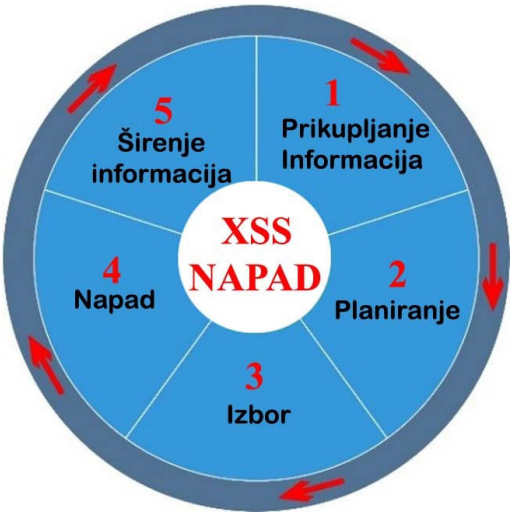
UNIVERZITET U BANJALUCI

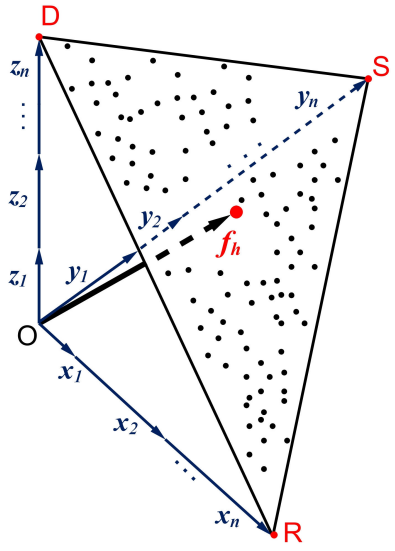
PRIRODNO-MATEMATIČKI FAKULTET

Dragan M. Korać

ZAŠTITA INFORMACIJA U OKVIRU SISTEMA MENADŽMENTA IDETITETA I UPRAVLJANJA PRISTUPOM

Naučna monografija





Banjaluka, 2022

UNIVERZITET U BANJALUCI

PRIRODNO MATEMATIČKI FAKULTET

Dragan M. Korać

ZAŠTITA INFORMACIJA U OKVIRU SISTEMA MENADŽMENTA IDETITETA I UPRAVLJANJA PRISTUPOM

Naučna monografija

Banjaluka, 2022

UNIVERSITY OF BANJA LUKA

FACULTY OF NATURAL SCIENCES AND MATHEMATICS

Dragan M. Korać

INFORMATION SECURITY IN FRAME OF IDENTITY AND ACCESS MANAGEMENT SYSTEMS

Scientific monograph

Banja Luka, 2022

Zaštita informacija u okviru sistema menadžmenta idetiteta i upravljanja pristupom

Autor
Doc. dr Dragan Korać

Recezenti
Prof. dr Boško Nikolić
Prof. dr Dejan Simić

Izdavač
Univerzitet u Banjoj Luci
Prirodno – matematički fakultet

Za izdavača
Prof. dr Goran Trbić, dekan

Urednik
Prof. dr Duško Jojić

Tehnički urednik
Doc. dr Dragan Korać

Lektor
Mr Sanja Bajić

Štampa
Makoprint, Banjaluka

Tiraž
200 primjeraka

ISBN 978-99976-86-06-0

Monografija je odobrena Odlukom Nastavno-naučnog vijeća Prirodno-matematičkog fakulteta, Univerziteta u Banjoj Luci (broj: 19/3.1893/22. godine), a njeno štampanje je sufinansiralo Ministarstvo za naučnotehnološki razvoj, visoko obrazovanje i informaciono društvo Republike Srpske.

Mojoj familiji
Familiji moje sestre
Mojim roditeljima, posebno majci znajući koliko bi ona bila ponosna

Predgovor

Posljednjih godina, zaštita informacija u okviru sistema menadžmenta identiteta i upravljanja pristupom (IAM) se izdiferencirala kao poseban izazov. Prije svega, izazov je povezan sa fundamentalnim istraživačkim ciljevima usmjerenim na osnovne modele zaštite infomacija, alate zaštite u okruženjima e-učenja, kao i prijetnje i posljedice od sajber napada kao što je Cross Site Scripting (XSS). Sadržaj monografije integriše važnost u pojmu teorije i primjene i kao takav treba da bude jednako zanimljiv istraživačima i praktičarima.

Pored brojnih razvijenih modela zaštite informacija, napadači iznova pronalaze praznine u aspektu zaštite stvarajući nove i sve opasnije sajber prijetnje. Mnogo je faktora koji ukazuju da do sada nema lakih i konkretnih odgovora sa kojima bi se to spriječilo, a vjerojatno ih nikada neće ni moguće dobiti. Jedna od najvećih sajber prijetnji je XSS napad sa kojima napadači mogu da uspješno zaobiđu postojeća tehnička rješenja. Treba naglasiti da su XSS napadi obično pod vanjskom kontrolom (napadača) i često se izvode upotrebom dodatnih tehnika, dok je provođenje zaštite pod unutrašnjom kontrolom (sistema). Dakle, centralni problem ove monografije je usmjeren na analizu postojećih modela zaštite informacija s ciljem stvaranja bezbjednijeg sajber okruženja.

Područje zaštite informacija je ogromno i nije moguće da se pokrije u pojedinačnom opsegu. Međutim, napravljen je napor da se uključe radovi koji su pristupačni ka opštem čitaocu, ali koji takođe imaju dovoljnu dubinu za istraživače iz ove oblasti. To je urađeno s nadom da većina čitalaca bude u stanju da mnogo lakše shvati i upotrijebi informacije predstavljene u različitim sekcijama.

Materijal ove monografije je organizovan u 10 međusobno povezanih cjelina.

Prvi dio monografije započinje sa "Zašto istraživati zaštitu informacija u okviru IAM sistema". U nastavku, problemi su definisani sa detaljnom elaboracijom svih otvorenih pitanja prisutnih u okviru IAM sistema.

Drugi dio monografije daje detaljni uvid u prethodna referentna istraživanja u ovoj oblasti.

Treći dio monografije daje pregled i definicije osnovnih pojmova u aspektu zaštite informacija u okviru IAM sistema obuhvatajući pojmove informacije i zaštite, principe i kontrolu zaštite informacija, pregled i opis osnovnih korisničkih faktora, tipove kolačića, kao i učesnika u XSS napadima.

Četvrti dio monografije je posvećen IAM sistemima sa jasnim pregledom i detaljnim opisom njegovih bazičnih komponenti i funkcija. Na ovaj način, struktuirani uvod u metode autentifikacija je obezbijeđen.

Peti dio monografije daje detaljan pregled i analizu bazičnih metoda autentifikacija. Ovaj dio definiše višestruke autentifikacione mehanizme (MFA), njihove prednosti odnosno ograničenja u pogledu višefaktorskog integrisanja.

Šesti dio monografije daje detaljnu analizu osnovnih modela zaštite informacija. Ovaj dio započinje pregledom i opisom osnovnih modela zaštite naglašavajući posebno njihova ograničenja. U nastavku dijela, zbog značaja i važnosti koji imaju u zaštiti informacija posebno su izdiferencirani i analizirani Model digitalnog identiteta (MDI) i Fishbone model.

Sedmi dio monografije daje primjere implementacije MDI i Fishbone modela. Ovaj dio započinje primjerom implementacije MDI u formi alata zaštite u Moodle LMS dok je u nastavku dat primjer implementacije Fishbone modela zasnovanog na primjeni Fazi ekspertnog sistema (FES) alata za MFA.

Osmi dio monografije je posvećen sajber zaštiti u pogledu krađe i budućnosti identiteta. Ovaj dio se bavi elaboracijom fenomena krađe identiteta u pogledu zloupotrebe kolačića. Izdiferencirane su prijetnje u formi XSS napada kao jedan od najopasnijih napada sa kojima je to moguće učiniti. Osim toga, pregled i opis postojećih osnovnih metoda zaštite od tih prijetnji je takođe dat.

Deveti dio monografije daje kritički osvrt u pogledu diskusije koja prati fundamentalni istraživački izazov ove studije. Takođe, diskutovani su pravci daljeg istraživanja.

Deseti dio monografije daje zaključna razmatranja sublimirajući ih kroz zaključke koji prate tri ključna istraživačka pravca.

Za realizaciju ove monografije, dodatni napor je uložen kako bi se tekst učinio mnogo čitljivijim u rednom redoslijedu, ali čitalac treba da bude svjestan da dublje razumijevanje ove studije vjerovatno zahtijeva da se prate povezane cjeline naprijed i unazad. Stoga čitalac treba uvijek biti svjestan unutrašnjih poteškoća koje treba savladati. Ova monografije može biti namijenjena studentima diplomskih i postdiplomskih studija, kao i svim drugima koji se bave zaštitom informacija posebno u aspektu IAM sistema.

