu sunt identice întotdeauna şi totuşi sunt acceptate în marea majoritate a cazurilor. Acest tip de autentificare este foarte rar folosit şi implementarea lui este destul de complexă.

2. Autentificarea biometrică

Verificarea biometrică este considerată un subset al autentificării biometrice. Tehnologiile biometrice implicate se bazează pe modurile în care indivizii pot fi identificați în mod unic, prin una sau mai multe trăsături biologice distinctive, cum ar fi amprentele digitale, geometria mâinii, geometria lobului urechii, structura retinei sau a irisului, vocea, dinamica apăsării tastelor, ADN sau semnături. Autentificarea biometrică reprezintă folosirea unei dovezi a identității, ca parte a unui proces de validare a unui utilizator, pentru a avea acces la un sistem. Tehnologiile biometrice sunt utilizate pentru securitatea unei game largi de comunicații electronice, inclusiv securitatea întreprinderii, comerțul on-line şi serviciile bancare.

Sistemele de autentificare biometrice compară datele biometrice captate cu cele autentice, confirmate, stocate într-o bază de date. În cazul în care acestea sunt identice, autentificarea este confirmată şi accesul este permis. Procesul este uneori parte dintr-un sistem de autentificare multifactorială. De exemplu, un utilizator de smartphone s-ar putea conecta cu numărul său de identificare personală (PIN), ca apoi să furnizeze o scanare a irisului pentru a finaliza procesul de autentificare.

În prezent, din păcate, se pare că nu există încă o singură metodă de culegere şi citire a datelor biometrice care să garanteze autentificare sigură. Fiecare dintre diferitele metode de identificare biometrice au anumite caracteristici ce le recomandă spre utilizare. Unele dintre acestea sunt mai puțin invazive, unele se pot face fără cunoaşterea subiectului, iar unele sunt foarte greu de falsificat.

Metode biometrice de autentificare:

a) recunoaşterea facială

Dintre diferitele metode de identificare biometrice, recunoaşterea feței este una dintre cele mai flexibile, ce funcționează chiar şi fără ca subiectul să fie conştient că este scanat. Aceasta reprezintă, de asemenea, o modalitate promițătoare de a căuta un subiect prin masele de oameni care au petrecut doar câteva secunde în fața unui "scaner".

Sistemele de recunoaştere facială funcționează prin analiza sistematică a caracteristicilor specifice care sunt comune pentru orice față - distanța dintre ochi, lățimea nasului, poziția pomeților, linia maxilarului, bărbie şi aşa mai departe. Aceste cantități numerice sunt apoi combinate într-un singur cod care identifică în mod unic fiecare persoană [4].

b) amprenta digitală

Amprentele digitale rămân constante pe tot parcursul vieții. În peste 140 de ani de analiză a amprentelor digitale la nivel mondial, nu au fost vreodată găsite două amprente digitale identice, nici măcar la gemenii identici. Fiecare dintre noi ne naştem cu un set unic de amprente, deşi specialiştii nu ştiu nici acum cu exactitate la ce ne folosesc acestea. Scanere performante pentru amprente digitale au fost instalate pe dispozitivele smart; astfel încât tehnologia de scanare este, de asemenea, uşor de folosit.

Identificarea amprentelor digitale implică compararea modelului denivelărilor (creste şi şanțuri) de pe vârfurile degetelor, precum şi detaliile precise ale punctelor caracteristice (caracteristici ale ridurilor care apar atunci când o creastă se desparte în două, sau se

termină) scanate ale unui subiect, cu cele dintr-o bază de date [5].

c) geometria mâinii

Geometria mâinii este o metodă biometrică de identificare a utilizatorilor prin forma mâinilor lor. Scanerele pentru geometria mâinii măsoară mâna unui utilizator şi compară aceste măsurători cu datele stocate într-un fişier sau bază de date.

