Studentas: Lukas Navašinskas	**Vadovas: Jonas Čeponis**

Darbo tema: Patikimas atsarginis algoritmas dviejų faktorių autentifikacijos procesui

Sprendžiama problema:

Iššūkis yra sukurti veiksmingą ir patikimą alternatyvų autentifikavimo metodą, kuris galėtų pakeisti pirminį dviejų faktorių autentifikavimo (2FA) metodą tais atvejais, kai pirminis metodas nepavyksta arba tampa nepasiekiamas. Tikslas yra užtikrinti, kad atsarginis metodas išlaikytų tokį patį saugumo ir patogumo lygį kaip ir originalus 2FA, nepakenkiant bendram autentifikavimo procesui. Dėl šios problemos reikia nustatyti, įdiegti ir išbandyti veiksmingą atsarginį algoritmą, kuris galėtų sklandžiai integruotis į esamą autentifikavimo infrastruktūrą.

Darbo tikslas:

Sukurti alternatyvų autentifikavimo metodą, kurį būtų galima sklandžiai integruoti į esamą sistemą, išlaikant aukštus saugumo ir vartotojo patogumo standartus. Šiuo tyrimu siekiama išspręsti iššūkius, kylančius diegiant atsarginį sprendimą, kuris būtų ir techniškai tvirtas, ir patogus vartotojui, o tai galiausiai pagerintų bendrą sistemos saugumą.

Darbo uždaviniai:

1. Atlikti analizę apie esamas dviejų faktorių autentifikavimo metodų problemas ir pažeidžiamumus, daugiausia dėmesio skiriant gedimo ar nepasiekiamumo atvejams;
2. Sukurti veiksmingą alternatyvų autentifikavimo metodą, kuris pakeistų pirminį 2FA kritinėse situacijose;
3. Įgyvendinti eksperimentinę dalį integruojant sukurtą atsarginį algoritmą į testavimo aplinką;
4. Įvertinti sukurto metodo našumą ir patikimumą bei palyginti rezultatus su esamais 2FA sprendimais.

Kas numatoma atlikti darbo analizės dalyje. Darbo analizės turinys:

1. Dviejų faktorių autentifikavimo (2FA) ir atsarginių algoritmų problema
    - 1.1. Problemos apžvalga
    - 1.2. Dviejų faktorių autentifikavimo standartai ir tipai
    - 1.3. Pirminiai ir atsarginiai autentifikavimo metodai
    - 1.4. Sistemų ir duomenų saugumas naudojant dviejų faktorių autentifikavimą
    - 1.5. Esamų dviejų faktorių autentifikavimo sistemų pažeidžiamumas ir gedimai
    - 1.6. Dviejų faktorių autentifikavimo saugos priemonės
    - 1.7. Dviejų faktorių autentifikavimo atsarginių metodų realizacijos
    - 1.8. Analizės išvados ir tolimesni tyrimų uždaviniai

Koks bus pasiūlytas problemos sprendimo metodas / modelis / algoritmas / metodika / aparatinės realizacijos projektas / kita :

Remiantis analizės skyriuje gautais rezultatais, bus sukurtas patikimas atsarginis dviejų faktorių autentifikavimo algoritmas. Šis metodas užtikrins saugų, sklandų autentifikavimą, kai sugenda arba nepasiekiamas pagrindinis 2FA metodas, išlaikant jautrioms sistemoms reikalingus saugumo standartus.

Kokiomis priemonėmis ar būdais numatoma įgyvendinti darbo realizaciją:

Sprendimas bus kuriamas naudojantis „.NET C#“ programavimo kalba su „.NET Core“ karkasu, kad būtų sukurtas minimalus perspektyvus produktas (MPP, angl.: Minimum viable product) simuliuojantis dviejų faktorių autentifikavimo metodais saugomą sistemą. Taip pat „C#“ kalba bus kuriami ir dviejų faktorių autentifikavimo metodai, o patys metodai bus naudojams kviečiami iš android programėlės, kurtos naudojantis „Android Studio“

programine įranga.

Kokie bus eksperimento rezultatai ir kaip jie bus apdorojami:

Eksperimento rezultatus sudarys palyginimas ir įvertinimas, ar sukurtas dviejų veiksnių autentifikavimo atsarginis algoritmas veiksmingai išsprendžia nesėkmingų arba nepasiekiamų pirminio autentifikavimo metodų problemą. Bus įvertintas atsarginio dviejų faktorių autentifikavimo metodo našumas ir saugumas.