Banja Luka, septembar, 2022. Autor

Preface

In the last years, the information security in systems for identity and access management is differentiated itself as a special challenge. First off all, the challenge is related to fundamental research goals focused on basic information security models, security tools in e-learning environments, as well as threats and consequences from cyberattacks such as Cross Site Scripting (XSS). The content of the monograph integrates importance in term of theory and application, and as such it should be equally interesting to both researchers and practitioners.

Besides, the numerous developed information security, attackers are repeatedly finding gaps in the security aspect, creating new and increasingly dangerous cyber threats. There are many factors that indicate that there are no easy and concrete answers so far to prevent this, and it will probably never be possible to get them. One of the biggest cyber threats is the XSS attack, with which attackers can successfully bypass the existing technical solutions. It should be emphasized that XSS attacks are usually under external control (the attacker) and they are often carried out using additional techniques, while the enforcement of security is under internal control (the system). Therefore, the central problem of this monograph is to analyze the existing models of information security with the aim of creating a safer cyber environment.

The field of information security is huge and it is not possible to cover it in a single scope. However, an effort has been made to include manuscripts that are accessible to the general reader, but that have sufficient depth for research from this field. It is done with the hope that most readers will be able to much more easily understand and use the information presented in the various sections.

The material of this monograph is organized into 10 interconnected units.

The first part of the monograph begins with "Why research information security in frame of the IAM system". In the following, the problems are defined with a detailed elaboration of all open questions present in the framework of IAM system.

The second part of the monograph provides a detailed insight into previous reference research in this area.

The third part of the monograph gives an overview and definitions of basic terms in the aspect of information security in the IAM system, including the terms information and security, principles and control of information security, an overview and a description of basic user factors, types of cookies, as well as participants in XSS attacks.

The fourth part of the monograph is devoted to IAM systems with a clear overview and a detailed description of its basic components and functions. In this way, a structured introduction in authentication methods is provided.

The fifth part of the monograph gives a detailed overview and analysis of basic authentication methods. This part defines multiple authentication mechanisms (MFA), their advantages and limitations in terms of multi-factor integration.

The sixth part of the monograph provides a detailed analysis of the basic models of information security. This part begins with an overview and a description of the basic security models, emphasizing in particular their limitations. In the following section, because of their significance and importance in information security, the Model of Digital Identity (MDI) and the Fishbone model are specifically differentiated and analyzed.

The seventh part of the monograph gives examples of the implementation of MDI and Fishbone model. This part begins with an example of the implementation of MDI in the form of a security tool in Moodle LMS, hereafter an example of implementation of the Fishbone model based on application of the Fuzzy Expert System (FES) tool for MFA is given.

The eighth part of the monograph is dedicated to cyber security regarding identity theft and the future of identity. This part deals with the elaboration of phenomenon of identity theft with regard to the misuse of cookies. Threats in the form of XSS attacks are differentiated as one of the most dangerous attacks with which it is possible to do it. Moreover, an overview and a description of existing basic methods of security against these threats is also given.

The ninth part of the monograph gives a critical review regarding the discussion that follows the fundamental research challenge of this study. Also, directions for further research are discussed.

The tenth part of the monograph gives concluding considerations, sublimating them through conclusions that follow three key research directions.

For the realization of this monograph, the extra effort has been made to make the text much more readable in sequential order, but the reader should be aware that a deeper understanding of this study probably requires following the connected units forwards and backwards. Therefore, the reader should always be aware of the internal difficulties that need to be overcome. This monograph can be intended for undergraduate and postgraduate students, as well as for all others who deal with information security, especially in the aspect of the IAM system.

Banja Luka, September, 2022. Author

SADRŽAJ

XI Literatura

1. Hong, S., Liu, C., Ren, B., Huang, Y., Chen, J., 2017. Personal Privacy Protection Framework Based on Hidden Technology for Smartphones. IEEE Access, 5, 6515-6526.
2. Shen, C., Li, Y., Chen, Y., Guan, X., Maxion, R. A. 2018. Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication, IEEE Transactions on Information Forensics and Security, 13(1), 48 - 62.
3. Sabzevar, A.P., Stavrou A., 2008. Universal Multi-Factor Authentication Using Graphical Passwords. International Conference on Signal Image Technology and Internet Based Systems, IEEE, pp. 625 – 632.
4. Kiljan, S., van Eekelen, M. and Vranken, H. Evaluation of transaction authentication methods for online banking. Future Generation Computer Systems, 80, 430-447, 2018.
5. Al-Fraihat, D. Joy, M. Masa'deh R. and Sinclair, J. Evaluating E-learning systems success: An empirical study, Computers in Human Behavior, 102, 67-86, 2020.
6. Kambourakis, G. Kontoni, D.P. N. Rouskas A. and Gritzalis, S. A PKI approach for deploying modern secure distributed e-learning and m-learning environments, 48(1), 1-16, 2007.
7. Kambourakis, G. Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art, International Journal of u- and e- Service, Science and Technology, 6(3), 67-84, 2013.
8. Derawi, M. "E-learning protection of open access platforms," 2014 International Conference on Web & Open Access to Learning (ICWOAL), 2014.
9. Korać, D. and Simić, D. Fishbone Model and Universal Authentication Framework for Evaluation of Multifactor Authentication in Mobile Environment. Computers & Security, 85, 313-332, 2019.
10. Korać, D. and Simić, D. Design of Fuzzy Expert System for Evaluation of Contemporary User Authentication Methods Intended for Mobile Devices, Journal of Control Engineering and Applied Informatics, 19(4), 2017.
11. Ray, S., Biswas, G.P., 2011. Design of mobile-PKI for using mobile phones in various applications. In Proceedings of IEEE international conference on recent trends in information systems. IEEE, pp. 297-302.
12. Friedewald, M. Vildjiounaite, E. Punie Y. and Wright, D. Privacy, identity and security in ambient intelligence: a scenario analysis, Telemat Inf, vol, 24(1), pp. 15-29, 2007.
13. Peltier, T.R. Peltier, J. and Blackley, J. Formation security fundamentals, Boca Raton, Fl, Auerbach, 2005, p. 39.
14. Balon, I. and Thabet, I. Biba security model comparison. CIS 576, 2004.
15. Alharby, N. E-government Security: Explaing Main Factors and Analysing Existing Models. World Academy of Science, Engineering and Technology International Journal of Social, Human Science and Engineering 7(9), pp. 1319-1321, 2013.

16. Bell, D.E. and LaPadula, L. Secure Computer Systems: Unified Exposition and Multics Interpretation. ESD-TR-75-306, MITRE MTR-2997, MITRE Corporation, 1976.
17. Biba, K.J. Integrity constraints for secure computer systems. Technical Report EST TR-76-372, Hanscom AFB, 1977.
18. Sandhu, R.S. and Mason, G. Lattice-based Access Control Models. IEEE, pp. 9-19, 1993.
19. Lipton, R. J. and Snyder, L. "A linear time algorithm for deciding subject security." Journal of the ACM, 24(3), 455-464, 1977.
20. Denning, D. E., Lunt T.F., Schell, R. R., Shockley, W.R., and Heckman M. The sea view security model. IEEE, pp. 218-233, 1998.
21. Korać, D. Comparison of Information Security Models. *Info M*, FON, 56(4), 17-24, 2015.
22. Ayodele, T., Shoniregun, C.A. and Akmayeva, G. Towards e-learning security: A machine learning approach. *In Information Society (i-Society), 2011 International Conference* (pp. 490-492). IEEE, 2011.
23. Cole, J., Foster, H. 2008. Using Moodle – Teaching with the popular open source course management system, O.R. Media, Editor: United Sates of America.
24. Wang, M., Vogel, D. and Ran, W. Creating a performance-oriented e-learning environment: A design science approach. Information & Management, 56(7), 260-269, 2011.
25. Shaw, R.H., Chen, C.C., Harris, A., Huang, H.J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92-100.
26. Venkatraman, S., Alazab, M., Vinayakumar, R. (2019). A hybrid deep learning image-based analysis for effective malware detection. Journal of Information Security and Applications, 47, 102358.
27. Safa, N.S., Maple, C., Watson, T., Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. Journal of Information Security and Applications, 40, 377-389.
28. Furnell, S.M., Karweni, T. (2001). Security issues in online distance learning. Vine, 31(2), 28-35.
29. Fenu, G., Marras, M., Boratto, L. (2018). A multi-biometric system for continuous student authentication in e-learning platforms. Pattern Recognition Letters, 113, 83-92.
30. Feizollah, A., Anuar, N.B., Salleh, R., Suarez-Tangil, G., Furnell, S. (2017). AndroDialysis: Analysis of Android Intent Effectiveness in Malware Detection. Computers & Security, 65, 121-134.
31. Meng, W., Wong, D.S., Furnell, S., Zhou, J. (2014). Surveying the development of biometric user authentication on mobile phones. IEEE Communications Surveys & Tutorials 17(3), 1268-1293.
32. Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., Shabtai, A. (2018). Taxonomy of mobile users' security awareness. Computers & Security, 73, 266-293.
33. Verkijika, S.F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. Computers & Security, 77, 860-870.
34. Moodle, (2020). http://moodle.org/stats (Accessed October 20, 2020).
35. Walt, E., Eloff, J.H.P., Grobler, J. (2018). Cyber-security: Identity deception detection on social media

platforms. Computers & Security, 78, 76-89.