Dispozitive de analiză a geometriei mâinii au fost fabricate încă de la începutul anilor 1980, ceea ce face ca această metodă, prima metodă de autentificare biometrică computerizată, să fie folosită la scară largă. Nu este o metodă de testare intruzivă, fiind adesea folosită în mediile industriale.

d) scanarea retinei

Nu există nici o modalitate de a reproduce o retină deoarece modelul vaselor de sânge din spatele ochiului este unic şi rămâne acelaşi pentru întreaga viaţă. Cu toate acestea, este nevoie de aproximativ 15 secunde de concentrare pentru a obține o scanare validă. Scanarea retinei rămâne un standard utilizat în organizațiile militare şi guvernamentale [12].

e) scanarea irisului

Similar cu scanarea retinei, scanarea irisului oferă, de asemenea, date biometrice unice, care sunt foarte dificil de duplicat şi rămân aceleaşi pentru toată viaţa. Scanarea irisului este la fel de dificil de efectuat ca şi în cazul scanării retinei, însă cu toate acestea, există modalităţi de codare a datelor biometrice rezultate din scanarea irisului, astfel încât acestea să poată fi purtate în siguranţă într-un format de tip "cod de bare" [6].

f) semnătura digitală

O semnătură este un alt exemplu din categoria date biometrice, uşor de colectat şi neintruzive din punct de vedere fizic. Semnăturile digitale sunt folosite uneori, dar de obicei, au o rezoluţie insuficientă pentru a asigura autentificarea.

g) analiza vocii

Ca şi recunoaşterea facială, datele biometrice vocale furnizează o modalitate de a autentifica identitatea fără ştirea subiectului. Este mai uşor de falsificat (folosind o înregistrare pe bandă) însă nu este posibilă păcălirea un analist imitând vocea altei persoane.

Cu toate acestea, sistemele de verificare biometrice pot necesita o cheltuială semnificativă pentru implementarea la nivel de întreprindere. În funcție de gradul de securitate necesar, poate fi preferabil să fie utilizată autentificarea bazată pe mai mulți factori.

3. Keystroke Dynamics - mod biometric de autentificare

În 1984 toate drepturile asupra tehnologiei Keystroke Dynamics au fost cumpărate de către International Bioaccess Systems Corporation împreună cu toate brevetele şi secretele acestei tehnologii.

Tehnologia care stă în spatele Keystroke Dynamics măsoară o serie de temporizări ale apăsării tastelor în jos în timp ce utilizatorul introduce un şir de caractere. Aceste măsurători brute pot fi înregistrate de la aproape orice tastatură şi pot fi stocate pentru a determina timpul de aşteptare (timpul dintre tasta şi "tasta în sus") şi timpul de zbor (timpul de la "tastă în jos" la următoarea "tastă în jos" o "tasta în sus" şi următoarea "tastă în sus").

O data ce măsurătorile au fost captate datele sunt procesate printr-un algoritm neural unic care determină un model primar pentru o comparație viitoare. Ca şi orice altă tehnologie biometrică aceasta este folosită în două scopuri:

- înregistrarea utilizatorului;
- autentificarea utilizatorului.

Un şablon biometric ar putea fi generat de la o singură adresă de e-mail, o expresie sau o combinație de nume de utilizator şi parolă.

În prima parte a procesului de autentificare utilizatorul introduce de la tastatură o serie de caractere, iar apoi acestea sunt comparate pe baza şablonului creat în timpul procesului de înregistrare a utilizatorului. Pe baza temporizării apăsării tastelor este returnat un scor. Acest scor este folosit în luarea deciziei legate de controlul accesului în aplicație.

Aşa cum este descris mai sus, un şablon este creat la înregistrarea utilizatorului. Acest şablon se poate modifica având în vedere că utilizatorul poate deveni familiar cu tastarea unui anumit cuvânt. Rețeaua neuronală din

spatele acestei tehnologii învață noul pattern de tastare ca autentificarea utilizatorului care a devenit mai rapid în tastarea unor anumite cuvinte să se poată face cu succes.

Sunt o serie de termeni specifici care descriu securitatea autentificării de tip biometric:

- FAR – False Accept Error Rate;
- FRR – False Reject Error Rate;
- CER – Cross-over Error Rate.

De exemplu, FAR de 3% indică faptul că 3 utilizatori din 100 de utilizatori nelegitimi sunt acceptați ca utilizatori valizi.

FRR - sistemul respinge utilizatorii legitimi care sunt neacceptați în sistem în mod eronat. De exemplu, FRR de 3% indică faptul că 3 utilizatori din 100 de utilizatori legitimi sunt refuzați de sistem ca fiind utilizatori nelegitimi.

CER - rata erorilor de încrucişare (rata de eroare egală): rata la care FAR este egal cu FRR. În exemplele de mai sus CER este de 3%.

Tehnologia keystroke dynamics este mult superioară comparând cu alte metode non-biometrice de autentificare, cum ar fi: tehnologiile de proliferare şi parolele complexe. După cum au constatat multe companii, securitatea, utilitatea şi costurile sunt componente critice de înțeles ca parte a oricărei implementări a tehnologiilor de securitate.

