Anotuotas literatūros sąrašas

Studentas: Lukas Navašinskas

Vadovas: Jonas Čeponis

Tema: **Patikimas atsarginis algoritmas dviejų faktorių autentifikacijos procesui**

Raktažodžiai:  
**2FA** - dviejų veiksnių autentifikavimas (angl.: Two factor authentication)

**MFA** – kelių veiksnių autentifikavimas (angl.: Multifactor authentication)

Literatūros sąrašas:

[1] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, “A Usability Study of Five Two-Factor Authentication Methods”.

Straipsnyje įvertinami penki 2FA metodai: SMS, TOTP, iš anksto sugeneruoti kodai, tiesioginiai pranešimai (angl.: push notifications) ir U2F raktai. Analizėje pabrėžiami 2FA metodų naudojimo tinkamumo (angl.: usability) bei įdiegimo iššūkiai pabrėžiant būtinybę išlaikyti balansą tarp saugumo ir naudojimo patogumo.

[2] A. Kuzior, P. Brożek, O. Kuzmenko, H. Yarovenko, and T. Vasilyeva, “Countering Cybercrime Risks in Financial Institutions: Forecasting Information Trends,” *JRFM*, vol. 15, no. 12, p. 613, Dec. 2022, doi: [10.3390/jrfm15120613](https://doi.org/10.3390/jrfm15120613).

Straipsnyje prognozuojamos kibernetinių nusikaltimų tendencijos finansų institucijose naudojant duomenimis pagrįstus modelius (angl.: Data-driven models). Analizuojama kylanti riziką debesų infrastruktūrai, tinklams ir kitoms IT sistemoms. Tyrime pabrėžiamas finansinio sektoriaus pažeidžiamumas ir didelių investicijų į kibernetinį saugumą poreikis.

[3] K. M. Rajasekharaiah, C. S. Dule, and E. Sudarshan, “Cyber Security Challenges and its Emerging Trends on Latest Technologies,” *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 981, no. 2, p. 022062, Dec. 2020, doi: [10.1088/1757-899X/981/2/022062](https://doi.org/10.1088/1757-899X/981/2/022062).

Straipsnyje nagrinėjamos vis augančios kibernetinės grėsmės, tendencijos. Aptariami įvairūs kibernetinio saugumo metodai, tokie kaip prieigos kontrolė (angl.: access control), kenkėjiškų programų skaitytuvai (angl.: malware scanners) ir ugniasienės.

[4] A. Kuzior, I. Tiutiunyk, and R. Kelemen, “Cybersecurity and cybercrime: Current trends and threats,” 2024.

Straipsnyje analizuojamos pasaulinės 2016–2023 m. kibernetinio saugumo tendencijos. Analizuojamos skaitmeninės transformacijos ir elektroninių nusikaltimų padaugėjimo temos, įskaitant išpirkos reikalaujančias programas (angl.: Ransomware) ir duomenų įsilaužimus (angl.: Data Breach).

[5] V. Papaspirou *et al.*, “Cybersecurity Revisited: Honeytokens meet Google Authenticator,” Dec. 15, 2021, *arXiv*: arXiv:2112.08431. doi: [10.48550/arXiv.2112.08431](https://doi.org/10.48550/arXiv.2112.08431).

Šiame tyrime pristatoma 2FA sistema, apjungianti medaus žetonus (angl.: Honeytokens) su „Google Authenticator“. Šis metodas suteikia tvirtą apsaugą, o autentifikavimo procesas išlieka paprastas ir patogus vartotojui

[6] J. Berrios, E. Mosher, S. Benzo, C. Grajeda, and I. Baggili, “Factorizing 2FA: Forensic analysis of two-factor authentication applications,” *Forensic Science International: Digital Investigation*, vol. 45, p. 301569, Jul. 2023, doi: [10.1016/j.fsidi.2023.301569](https://doi.org/10.1016/j.fsidi.2023.301569).

Straipsnyje analizuojami 15’os populiariausių 2FA programų veikimas. Nagrinėjama, kaip jose saugomi slapti duomenys, pvz., slaptieji raktai (angl.: Secret keys), paskyrų pavadinimai ir el. pašto adresai. Atskleidžiami pažeidžiamumai, pvz.: nešifruotų raktų saugojimas, dėl kurio užpuolikai gali apeiti 2FA apsaugą.

[7] R. A. Grimes, *Hacking Multifactor Authentication*. Wiley, 2020. [Online]. Available: <https://books.google.lt/books?id=Zpv9DwAAQBAJ>

Roger A. Grimes, knygoje, "Hacking Multifactor Authentication", gilinasi į MFA sistemų pažeidžiamumą. Patyręs saugumo ekspertas, tiria įvairius MFA metodus, įskaitant SMS žinutėmis pagrįstas autentifikavimo programas ir biometrinio autentifikavimo metodus. Autorius pabrėžia bendras silpnybes, tokias kaip SIM keitimas (angl.: SIM swapping) ir sukčiavimo atakos (angl.: Phishing attacks), siūlo strategijas, kaip sumažinti šią riziką.