36. Safa, N.S., Maple, C., Furnell, S., Azad, M.A., Muhammad Perera, C., Dabbagh,M., Sookhak, M. (2019). A deterrence and prevention-based model to mitigate information security insider threats in organisations. Future Generation Computer Systems, 97, 587-597.
37. Markelj, B., Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. Journal of Information Security and Applications, 20, 84-89.
38. Agrawal, N. and Tapaswi, S. A trustworthy agent-based encrypted access control method for mobile cloud computing environment. Pervasive and Mobile Computing, 52, 13-28, 2019.
39. Yang, W., Li, J., Zhang, Y., Gu, D. (2019). Security analysis of third-party in-app payment in mobile applications. Journal of Information Security and Applications, 48, 102358.
40. Alotaibi, M., Furnell, S., Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, pp. 352-358.
41. Capobianco, B.M., French, B.F., Diefes-Du, H.A. (2012). Engineering identity development among pre-adolescent learners. Journal of Engineering Education, 101(4), 698–716.
42. Windley, P. *Digital Identity*. United States of America: O'Reilly Media, Inc., 2005.
43. Dykstra, J., Spafford, E.H. (2018). The case for disappearing cyber security. Communications of the ACM, 61(7), 40-42.
44. Yamauchi, B. 1997. A frontier-based approach for autonomous exploration. In: Proceedings of the 1997 IEEE International symposium on computational intelligence in robotics and automation (CIRA-97). Washington, DC: IEEE Computer Society, pp. 146–151.
45. Albeshri, A., Caelli, W. (2010). Mutual protection in a cloud computing environment. In High Performance Computing and Communications (HPCC). 12th IEEE International Conference on, IEEE (pp. 641-646).
46. Gomi H. A persistent data tracking mechanism for user-centric identity governance. *Identity in the Information Society*, 3(3), 639-656, 2010.
47. Asaddok, N., Ghazali, M. 2017. Exploring the usability, security and privacy taxonomy for mobile health applications. Research and Innovation in Information Systems (ICRIIS), 2017 International Conference on. IEEE, pp. 1-6.
48. Dasgupta, D., Roy, A., Nag, A., (2017). Multi-Factor Authentication. In: Advances in User Authentication. Infosys Science Foundation Series. Springer, Cham, Springer International Publishing, pp. 185-233.
49. Kim, S., Oh, H.T., Kim, Y.G., 2016. Certificate sharing system for secure certificate distribution in mobile environment. Expert Systems with Applications, 44, 67-77.
50. Korać, D. and Čiča, Đ. *A mathematical model for evaluation of intelligence products value,* Journal of Information and Optimization Science, 39(4), 903-926, 2018.

51. Bonneau, J., Herley, C., Oorschot, P.C., Stajano, F., 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. 2012 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 553-567.
52. Kirda, E., Kruegel, C., Giovanni Vigna, G. and Jovanovic, N. Noxes: a client-side solution for mitigating cross-site scripting attacks. In Proceedings of the 2006 ACM symposium on Applied computing. ACM, 330–337, 2006.
53. Liu, S. and Cheng, B. Cyberattacks: "Why, what, who and how",in:ITPro.,IEEE Computer Society, May/June 2009.
54. Tsipenyuk, K., Chess, B. and McGraw, G. Seven pernicious kingdoms: A taxonomy of soft waresecurity errors, IEEESecur. Priv. 3(6) (2005) 81–84, 2005.
55. Kals, S. Kirda, E. Kruegel, C. and Jovanovic, J. "SecuBat: a web vulnerability scanner," Proceedings of the 15th international conference on World Wide Web, WWW 2006, Edinburgh, Scotland, UK, May 23-26, 2006.
56. Zhou, Y. and Wang, P. An ensemble learning approach for XSS attack detection with domain knowledge and threat intelligence. Computers & Security, 82, 261-269, 2019.
57. Mokbal, F.M.M., Dan, W. Imran, A. Jiuchuan, L. Akhtar, F. and Xiaoxi, W. "MLPXSS: An Integrated XSS-Based Attack Detection Scheme in Web Applications Using Multilayer Perceptron Technique," in IEEE Access, vol. 7, pp. 100567-100580, 2019.
58. Rodríguez, G.E., Benavides D.E., Torres J., Flores P. and Fuertes W. Cookie Scout: An Analytic Model for Prevention of Cross-Site Scripting (XSS) Using a Cookie Classifier. In: Rocha Á., Guarda T. (eds) Proceedings of the International Conference on Information Technology & Systems (ICITS 2018). ICITS 2018. Advances in Intelligent Systems and Computing, vol 721. Springer, Cham.
59. Verizon. 2018. 2017 data breach investigations report. (April 2018). http://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf.
60. Sarmah, U., Bhattacharyya, D.K., and Kalita, J.K. A Survey of Detection Methods for XSS Attacks, Journal of Network and Computer Applications, 118, 113-143, 2018.
61. Singh, J. P. Analysis of SQL Injection Detection Techniques, Theoretical and Applied Informatics (TAAI) 28 (1-2) (2016) 37–55.
62. Nithya, V. Pandian S. L., and Malarvizhi, C. A Survey on Detection and Prevention of Cross-site Scripting Attack, International Journal of Security and Its Applications 9(3), 139–152, 2015.
63. What Are Cookies and How Do They Work on Desktop vs. Mobile? https://www.spotx.tv/resources/blog/product-pulse/what-are-cookies-and-how-do-they-work-on-desktop-vs-mobile/ (accessed January 10, 2020).
64. Anderson, M., Montague, P. and Long, B. A Formal Integrity Framework with Application to a Secure Information ATM (SIATM). DSTO Defence Science and Technology Organisation. Commonwealth of Australia 2012.

65. Brewer, D. F. C. and Nash, M. J., The Chinese Wall security policy. IEEE Symp. on Security and Privacy, 1989, pp. 215-228.
66. Lipner, S. B. Non-discrentionary controls for commercial applications. In IEEE Symposium on Security and Privacy, pp. 2-10, Oakland, May 1982.
67. Clark, DD., & Wilson, D. R., A comparison of commercial and military computer security policies, in IEEE Symposium of Security and Privacy, pp. 184-194, 1987.
68. Korać, D., Damjanović, B. & Simić, D. A model of digital identity for better information security in e-learning systems. J Supercomput, 78, 3355 (2022). https://doi.org/10.1007/s11227-021-04006-w.
69. Beres, Y., Baldwin, A. Mont, M.C. and Shiu, S. On identity assurance in the presence of federated identity management systems. Proceeding DIM '07 Proceedings of the 2007 ACM workshop on Digital identity management, ACM, pp. 27-35, 2007.
70. Bosworth, K. Gonzalez, M. G. Jaweed S. and Wright, T. Entities, Identifiers and Credentials – what does it all mean? *Bt Technology Journal*, 23(4), 25-36, 2005.
71. Bertino, E., and Takahashi, K. Identity Management: Concepts, technologies, and systems. London: Artech House Inc. 2010.
72. Cunningham, K.J. How language choices in feedback change with technology: Engagement in text and screencast feedback on ESL writing, Computers & Education, 135, 91-99, 2019.
73. Filius, R.M., de Kleijn, R.A.M., Uijl, S.G., Prins, F.J., van Rijen, H.V.M., and Grobbe, D.E. Strengthening dialogic peer feedback aiming for deep learning in SPOCs. Computers & Education, 125, 86-100, 2018.
74. Rowe, A.D., Fitness, J., and Wood, L.N. The role and functionality of emotions in feedback at university: A qualitative study. Australian Educational Researcher, 41, 283-309, 2014.
75. Rowe, A. The personal dimension in teaching: Why students value feedback. International Journal of Educational Management, 25, 343-360, 2011.
76. Alotaibi, F., Furnell, S., Stengel, I., and Papadaki, M. Gamifying cyber security awareness via mobile training apps, In CERC 2017 Collaborative European Research Conference Proceedings, CEUR Workshop Proceedings, pp. 236-238, 2017.
77. Kirlappos, I., Parkin, S., Sasse, M.A. "Shadow security" as a tool for the learning organization, ACM SIGCAS Computers and Society, 45(1), 29-37, 2015.
78. Xu, Y., Yin, D. and Zhou, D. Investigating Users' Tagging Behavior in Online Academic Community Based on Growth Model: Difference between Active and Inactive Users. Information Systems Frontiers, 21(4) 761–772, 2019.
79. Kima, K.K., Lee, A.R., and Lee, U.K. Impact of anonymity on roles of personal and group identities in online communities. Information & Management, 56, 109-121, 2019.
80. Christopherson, K. The positive and negative implications of anonymity in Internet social interactions: 'on the Internet, Nobody Knows You're a Dog', Computers in Human Behavior, 23(6), 3038–3056, 2007.