Există compromisuri care trebuie făcute pentru fiecare tip de tehnologie. Spre deosebire de alte tehnologii de securitate biometrice, keystroke dynamics este singura tehnologie de securitate care oferă posibilitatea de a îmbina securitatea şi utilitatea pentru a oferi o soluție eficientă pentru fiecare mediu de aplicație.

Keystroke dynamics se poate implementa în mai multe cazuri.

- accesul în site-urile web;
- accesul angajaților din mediul corporatist;
- în autentificare în cazul unor tranzacții de mare valoare (tranzacții bancare).

Keystroke dynamics prezintă multiple avantaje precum [16][18]:

- soluție foarte rapidă;
- precisă;
- scalabilă la milioane de useri;
- poate fi implementată foarte rapid în aplicațiile din internet;
- disponibil oriunde există o tastatură - nu este necesar un echipament special;
- utilizabil - nu se modifică comportamentul utilizatorilor;
- neinvazivă - fără a utiliza amprente;
- ritmul de tastare al unei persoane nu poate fi pierdut sau uitat;
- pentru resetare se generează un şablon nou;
- se integrează perfect cu mediile şi procesele tehnologice existente - integrare completă cu Windows;
- nu necesită distribuirea, gestionarea sau înlocuirea unui senzor special, tokens, card-uri sau tastaturi speciale.

Un exemplu de implementare pentru Keystroke Dynamics este măsurarea timpului în care utilizatorul ține apăsată o tastă. Pentru implementarea în C# se declară 3 variabile:

```
private DateTime startDate;
private DateTime endDate;
private double duration;
```

Variabila *startDate* o să fie folosită pentru memorarea momentului în care utilizatorul apasă tasta. Variabila *endDate* este folosită pentru memorarea momentului în care utilizatorul ridică degetul de pe tasta apăsată. Iar variabila *duration* este folosită pentru calcularea timpului dintre cele două momente.

Pentru obținerea celor două momente se creează două metode. O metodă este abonată la evenimentul de KeyDown al unui Control de tipul TextBox, iar a doua metodă este abonată la evenimentul de KeyUp al aceluiaşi control de tip TextBox:

```
private void textBoxNume_KeyDown(object sender, KeyEventArgs e)
        {
            startDate = DateTime.Now;
        }
private void textBoxNume_KeyUp(object sender, KeyEventArgs e)
        {
            endDate = DateTime.Now;
            duration = (endDate - startDate).TotalMilliseconds;
            //salvarea sau procesarea valorii variabilei
duration
        }
```

Astfel, în prima metodă se salvează momentul apăsării unei taste de către utilizator. În cadrul celei de a doua metode se salvează momentul eliberării tastei şi se calculează durata cât a stat apăsată. Această durată este salvata în fişier sau în baza de date sau poate fi procesată pentru calcularea unei medii a duratelor de apăsare a tastelor. Acest lucru diferă de la aplicație la aplicație şi de la model la model.

4. Utilizarea API-ului TypingDNA pentru dezvoltarea aplicațiilor web

Implementarea modului de typing biometrics a devenit tot mai utilizat în ultima perioadă, datorită beneficiilor aduse în interacțiunea cu utilizatorul. TypingDNA.com [22] propune un nou mod de autentificare prin recunoaşterea user-ului pe baza unui text scris de acesta anterior. În acest mod, dacă parola este uitată, nu este necesară urmarea procedurii birocratice de recuperare a parolei, ci recuperarea se va face prin recunoaşterea utilizatorului pe baza modului de scriere a textului în mod automat de către aplicație, utilizatorul trebuind doar să scrie un text furnizat. Orice aplicație poate implementa TypingDNA API după ce în prealabil trebuie sa înregistreze un pattern de tastare al user-ului apoi sa apeleze TypingDNA API pentru a valida autentificarea acestuia.

API-ul TypingDNA este folosit pentru mai multe aplicații. Astfel se consideră mulțimea de aplicații:

$$MA = \{A_1, A_2, ..., A_i, ..., A_{na}\}$$

Unde:

- *na* reprezintă numărul de aplicații;
- *A* reprezintă aplicația *i* din mulțimea MA.

TypingDNA foloseşte algoritmi de inteligență artificială pentru autentificare ceea ce duce la reducerea erorilor la un nivel care nu a mai fost atins până acum. Folosirea metodei de autentificare prin recunoaşterea biometricii tastării poate fi folosită şi ca un factor de siguranță al autentificării în plus față de modul de autentificare prin username şi parolă. Acest lucru va micşora considerabil riscul ca cel care încearcă acea parola să nu fie deținătorul de drept al acelei parole.