[8] M. Lamba, R. K. Jaiswal, U. Kashyap, and S. K. Lakhan, “Is Two Factor Authentication Enough to Secure your System: A Study,” *Journal of Management*, vol. 13, no. 01, 2024.

Šiame tyrime nagrinėjamas 2FA efektyvumas gerinant sistemos saugumą. Jame aptariamos 2FA stiprybės bei pažeidžiamumai, taip pat nagrinėjamos būsimos autentifikavimo technologijos.

[9] Okta, Inc., *Ką daryti, jeigu Okta sistemos tampa nebepasiekiamos?* [Online]. Available: <https://support.okta.com/help/s/article/What-should-i-do-if-Okta-goes-down?language=en_US#:~:text=If%20our%20services%20were%20to,accessible%20through%20a%20direct%20link.>

Šiame puslapyje pateikiamas pavyzdys, kaip plačiai naudojama 2FA sistema “Okta” tvarkosi su sistemos veikimo nutrūkimu (angl.: system outage), atsakant į klausimą: “Ką daryti, jei Okta neveikia?”

[10] Cisco Duo, *Kaip “Duo Access Gateway” veikia nesekmės rėžime (ang.: failmode)*. [Online]. Available: <https://help.duo.com/s/article/5352?language=en_US#:~:text=The%20fail%20mode%20determines%20whether,primary%20authentication%20source%20is%20unreachable.>

Šiame puslapyje pateikiamas pavyzdys, kaip viena populiariausių 2FA sistemų “Cisco Duo” veikia jeigu klientui nepavyksta pasiekti “Cisco Duo” 2FA servisų.

[11] R. Bruzgiene and K. Jurgilas, “Securing Remote Access to Information Systems of Critical Infrastructure Using Two-Factor Authentication,” *Electronics*, vol. 10, no. 15, p. 18, Jul. 2021, doi: [10.3390/electronics10151819](https://doi.org/10.3390/electronics10151819).

Straipsnyje pristatomas 2FA metodas, skirtas nuotolinei prieigai prie svarbios infrastruktūros užtikrinti. Demonstruojamas pasiūlyto metodo greitas veikimas ir atsparumas kibernetinėms atakoms.

[12] C. Gilsenan and S. Egelman, “Security and Privacy Failures in Popular 2FA Apps”.

Šiame darbe analizuojami saugos ir privatumo trūkumai populiariose vienkartinio slaptažodžio (TOTP) programėlėse. Tyrimas atskleidžia, kad daugelis programų nesaugiai saugo TOTP slaptažodžius arba neapsaugo ir nutekina asmeninius naudotojų duomenis.

[13] I. Szczygieł, S. Florczak, and A. Jasiak, “Two-factor authentication (2FA) comparison of methods and applications,” *Advances in Web Development Journal*, vol. 1, no. 1, Oct. 2023, doi: [10.5281/zenodo.10050024](https://doi.org/10.5281/zenodo.10050024).

Straipsnyje lyginami įvairūs 2FA metodai ir programos. Tyrime aptariami populiarūs metodai, kaip SMS, TOTP ir aparatinės įrangos prieigos raktai (angl.: Hardware tokens). Aptariamos šių metodų stipriosios ir silpnosios pusės.

[14] G. Ali, M. Ally Dida, and A. Elikana Sam, “Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures,” *Future Internet*, vol. 12, no. 10, p. 160, Sep. 2020, doi: [10.3390/fi12100160](https://doi.org/10.3390/fi12100160).

Straipsnyje apžvelgiami mobiliųjų pinigų 2FA metodų saugumo iššūkiai, analizuojami grėsmių modeliai ir atsakomosios priemonės (angl.: Countermeasures). Tyrime nustatomi pažeidžiamumai, pvz.: apsimetinėjimas (angl.: impersonation) ir socialinės inžinerijos atakos, ir aptariami kriptografiniai ir biometriniai sprendimai, siekiant padidinti saugumą.

[15] D. Wang, X. Zhang, Z. Zhang, and P. Wang, “Understanding security failures of multi-factor authentication schemes for multi-server environments,” *Computers & Security*, vol. 88, p. 101619, Jan. 2020, doi: [10.1016/j.cose.2019.101619](https://doi.org/10.1016/j.cose.2019.101619).

Šiame darbe analizuojami saugumo trūkumai MFA metoduose. Straipsnyje nustatomi kritiniai saugos trūkumai, kaip sistemų pažeidžiamumas dėl intelektualiųjų kortelių (angl.: Smart card) vagystės, biometrinių duomenų suklastojimai.