81. Owens, T.J., Robinson, D.T., and Smith-Lovin, L. Three faces of identity. Annual Review of Sociology, 36, 477-499, 2010.
82. Reicher, S.D., Spears, R., and Postmes, T. A Social Identity Model of Deindividuation Phenomena. European Review of Social Psychology, 6(1), 161-198, 1995.
83. Jia, H., Chen, Y., Li, Y., Yan, X., Fenlin Liu, F., Luo, X., Wang, B. Attributes revocation through ciphertext puncturation. Journal of Information Security and Applications, 48, 102355, 2019.
84. Nasir, A., Arshah, R.A., Hamid, M.R.A., and Fahmy, S. An analysis on the dimensions of information security culture concept: A review. Journal of Information Security and Applications, 44, 12-22, 2019.
85. Kunz, K., Puchta, A., Groll, S., Fuchs, L., Pernul, G. Attribute quality management for dynamic identity and access management. Journal of Information Security and Applications, 44, 64-79, 2019.
86. Taylor, T.L. Intentional bodies: Virtual environments and the designers who shape them. International Journal of Engineering Education, 19(1), 25-34, 2003.
87. Koole, M. The Web of Identity: Selfhood and Belonging in Online Learning Networks. Proceedings of the 7th International Conference on Networked Learning 2010. Seventh International Conference on Networked Learning 2010, pp. 241-248, 2010.
88. Esparza, J.M. Understanding the credential theft lifecycle. Computer Fraud & Security, 2, 6-9, 2019.
89. Ueda, H., and Nakamura, M. Deployment of Multilanguage Security Awareness Education Online Course by Federated Moodle in Japan. Computer Software and Applications Conference (COMPSAC), 2017 IEEE 41st Annual, 2, IEEE, pp. 49-52, 2017.
90. Hernandez, J.C.G., and Chavez, M.A.L. Moodle security vulnerabilities. 2008 5th International Conference on Electrical Engineering, Computing Science and Automatic Control, IEEE, pp. 352-357, 2008.
91. Manzo, M. A model for users behavior analysis and forecasting in Moodle. Journal of e-Learning and Knowledge Society, 13(2), 129-139, 2017.
92. Fang, B., Ding, J., and Wang, Z. Autonomous robotic exploration based on frontier point optimization and multistep path planning. IEEE Access, 7, 46104 – 46113, 2019.
93. Keidar, M., and Kaminka, G.A. Efficient frontier detection for robot exploration, The International Journal of Robotics Research, 33(2), 215-236, 2014.
94. Krishnamurthi, R., Patan, R., and Gandomi, A.H. Assistive pointer device for limb impaired people: A novel Frontier Point Method for hand movement recognition. Future Generation Computer Systems, 98, 650-659, 2019.
95. Chou, H.L. and Chen, C.H. Beyond Identifying Privacy Issues in E-learning Settings, Computers & Education, 103, 124-133, 2016.
96. Jerman-Blažič, B. and Klobučar, T. Privacy provision in e-learning standardized systems: status and improvements, Computer Standards & Interfaces, 27(6), 561-578, 2005.

97. Plamondon, R. Pirlo, G. Anquetil, É. Rémid, C.. Teulings, H.L and Nakagawa, M. Personal digital bodyguards for e-security, e-learning and e-health: A prospective survey, Pattern Recognition, 81, 633-659, 2018.
98. Miguel, J. Caballé S. and Xhafa, F. Intelligent Data Analysis for e-Learning, Enhancing Security and Trustworthiness in Online Learning Systems Intelligent Data-Centric Systems, Chapter 2 - Security for e-Learning, pp. 7-23, 2017.
99. Miletić, D. Moodle Security. Birmingham – Mumbai, 2011, Packt Publishing.
100. Nieles, M. Dempsey, K. and Pillitteri, V. An Introduction to Information Security, NIST Special Publication 800-12. NIST, 2017.
101. Adejo, O.W. Ewuzie, I. Usoro, A. and Connolly, T. E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastructure. I.J. Information Technology and Computer Science, Modern Education and Computer Science Press, 2018, p.1-9.
102. Shen, R. Wang, M. and Pan, X. Increasing interactivity in blended classrooms through a cutting-edge mobile learning system. British ournal of Educational Technology, 39(6), 1073–1086, 2008.
103. Wu, W.H. Wu, Y.C.J. Chen, C.Y. Kao, H.Y. Lin, C.H. and Huang, S.H. "Review of trend from mobile Learning studies: A meta-analysis". Computers & Education, 59, 817–827, 2012.
104. Danish, J. and Hmelo-Silve, C.E. Contemporary Educational Psychology, On activities and affordances for mobile learning, 60, 101829, 2020.
105. Rodríguez, G.E. Torres, J.G. Flores, P. and Benavides, D.E. Cross-site scripting (XSS) attacks and mitigation: A survey, Computer Networks, 166, 106960, 2020.
106. Al-Fahad, F.N. Students' attitudes and perceptions towards the effectiveness of mobile learning in King Saud University, Saudi Arabia, The Turkish Online Journal of Educational Technology, 8(2), 111-119, 2009 .
107. Čagalj, M. Perković, T, Bugarić, M. and Li, S. Fortune cookies and smartphones: Weakly unrelayable channels to counter relay attacks, Pervasive and Mobile Computing, 20, 64-81, 2015.
108. Takahashi, H. Yasunaga, K. Mambo, M. Kim, K. and Youm, H.Y. Preventing abuse of cookies stolen by XSS, 2013 Eighth Asia Joint Conference on Information Security, 2013, pp. 85-89.
109. Murdoch, S.J. Hardened stateless session cookies, B. Christianson, J.A. Malcolm, V. Matyas, M. Roe (Eds.), Security Protocols XVI, Springer Berlin Heidelberg, Berlin, Heidelberg (2011), pp. 93-101.
110. Mundada, Y. Feamster, N. and Krishnamurthy, B. Half-baked cookies: hardening cookie-based authentication for the modern web, Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ASIA CCS '16 (2016), pp. 675-685.
111. O'Gorman, L.: Comparing passwords, Tokens, and Biometric for User Authentication", In Proc. of IEEE, 91, pp. 2019-2040, 2003.
112. Vapen, A. and Shahmehri, N. Security levels for Web Authentication using Mobile Phones. *Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology*, Springer Heidelberg, 352, pp. 130-143, 2011.

113. Kartakis, S. and Stephanidis, C.A. Design-and-play approach to accessible user interface development in ambient intelligence environments. *Computers in Industry*, Elsevier, 61, 318-328, 2010.
114. Billi, M., Burzagli, L., Catarci, T., Santucci, G., Bertini, E, Gabbanini, F., Palchetti, E., 2010. A unified methodology for the evaluation of accessibility and usability of mobile applications. Universal Access in the Information Society, 9(4), 337-356.
115. Mourouzis, A., Antona, M., Stephanidis, C., 2011. A diversity-sensitive evaluation method. Universal Access in the Information Society, 10(3), 337-356.
116. Crawford, H., Renaud, K. and Storer, T. A framework for continuous, transparent mobile device authentication. *Computers & Security*, Elsevier, 39, 127-136, 2013.
117. Fuglerud, K.S. and Røssvoll, T.H. An evaluation of web-based voting usability and accessibility. *Universal Access in the Information Society*, Springer Heidelberg, 11, 359-373, 2012.
118. Grudin, J. Utility and usability: research issues and development contexts. *Interact. Comput*. Elsevier, 4, 209-217, 1992.
119. Pribeanu, C., Neszly, P.F. and Patru A. Municipal web sites accessibility and usability for blind users: preliminary results from a pilot study. *Universal Access in the Information Society*. Springer Heidelberg, 13, 339-349, 2014. doi: 10.1007/s10209-013-0315-2.
120. Helkala, K. and Snekkenes, E. A Method for Ranking Authentication Products. Proceedings of the Second International Symposium on Human Aspects of Information Security and Assurance, HAISA, 2008.
121. Burr, W.E., Dodson, D.F. and Polk, W.T. Electronic authentication guideline. *Technical Report 800-63, National Institute of Standards and Technology*, 2008. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf. Accessed 15 May 2017.
122. Pond, R., Podd, J., Bunnell, J. and Henderson, R. Word Association Computer Passwords: The Effect of Formulation Techniques on Recall and Guessing Rates, *Computers & Security*, 19, 645-656, 2000.
123. Husemann, D. The smart card: don't leave home without it, IEEE Concurrency, 7, pp 24-27, 1999.
124. Abott, J. Smart cards: How secure are they. www.sans.org/reading_room/ whitepapers/authentication/131.php, 2003. (Accessed 30 may 2017).
125. Phillips, P.J., Moon, H., Rizvi, S.A. and Rauss, P.J. The FERET Evaluation Methodology for Face-Recognition algorithms, Trans. on pattern analysis and machine intelligence, 22, 1090-1104, 2000.
126. Maio, D., Maltoni, D., Cappelli, R., Wayman J. and Jain, A. FVC2000: Fingerprint Verification Competition, Trans. on pattern analysis and machine int., 24, pp. 402-412, 2002.
127. Mansfield, A. and Wayman, J. Best practices in Testing and Reporting Performance of Biometric Devices, NPL Report CMSC 14/02, Version 2.01., 2002.
128. Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S. *Handbook of Fingerprint Recognition, cap.1*, New York, 2003.
129. Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S. Handbook of Fingerprint Recognition. Second Edition, Springer Verlag, London, Limited, 2009.