Tipul de autentificare typing biometrics oferă o gamă largă de avantaje şi previne unele tentative de fraudă cum ar fi:

- identificarea tranzacțiilor frauduloase cu carduri bancare;
- fraudarea examenelor online;
- activități de "account sharing".

Pentru a exemplifica un tip de autentificare (typing biometrics) am implementat pe o maşină virtuală un client care să înregistreze un utilizator şi apoi să ceară API-ului TypingDNA o cerere de autentificare.

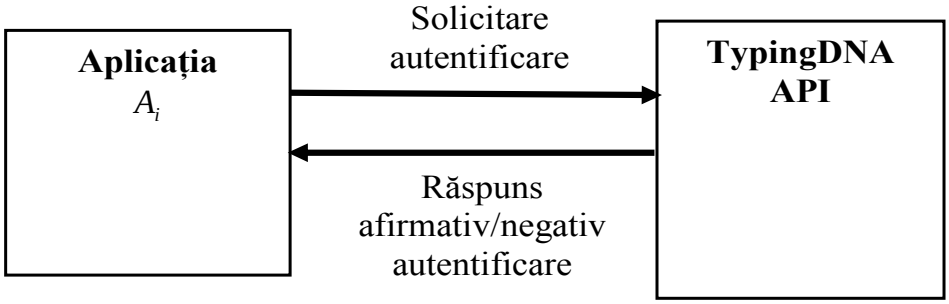

Figura 1. Diagrama utilizării TypingDNA API

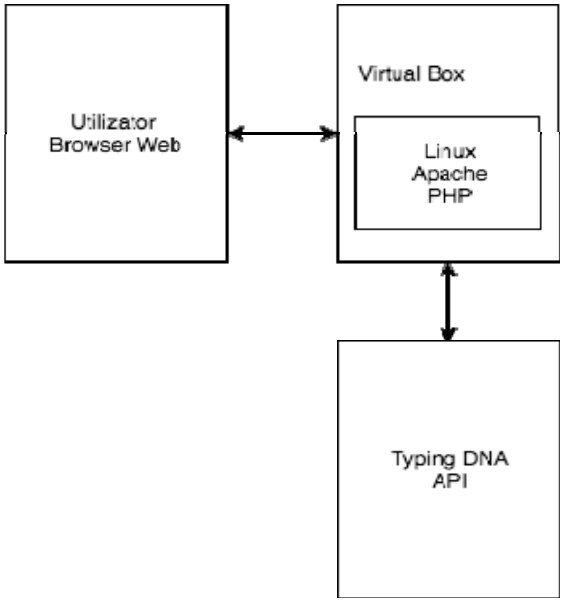

Figura 2. Fluxul utilizării TypingDNA API

Pe un software Virtual Box am instalat un sistem de operare Linux (Ubuntu). Pe acest sistem am pus un interpretor al limbajului PHP. Am ales acest interpretor deoarece acesta este limbajul în care a fost dezvoltat clientul care face autentificarea către TypingDNA. Tot pe această maşină am instalat şi un server web Apache. În schema de mai jos este conturat un model de funcționare al clientului de test pentru autentificarea pe baza pattern-ului de tastare.

Pentru a putea construi clientul ce apelează API-ul Typing DNA în prealabil trebuie realizat un cont pe site-ul typingdna.com. În urma autentificării se primeşte un API key şi un security code. Acestea sunt 2 hash-uri care trebuie implementate în codul clientului PHP ce face cererea către API. În prima faza utilizatorul trebuie înrolat în aplicație.

Mai exact este creat în folder-ul de root al serverului instalat pe maşina de Linux un fişier de tip php care generează un template de HTML ce permite inserarea de text. Un user care doreşte să fie înregistrat pe baza biometricii de tastare trebuie să introducă în prima fază un text care este trimis către serverul Apache de pe maşina virtuală de Linux, iar aceasta trimite cererea mai departe către API-ul TypingDNA.

Pentru o identificare mai precisă la înregistrarea utilizatorului acesta trebuie să introducă încă un text suplimentar.

După ce paternul de tastare este trimis către API, utilizatorul poate să se autentifice pe baza unei fraze de 170 de caractere pe care o va scrie. Pentru acest lucru am creat încă o pagină php care generează un fişier HTML în care utilizatorul scrie fraza de autentificare.