130. Karovaliya, M., Karedia, S., Oza, S. and Kalbande, D.R. Enhanced security for ATM machine with OTP and Facial recognition features. Procedia Computer Science, 45, 390-396, 2015.
131. Clarke, N.L. and Furnell, S.M. Advanced user authentication for mobile devices. *Computers & Security* Elsevier, 26, 109-119, 2007.
132. Clarke, N.L., Furnell, S.M., 2005. Authentication of users on mobile telephones - a survey of attitudes and practices. Computers & Security, 24(7), 519-527.
133. Coskun, V., Ozdenizci, B., Ok, K., 2013. A Survey on Near Field Communication (NFC) Technology. Wireless Personal Communications, 71(3), 2259-2294.
134. Ogbanufe, O., Kim, D.J., 2017. Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems, https://doi.org/10.1016/j.dss.2017.11.003
135. Renaud, K. Quantifying the quality of web authentication mechanisms: A usability perspective, J. Web Eng. 3(2), 95–123, 2004.
136. Mihajlov, M., Jerman-Blazic, B. and Josimovski, S. A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives, in: 2011 5th International Conference on Network and System Security, NSS, pp. 332–336, 2011a.
137. Mihajlov, M., Blazic, B., Josimovski, S. Quantifying usability and security in authentication, in: 2011 IEEE 35th Annual Computer Software and Applications Conference, COMPSAC, pp. 626–629, 2011b.
138. FIDO standard 2018. Available on: https://fidoalliance.org/aetna-deploys-fido-authentication/
139. Zhou, L., Kang, Y., Zhang, D. and Lai, J. Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones, Decision Support Systems, 2016. DOI:10.1016/j.dss.2016.09.007
140. Hydara, I., Sultan, A.B., Zulzalil, H. and Novia Admodisastro, A. Current state of research on cross-site scripting (XSS) – A systematic literature review, Information and Software Technology 58, 170–186, 2015.
141. Chen X., Li M., Jiang Y., Sun Y. A Comparison of Machine Learning Algorithms for Detecting XSS Attacks. In: Sun X., Pan Z., Bertino E. (eds) Artificial Intelligence and Security. ICAIS 2019. Lecture Notes in Computer Science, vol 11635., 2019, Springer, Cham.
142. Kazemian, H.B., Ahmed, S.: Comparisons of machine learning techniques for detecting malicious webpages. Expert Syst. Appl. 42(3), 1166–1177, 2015.
143. Shanmugasundaram, G. Ravivarman, S. and Thangavellu. P. 2015. A study on removal techniques of cross-site scripting from web applications. In 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), 0436–0442. doi: 10.1109/ICCPEIC.2015.7259498.
144. Deepa, G. and Thilagam, P.S.. Securing web applications from injection and logic vulnerabilities: Approaches and challenges. Information and Software Technology, 74, pp. 160-180, 2016.
145. Csontos, B., Heckl, I. 2020. Accessibility, usability, and security evaluation of Hungarian government

websites. Univ Access Inf Soc. https://doi.org/10.1007/s10209-020-00716-9.

146. Wang, R. Xu, G. Zeng, X., Li, X., Feng, Z. TT-XSS: A novel taint tracking based dynamic detection framework for DOM Cross-Site Scripting, Journal of Parallel and Distributed Computing, 118(1), 100-106, 2018.
147. Line, M.B., Nordland, O., Røstad, L., Tøndel, I.A. SAFETY VS. SECURITY? Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management May 14-18, 2006, Management (PSAM), ASME Press, New Orleans.
148. Kissel R.L. Glossary of Key Information Security Terms. NIST Interagency/Internal Report (NISTIR) 2013.
149. Whitman, M.E. and Mattord H.J. Principles of Information Security Fourth Edition, Boston, MA, Course Technology, 2012.
150. Maconachy, W.V., Schou C.D., Ragsdale, D. and Welch, D.A Model for Information Assurance: An Integrated Approach. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June.
151. Krause, M. and Tipton, H.F. Handbook of Information Security Management. CRC Press LLC 1998.
152. Krause, M. and Tipton, H.F. Handbook of Information Security Management, fifth edition. CRC Press LLC 2004.
153. Murphy, G.B. Systems Security Certified Practitioner Study Guide, Indianapolis, Indiana, John Wiley & Sons, Inc., 2015.
154. Harris, S. and Maymí, F. Cissp All-In-One Exam Guide, Seventh Edition (Hardcover), New York Mcgraw-Hill, 2016.
155. Hansche, S., Berti, J., Hare, C. Official (ISC)² guide to the CISSP exam, Boca Raton, Fl, Auerbach Publications, 2003.
156. Tudor, J.K. Information security architecture: an integrated approach to security in the organization. Boca New York Washington, D.C by CRC Press LLC, 2001.
157. Memon, I., Mohammed, M.R., Akhtar, R., Memon, H., Memon, M.H. and Shaikh, R.A., Design and Implementation to Authentication over a GSM System Using Certificate-Less Public Key Cryptography (CL-PKC). *Wireless Personal Communications*, Springer US, 79, 661-686, 2014. doi: 10.1007/s11277-014-1879-8.
158. ISO 9241. *Ergonomics Requirements for Office Work with Visual Display Terminals (VDTs) International Standards Organisation,* Geneva, 1997.
159. Nielsen, J. Usability engineering. *Morgan Kaufmann Pub*., 1994.
160. Harrison, R., Flood, D. and Duce, D. Usability of mobile applications. Literature review and rationale for a new usability model Wireless. *Journal of Interaction Science*, Springer, 1-16, 2013. doi: 10.1186/2194-0827-1-1.
161. Bevan, N. Classifying and selecting UX and usability measures. *In the Proceedings of Meaningful Measures: Valid Useful User Experience Measurement (VUUM), 5th COST294-MAUSE Open*

Workshop, Reykjavik, Iceland, 2008.

162. Miao, M., Pham, H.A., Friebe, J. and Weber, G. Contrasting usability evaluation methods with blind users. *Universal Access in the Information Society*, Springer Heidelberg, 2014. doi: 10.1007/s10209-014-0378-8.
163. Parhi, P., Karlson, A.K. and Bederson, B.B. Target size study for one-handed thumb use on small touch screen devices. *In: Proceedings of the 8th Conference on Human–Computer Interaction with Mobile Devices and Services*, New York, NY, USA, MobileHCI' 06, ACM, pp. 203-210, 2006.
164. Zhou, J., Rau, P.L.P. and Salvendy, G. Age-related difference in the use of mobile phones. *Universal Access in the Information Society*, Springer Heidelberg, 13, 401-413, 2014. doi: 10.1007/s10209-013-0324-1.
165. Bevan, N. European Usability Support Centres: Support for a More Usable Information Society. *Proceedings of TAP Annual Concertation Meeting*, Barcelona, 1998.
166. Bevan, N. Claridge, N. and Petrie, H. Tenuta: simplified guidance for usability and accessibility. *In: Proceedings of HCI International 2005*, Las Vegas, 2005.
167. Weir, C.S., Douglas, G., Carruthers, M. and Jack, M. User perceptions of security, convenience and usability for eBanking authentication tokens. *Computers & Security*, Elsevier, 28, 47-62, 2009.
168. Weir, C.S., Douglas, G., Richardson, T. and Jack, M. "Usable security: user preferences for authentication methods in eBanking and the effects of experience." *Computers & Security*, Elsevier, 22, 153-164, 2010.
169. Thatcher, J., Waddell, C.D., Henry, S.L., Swierenga, S., Urban, M.D., Burks, M., Regan, B. and Bohman, P. *Constructing Accessible Web Sites*. Glasshaus, San Francisco, 2003.
170. Galvez, R.A. and Youngblood, N.E. e-Government in Rhode Island: what effects do templates have on usability, accessibility, and mobile readiness? *Universal Access in the Information Society*, Springer, Heidelberg 2014. doi: 10.1007/s10209-014-0384-x.
171. Calvo, R., Iglesias, A. and Moreno, L. Accessibility barriers for users of screen readers in the Moodle learning content management system. *Universal Access in the Information Society*, Springer Heidelberg, 13, 315-327, 2014.
172. Emiliani, P.L. and Stephanidis, C. *Universal access to ambient intelligence environments: Opportunities and challenges for people with disabilities*, IBM Sys, 44, 2005.
173. Gajos, K.Z., Wobbrock, J.O. and Weld, D.S. Automatically generating user interfaces adapted to users' motor and vision capabilities. In: *UIST'07: Proceedings of the 20th Annual ACM Symposium on User Interface Software and Technology*, ACM, New York, pp. 231–240, 2007.
174. Stephanidis, C. and Savidis, A. Universal access in the information society: methods, tools and interaction technologies. *Universal Access in the Information Society*, Springer Heidelberg, 1, 40-55, 2001.
175. Shaikh, A. and Karjaluoto, H. Mobile banking adoption: A literature review. *Telematics and Informatics*, Elsevier, 32, 129-142, 2015.

176. Baseri, Y., Hafid, A. and Cherkaoui, S. Privacy preserving fine-grained location-based access control for mobile cloud, *Computers & Security*, Elsevier, 73, 249-265, 2018.
177. Ntalkos, L., Kambourakis, G. and Damopoulos, D. Let's Meet! A participatory-based discovery and rendezvous mobile marketing framework, *Telematics and Informatics*, Elsevier, 32, 539-563, 2015.
178. Bettini, C. and Riboni, D. Privacy Protection in Pervasive Systems: State of the Art and Technical Challenges. *Pervasive and Mobile Computing*; Elsevier, 17, 159-174. 2015.
179. Veeningen, M., Weger, B. and Zannone, N. *Data minimisation in Communication protocols: A Formal Privacy Analysis of Identity Management Systems*. International Journal of Information Security, Springer Verlag, 1-52, 2013.
180. Korać, D. Damjanović, B. and Simić, D. Information security in m-learning systems: Challenges and Threats of using Cookies. 19th International Symposium INFOTEH-JAHORINA, 18-20 March 2020, IEEE.
181. Jiang, L., Jiang, N. and Liu, S. Consumer Perceptions of E-Service Convenience: An Exploratory Study. Procedia Environmental Sciences, 11, 406-410, 2011.
182. Dabholkar, P.A., Bobbitt, L.M. and Lee, E.J. Understanding consumer motivation and behavior related to self-scanning in retailing: implications for strategy and research on technology-based self-service, International Journal of Service Industry Management, 14(1), 59-95, 2003.
183. H. Shahriar and M. Zulkernine, 2012. Mitigating program security vulnerabilities: Approaches and challenges, ACM Comput. Surv. 44 (3), Article No.11.
184. G. Popescu, A. Pupescu and C.R. Pupescu 2008. Conducting an Information Security Audit, IT Information Technology Manager No.7.
185. Korać, D. and Simić, D. Digital Identity in Identity Management Models. Proceeding of the 2014 International Conference on ICT Conference and Exibition, Aranđelovac, InfoTech 2014.
186. Nuñez, D. and Agudo, I. BlindIdM: A privacy-preserving approach for identity management as a service. *International Journal of Information Security*, Springer Berlin Heidelberg, 13(2), 199-215, 2014.
187. Noëmi Manders-Huits. *Practical versus moral identities in identity management*. Ethics and Information Technology. Springer Netherlands 12(1), 43-55, 2010.
188. Wood, P. Implementing identity management security-an ethical hacker's view, *Network security*, 9, 12-15, 2005.
189. Sullivan, C. Digital Identity: An Emergent Legal Concept. University of Adelaide Press, 2011.
190. Dehing, A.J.M., Baartman, L.K.G. and Jochems, W.M.G., (2011). Mechanisms of students' engineering identity development during workplace learning in the bachelor curriculum. *WEE2011, September 27-30*, 2011, Lisbon, Portugal. Retrieved from http://www.sefi.be/wp-content/papers2011/T7/99.pdf

191. Pfitzman, A. and Hansen, M. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, v0.34. 2010.
192. Hansenu, M., Pfitzmannb, A., and Steinbrecherb, S. Identity management throughout one's whole life. Information Security Technical Report, 13(2), 83–94, 2008.
193. Damiani, E., Vimercati, C.S. and Samarati, P. Managing multiple and dependable identities. *IEEE Internet Computing*, 7(6), 29–37, 2003. doi: 10.1109/MIC.2003.1250581
194. Afzal, M.T., Kulathuramaiyer, N. and Maurer, H. Creating Links into the Future. *Journal of Universal Computer Science,* 13(9), 1234-1245, 2007.
195. Goodstadt, L.F., Connolly, R. and Bannister, F. The Hong Kong e-Identity Card: Examining the Reasons for Its Success When Other Cards Continue to Struggle. *Information Systems Management*, 32(1), 72-80, 2015.
196. Danner, P. and Hein, D.A. Trusted Computing Identity Collation Protocol to Simplify Deployment of New Disaster Response Devices. *Journal of Universal Computer Science,* 16(9), 1139-1151, 2010.
197. Jøsang, A., AlZomai, M. and Suriadi, S. Usability and privacy in identity management architectures. In Proceding Fifth *Australasian Information Security Workshop: Privacy enhancing technologies (AISW 2007), Ballarat, Australia, 2007,* CRPIT, (vol. 68, pp. 143-152x). Australian Computer Society Inc., 2007.
198. Aresta, M., Pedro, L., Santos, C. and Moreira, A. Online identity analysis model. *International Journal of Knowledge Society Research,* 4(3), 89-102, 2013.
199. Guo, L., Zhang, C., F, Y. and Lin, P. A Privacy-Preserving Attribute-Based Reputation System in Online Social Networks. Journal of Computer Science and Technology 30(3), 578–597, 2015. doi: 10.1007/S11390-015-1547-9
200. Vacca, J.R. Computer and Information Security Handbook. Morgan Kaufmann Publishers is an imprint of Elsevier, Burlington, MA 01803, USA, 2009.
201. Prasad, G. and Rajbhandari, U. "Identity Management on a Shoestring", 2011, Available on: http://www.infoq.com/min/books/Identity-Management-Shoestring.
202. Kent, S.T. and Millett, L.I. *Who Goes There? Authentication Through the Lens of Privacy*, The National Academies Press, Washington, D.C., 2003.
203. Korać, D. and Simić, D. A. Survey of Authentication Methods for Mobile Devices. Proceeding of the 2013 International Conference on ICT Conference and Exibition, Aranđelovac, InfoTech 2013.
204. Stewart, J.M., Tittel, E. and Chapple, M. CISSP: Certified Information Systems Security Professional Study Guide. Wiley publishing, Inc., Canada, 2008.
205. Wong, R., Berson, T. and Feiertag, R. *Polonius: an identity authentication system*, Proceedings of the 1985 IEEE Symposium on Security and Privacy, pp. 101-107, 1985. Available on: http://www.anagram.com/berson/abspolo.html

206. MeT: *Personal Transaction Protocol Version 1.0*, Draft Specification 01-11-2002, Mobile Electronic Transactions Ltd, 2002.
207. Palfrey, J. and Gasser, U. Digital Identity Ineroperability and eInnovation, case study Berkman Publication Series, 2007.
208. Alpár, G., Hoepman, J.H. and Siljee, J. The identity crisis. Security, privacy and usability issues in identity management. *Computer Research Repository (CoRR)*, 2011.
209. Zwattendorfer, B., Stranacher, K. and Tauber, A. Towards a Federated Identity as a Service Model, *Technology-Enabled Innovation for Democracy, Government and Governance Lecture Notes in Computer Science*, 8061, 43-57, 2013.
210. Gopalakrishnan, A. Cloud Computing Identity Management. *SET Labs Briefings*, 7(7), 45-55, 2009.
211. Zwattendorfer, B., Zefferer, T. and Stranacher, K. An Overview of Cloud Identity Management-Models. *10th International Conference on Web Information Systems and Technologies (WEBIST)*, pp. 82-92, 2014.
212. RFC 2693-SPKI Certification Theory - IETF, 1999. Available on: www.ietf.org/rfc/rfc2693.txt
213. Miyata, T., Koga, Y., Madsen, P., Adachi, S.I., Tsuchiya, Y., Sakamoto, Y. and Takahashi, K. "Asurvey on identity management protocols and standards" IEICE TRANS. INF and SYST 2006.
214. Wiedenbeck, S., Waters, J., Sobrado, L. and Birget, J. Design and evaluation of a shoulder-surfing resistant graphical password scheme. *In Proceedings of the working conference on advanced visual interfaces*, ACM pp. 177–184, 2006.
215. Hayday, G. Security nightmare: How do you maintain 21 different passwords. http://tinyurl.com/ silicon-security nightmare.
216. Yan, J., Blackwell, A., Anderson, R. and Grant, A. Password Memorability and Security: Empirical Results. *IEEE Security and Privacy*, 2004.
217. Bonneau, J. Measuring Password Reuse Empirically, February 2011.
218. Corella, F. and Lewison, K.A Comprehensive Approach to Cryptographic and Biometric Authentication from a Mobile Perspective. 2013. Available on: http://pomcor.com/whitepapers/CryptographicAuthentication.pdf
219. Monisha, G., Prabhu, B.B. and Kumar, B.B. Secured Android Mobile Authentication. *International Journal of Research in Engineering and Advanced Technology*, 1(1), 1-7, 2013.
220. Strong password generator 2018. Available on: https://strongpasswordgenerator.com/
221. 10 Most Popular Password Cracking Tools 2018. Available on: http://resources.infosecinstitute.com/10-popular-password-cracking-tools/
222. Dunphy, P., Heiner, A.P. and Asokan, N. A closer look at recognition-based graphical passwords on mobile devices. *In: Proceedings of the 6th symposium on usable privacy and security*, pp. 26-38, 2010.
223. Zezschwitz, E.V., Koslow, A., Luca, A.D. and Hussmann, H. *Making Graphic-Based Authentication Secure against Smudge Attacks.* IUI13, March 19–22, pp.277-278, 2013.
224. Jiang, W., lI, H., Hu, G., Wen, M., Dong, G. and Lin, X. PTAS: Privacy-preserving Thin-client

Authentication Scheme in blockchain-based PKI. Future Generation Computer Systems, 96, 185-195, 2019.