Apoi va fi trimisă cererea către API-ul TypingDNA, iar acesta va trimite în urma analizei un răspuns afirmativ sau negativ (dacă utilizatorul este autentificat sau nu).

5. Concluzii

Există o serie de alternative viabile la utilizarea parolei ca metodă de autentificare, alternative care nu numai că îmbunătățesc eficacitatea securității pentru organizație, ci oferă şi beneficiul utilizabilității facile pentru utilizatorii finali. În ciuda măsurilor avansate de securitate pe care întreprinderile le pun în aplicare, utilizarea parolelor pentru autentificare împiedică atingerea unui nivel ridicat de securitate. Înlocuirea acestora este o abordare excelentă în prevenirea celor 63% din atacurile cibernetice confirmate, care au implicat parole slabe, implicite sau furate, aşa cum reiese din

raportul de investigații cu privire la incidentele de securitate al Verizon [13].

Acknowledgment

Această lucrare a fost realizată ca parte a proiectului Nucleu: PN 16 09 01 02 - Cercetări privind autentificarea online în cadrul aplicațiilor software bazate pe comportamentul utilizatorilor.

BIBLIOGRAFIE

1. **SHI, E.; NIU, Y.; JAKOBSSON, M.; CHOW, R.:** Implicit Authetication through Learning User Behavior, Information Security. Springer Berlin Heidelberg, 2011, pp. 99-113.
2. **ROTH, J.:** On Continuous User Authentication via Typing Behavior. IEEE Transactions On Image Processing, July 28, 2014.
3. **YAMPOLSKIY, V. R.:** Action-based user authentication. Int. J. Electronic Security and Digital Forensics, Vol. 1, No. 3, 2008.
4. *** FTC seeks public comments on facial recognition, 2012, https://crisisboom.com/2012/01/10/ftc-seeks-public-comments-on-facial-recognition/
5. *** Fingerprint sensors, facial recognition and biometric surveillance to propel biometrics market, http://www.donseed.com/4278-2/
6. *** IBTimes, 2015, UN: Biometric iris scanners transforming Syrian refugee programme by preventing fraud, http://www.ibtimes.co.uk/un-biometric-iris-scanners-transforming-syrian-refugee-programme-by-preventing-fraud-1527362
7. *** 5 Things You Should Know About the FBI's Massive New Biometric Database, 2012, https://crisisboom.com/2012/01/11/fbi-biometric-database/
8. *** NIST Authentication Guideline. 2016, https://pages.nist.gov/800-63-3/sp800-63-3.html#sec4
9. *** Strong Authentication Best Practices, https://safenet.gemalto.com/multi-factor-authentication/strong-authentication-best-practices/
10. *** Biometric authentication: what method works best?, http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=16
11. *** Understanding Digital Certificates, https://technet.microsoft.com/en-us/library/bb123848(v=exchg.65).aspx
12. Retina scan, http://whatis.techtarget.com/definition/retina-scan
13. *** Highlights From Verizon Data Breach Report https://blogs.gartner.com/anton-chuvakin/2015/05/18/highlights-from-verizon-data-breach-report-2015/
14. *** Raportarea Incidentelor Cyber în UE - ENISA, august 2012 - https://www.enisa.europa.eu/publications/cyber-incident-reporting-in-the-eu/at_download/fullReport
15. *** Verizon Data Breach Investigations Report,2017 http://www.verizonenterprise.com/resourcs/reports/rp_DBIR_2017_Report_en_xg.pdf
16. *** BioPassword Whitepaper, Authentication Solutions Through Keystroke Dynamics, 11 pag.
17. **SWARNA BAJAJ; SUMEET KAUR:** Typing Speed Analysis of Human for Password Protection (Based On Keystrokes Dynamics), International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-3, Issue-2, July 2013.
18. **PIN SHEN TEH, ANDREW BENG JIN TEOH AND SHIGANG YUE:** A Survey of Keystroke Dynamics Biometrics, The ScientificWorld Journal, Volume 2013, Article ID 408280, 24 pages.

19. **D. SHANMUGAPRIYA, G. PADMAVATHI:** A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009.

20. **ARWA ALSULTAN; KEVIN WARWICK**: Keystroke Dynamics Authentication: A Survey of Free-text Methods. IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013, ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784

21. **MARGIT ANTAL*; LÁSZLÓ ZSOLT SZABÓ; IZABELLA LÁSZLÓ:** Keystroke Dynamics on Android Platform. 8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014, 9-10 October 2014, Târgu Mureş, România.

22. *** https://typingdna.com/