225. Schneier, B. Biometrics: truths and fictions, Available on: http://www.schneier.com/crypto-gram-9808.html

226. Sheeba, T. and Bernard, M.J. *Survey on Multimodal Biometric Authentication Combining Fingerprint and Finger vein.* International Journal of Computer Applications (0975 – 8887) volume 51, 2012.

227. Stockinger, T. *Implicit Authentication on Mobile Devices.* Media Informatics Advanced Seminar on Ubiquitous Computing, 2011.

228. Bayly, D., Castro, M., Arakala, A., Jeffers, J. and Horadam, K. Fractional biometrics: safeguarding privacy in biometric applications. *International Journal of Information Security*, Springer Heidelberg, 9, 69-82, 2010. doi: 10.1007/s10207-009-0096-z

229. Damousis, I., Tzovaras, D. and Bekiaris, E. *Unobtrusive multimodal biometric authentication: The humabio project concept.* EURASIP journal on advances in signal processing, 1–11, 2008.

230. Clarke, N., Furnell, S. and Reynolds, P. Biometric authentication for mobile devices. In: *Proceedings of the 3rd Australian Information warfare and security conference*, pp. 61- 69, 2002.

231. Furnell, S., Clarke, N. and Karatzouni, S. Beyond the PIN: Enhancing user authentication for mobile devices. *Computer Fraud and Security*, Elsevier, 12-17, 2008.

232. Tao, Q. and Veldhuis, R. *Biometric Authentification System on Mobile Personal Devices.* IEEE transaction on instrumentation and measurement, 59(4), 2010.

233. Wayman, J., Jain, A., Maltoni, D. and Maio, D. Introduction to Biometric Authentication Systems, Chapter, *Biometric Systems*, Springer London, pp. 1-20, 2005. doi: 10.1007/1-84628-064-8_1

234. Tulyakov, S. Farooq, F., Mansukhani, P. and Govindaraju, V. *Symmetric hash functions for secure fingerprint biometric systems. Pattern Recognition Letters*, 28(16), 2427–2436, 2007.

235. Adibi, S. A low overhead scaled equalized harmonic-based voice authentication system. Telematics and Informatics: An Interdisciplinary Journal on the Social Impacts of New Technologies, 31(1), 137-152, 2014.

236. Iwano, K., Hirose, T., Kamibayashi, E. and Furui, S. Audio-visual person authentication using Speech and Ear images. In: *Proceedings of workshop on multimodal user authentication*, 85-90, 2003.

237. Woo, R.H., Parkm, A. and Hazen, T.J. The MIT mobile device speaker verification corpus: data collection and preliminary experiments. In: *IEEE workshop on speaker and language recognition*, pp. 1-6, 2006.

238. Brunelli, R. and Falavigna, D. Person identification using multiple cues. *IEEE Transactions on pattern analysis and machine intelligence,* 17, 955-966, 1995.

239. Bodei, C., Degano, P., Focardi, R. and Priami, C. Authentication via localized names, in: *Proc. CSFW'99, New York,* IEEE Press, pp. 98–110, 1999.

240. Bowyer, K.W., Baker, S.E., Hentz, A, Hollingsworth, K., Peters, T. and Flynn, P.J. Factors that degrade the match distribution in iris biometrics. *Identity in the Information Society*, 2, 327-343, 2009.

241. Wildes, R.P. Iris recognition: An emerging biometric technology, Proceedings of the IEEE, 85, pp. 1348-1363, 1997.
242. Monrose, F. and Rubin, A. “Authentication via Keystroke Dynamics”, *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pp. 48-56, 1997.
243. Clarke, N.L. and Furnell, S.M. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*, Springer Heidelberg, 6, 1-14, 2007.
244. Kambourakis, G., Damopoulos, D., Papamartzivanos, D. and Pavlidakis, M. Introducing Touchstroke: Keystroke-based Authentication System for Smartphones. *Security and Communication Networks*, Wiley Online Library, 5, 3-14, 2014.
245. Yu, E. and Cho, S. Keystroke dynamics identity verification-its problems and practical solutions. *Computers & Security*, Elsevier, 23, 428-440, 2004.
246. Buchoux, A. and Clarke, N. Deployment of keystroke analysis on a smartphone. In: *Proceedings of the 6th Australian information security management conference*, pp. 40-47, 2008.
247. Saevanee, H. and Bhattarakosol, P. Authenticating user using keystroke dynamics and finger pressure. In: *Proceedings of the 6th IEEE consumer communications and networking conference*, pp. 1-2, 2009.
248. Maiorana, E., Campisi, P., Carballo, N.G. and Neri, A. Keystroke Dynamics Authentication for Mobile Phones. SAC '11 *Proceedings of the 2011 ACM Symposium on Applied Computing*, pp. 21-26, 2011.
249. Monrose, F. and Rubin, A.D. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, Elsevier, 16, 351–359, 2000.
250. Incel, O.D., Kose, M. and Ersoy, C. A Review and Taxonomy of Activity Recognition on Mobile Phones. BioNanoScience, 3(2), 145-171, 2013.
251. Ailisto, H.J., Lindholm, M., Mantyjarvi, J., Vildjiounaite, E. and Makela, S.M. Identifying people from gait pattern with accelerometers. In*: Proceedings of the SPIE 5779, Biometric Technology for Human Identification II*, Orlando 7, pp. 7–14, 2005.
252. Gafurov, D., Helkala, K. and Soendrol, T. Gait recognition using acceleration from mems. In: *The first international conference on availability, reliability and security*. IEEE 2006.
253. Bujari, A., Licar, B. and Palazzi, C.E. Movement pattern recognition through smartphone’s accelerometer. In: *Consumer communications and networking conference (CCNC)*, IEEE, pp. 502-506, 2012.
254. Derawi, M. and Bours, P. Gait and activity recognition using commercial phones. *Computers & Security*, Elsevier, 39, 137-144, 2013.
255. Frank, J., Mannor, S. and Precup, D. Activity and gait recognition with time-delay embeddings. In: *Proceedings of the twenty-fourth AAAI conference on artificial intelligence*, pp. 1-6, 2010.
256. He, Z. and Jin, L. Activity recognition from acceleration data based on discrete consine transform and SVM. In: *IEEE international conference on systems, man and cybernetics*, pp. 5041 – 5044, 2009.
257. Kwapisz, J.R., Weiss, G.M. and Moore, S.A. Activity recognition using cell phone accelerometers. *SIGKDD Explorations Newsletter*, 12, pp. 74-82, 2010.

258. Liu, Z, and Sarkar, S. Improved gait recognition by gait dynamics normalization. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 28, 863–876, 2006.

259. Han, J. and Bhanu, B. Individual recognition using gait energy image. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28, 316–322, 2006.

260. Derawi, M., Nickel, C., Bours, P. and Busch, C. Unobtrusive user authentication on mobile phones using biometric gait recognition. *In: Sixth international conference on intelligent information hiding and multimedia signal processing 2010*, IEEE Computer Society Washington, DC, USA, pp. 306-311, 2010.

261. Gafurov, D, Snekkenes, E. and Bours, P. Gait authentication and identification using wearable accelerometer sensor. *In 2007 IEEE Workshop on Automatic Identification Advanced Technologies*, pp. 220–225, 2007.

262. Cappelli, R., Ferrara, M., Franco, A. and Maltoni, D. Fingerprint verification competition 2006. *Biometric Technology Today*, 15, 7-9, 2007.

263. Mjaaland, B.B., Bours, P. and Gligoroski, D. Walk the walk: attacking gait biometrics by imitation. In: *Proceedings of the 13th international conference on information security*, pp. 361-380, 2011.

264. Braghin, C., Sharygina, N. and Barone-Adesi, K. A Model Checking-based Approach for Security Policy Verification of Mobile Systems. *Formal Aspects of Computing*, 23(5), 627-648, 2010.

265. Krause, M. and Tipton, H.F. Handbook of Information Security Management, fifth edition, vol.2, Taylor & Francis Group, 2005.

266. Stamp, M. Information Security Principles and practice. John Wiley & Sons, Inc., Hoboken, New Jersey. 2006.

267. Bishop, M. Computer Security: Art and Science, Addison Wesley, Boston, MA. 2003.

268. Castano, S., Fugini, M., Martella, G. and Samarati, P. Database Security, Addison Wesley, Harlow, England, 1995.

269. Therialut, M., and Newman, A. Oracle Security Handbook: Implementing a Sound Security-Plan in Your Oracle Environment. McGraw-Hill, Berkeley, CA. 2001.

270. Qingguang, J., Sihan, Q. and Yeping, H. A formal model for integrity protection based on DTE technique, Science in China Series F: Information Sciences 49, pp. 545-565, 2006.

271. Paci, F., Bauer, D., Bertino, E., Blough.D., Squicciarini, A. and Gupta, A. Minimal credential disclosure in trust negotiations. Identity in the Information Society, 2009.

272. Jensen, J. Identity management Lifecycle – Exemplifying the need for holistic Identity assurance frameworks. Information and Communication technology. Springer, 7804, 343 – 352, 2013.

273. Myers, M., Ankney, R., Malpani, A., Galperin, S. and Adams, C. "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP," IETF, RFC 2560, 1999.

274. Fournier-Bonilla, S.D., Watson, K., Malaveâ, C. and Froyd, J. Managing Curricula Change in Engineering at Texas A & M University, *International Journal of Engineering Education*, 17(3), 222-235, 2001.

275. OWASP Risk Rating Methodology, 2018. Available on: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.
276. Korać, D. A Comprehensive Overview and Comparison of Contemporary User Authentication Methods for Mobile Devices. *Info M*, FON, 53(2), 48-54, 2015.
277. Mamdani, E. and Assilian, S. An Experiment in Linguistic Synthesis with a Fuzzy Logic Controller. *International Journal of Man-Machine Studies*, 7(1), 1-13, 1975.
278. Mount, C. and Liao, T.W. Prototype of an intelligent failure analysis system, in Proceedings of the 4th International Conference on Case-Based Reasoning (ICCBR '01), Vancouver, BC, Canada, pp. 716–731, 2001.
279. Peng, Z. and Iwamura, K. A Sufficient and Necessary Condition of Uncertainty Distribution. *Journal of Interdisciplinary Mahematics*, 13(3); 277-285, 2013.
280. Monrose, F., Reiter, M.K. and Wetzel, S. Password hardening based on keystroke dynamics. *International Journal of Information Security*, Springer Verlag, 1(2), 69–83, 2001.
281. Gunson, N., Marshall, D., Morton, H. and Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, 30(4), 208–220, 2011.
282. Go, W., Lee, K. and Kwak, J. Construction of a secure two-factor user authentication system using fingerprint information and password. *Journal Intelligent. Manufacturing*, 25, 217–230, 2014.
283. Cha, B.R., Kim, Y.I. and Kim, W.J. Design of new P2P-enabled Mobile-OTP system using fingerprint features. *Telecommunication Systems*, 52(4), 2221-2236, 2013.
284. Tresadern, P., Cootes, T.F., Poh, N., Matejka, P., Hadid, A., Levy, C., McCool, C. and Marcel, S. Mobile biometrics: combined face and voice verification for a mobile platform, IEEE Pervasive Computation, 12(1), 79-87, 2013.
285. Kang, J., Nyang, D.H. and Lee, K.H. Two-factor face authentication using matrix permutation transformation and a user password, Information Sciences, 269, 1-20, 2014.
286. DeMarsico, M.,Galdi, C.,Nappi, M. and Riccio, D. FIRME: face and iris recognition for mobile engagement, Image and Vision Computing, 32(12), 1161-1172, 2014.
287. Shute, J. and User, I.D. A Novel of identity Theft. Mariner Books, 2006
288. Marcus, R. and Hasting, G. Identity Theft, inc. Disinformation Company, 2006.
289. Zalud, B. ID Theft tops fraud list again ABA Bank Compliance, 2, p. 5-6, 2003.
290. Putthacharoen, R. and Bunyatnoparat, P. Protecting cookies from Cross Site Script attacks using Dynamic Cookies Rewriting technique, Advanced Communication Technology (ICACT), 2011 13th International Conference on, Seoul, pp. 1090-1094, 2011.
291. Bherde, G. P. and Pund, M.A.. Recent attack prevention techniques in web service applications. In 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 1174–1180, 2016. doi: 10.1109/ICACDOT.2016.7877771.

292. Korać, D., Damjanović, B. & Simić, D. Exploring challenges and threats of XSS attacks. *Info M*, FON, 19(72), 12-18, 2020.
293. Snyder C, Myer T, Southwell M, (2010) Pro PHP Security: From Application Security Principles to the Implementation of XSS Defenses, Second Edition, apress.
294. Vallabhaneni SR, (2019) Business Knowledge for Internal Auditing, pp. 1104, Wiley
295. Y. Zhou, P. Wang, An ensemble learning approach for XSS attack detection with domain knowledge and threat intelligence. Computers & Security, 82 (2019) 261-269.
296. Acunetix, Cross-site Scripting (XSS) (2020). https://www.acunetix.com/acunetix-web-application-vulnerability-report-2019/.
297. Gupta S, Gupta BB, (2019) Evaluation and monitoring of XSS defensive solutions: a survey, open research issues and future directions. J Ambient Intell Human Comput, 10: 4377-4405.
298. Korać, D., Damjanović, B., Simić, D. & Choo, KKR. A hybrid XSS attack (HYXSSA) based on fusion approach: Challenges, threats and implications in cybersecurity. *Journal of King Saud University - Computer and Information Sciences*, https://doi.org/10.1016/j.jksuci.2022.09.008.
299. Thames, J.L. Comparing Cross-site Scripting Vulnerabilities. Vulnerability and Exposure Research Team Tripwire, Inc. 2015. DOI: 10.13140/RG.2.1.1488.2725
300. Mitropoulos, D., Louridas, P., Polychronakis, M. and Keromytis, A.D. Defending Against Web Application Attacks: Approaches, Challenges and Implications, in IEEE Transactions on Dependable and Secure Computing, 16 (2), pp. 188-203, 2019.
301. Preventing XSS, 2020. available at: https://excess-xss.com/ (Accessed July 2020).
302. Coker, G., Guttman, J., Loscocco, P., Sheehy, J., Sniffen, B. Attestation: Evidence and trust, in: ICICS'08, 2008, pp.1–18.
303. Thomé, J. Shar, L. K. Bianculli D. and Briand, L.. Security slicing for auditing common injection vulnerabilities. Journal of Systems and Software, 137, 766-783, 2018.
304. Tehranipoor, M. and Wang, C. Introduction to Hardware Security and Trust, Springer, 2011.
305. Lekies, S., Kotowicz, K., Groÿ, S. Nava, E.A.V. and Johns, M. Codereuse attacks for theWeb, in Proc. ACMSIGSAC Conf. Comput. Commun. Secur., Oct./Nov. 2017, pp. 1709-1723.
306. Murphree, J. Machine learning anomaly detection in large systems, in *Proc. IEEE AUTOTESTCON*, Sep. 2016, pp. 1-9.
307. Abeshu, A. and Chilamkurti, N. Deep learning: The frontier for distributed attack detection in fog-to-things computing, IEEE Commun. Mag., 56(2), 169-175, 2018.
308. Fang, Y., Li, Y., Liu, L. and Huang, C. DeepXSS: Cross site scripting detection based on deep learning, in Proc. Int. Conf. Comput. Artif. Intell., Mar. 2018, pp. 47-51.
309. Arias-Cabarcos, P., Almenárez-Mendoza, F., Marin-López, A., Diaz-Sánchez, D. and Sánchez-Guerrero, R. A Metric-Based Approach to Assess Risk for ''On Cloud'' Federated Identity Management. *Journal of Network and Systems Management*, Springer US, 20(4), 513-533, 2012.

Dragan (Milan) Korać je doktorirao 2018. godine na Fakultetu organizacionih nauka (FON), Univerzitet u Beogradu, Srbija. Trenutno je angažovan kao docent na Katedri za matematiku i informatiku, Prirodno-matematičkom fakultetu, Univerziteta Banjaluci, Republika Srpska, Bosna i Herzegovina. Glavna istraživačka interesovanja su zaštita, sajber zaštita, zaštita informacija u računarskim sistemima i fazi logika. Tokom svog dosadašnjeg naučno-istraživačkog rada, u svojstvu prvog autora objavio je 15 radova, od kojih su nekoliko publikovani u najprestižnijim časopisima na SCI listi, kao i brojnim konferencijama održanim kod nas i u inostranstvu. Na kraju potrebno je istaknuti da se radi o bivšem dugogodišnjem vrhunskom sportisti, karatisti osvajaču mnogih evropskih odličja.

CIP - Каталогизација у публикацији
Народна и универзитетска библиотека
Републике Српске, Бања Лука

004.72.057.4

КОРАЋ, Драган М., 1974-
Zaštita informacija u okviru sistema menadžmenta idetiteta i upravljanja pristupom : naučna monografija / Dragan M. Korać. - Banja Luka : Prirodno-matematički fakultet, Univerzitet u Banjoj Luci, 2022 ([S.l. : s.n.]). - 201 стр. : граф. прикази, табеле ; 30 cm

На спор. насл. стр.: Information security in frame of identity and access management systems. - Тираж 200. - Библиографија: стр. 176-194.

ISBN 978-99976-86-06-0

COBISS.RS-ID 137058049