Filozofski fakultet
Univerziteta u Zenici

Predmet: Sigurnosti informacionih sistema (IS)

Naziv teme: Password politika (Password policy)

Seminarski rad

Mentor:

Ass. Muharem Redžibašić

Student:

Dino Marković

Zenica 2021/2022

SADRŽAJ

1. UVOD

U ovom seminarskom radu govorit ćemo o politici lozinki (password policy).

Krenimo od toga šta je to politika lozinki? To je skup pravila dizajniranih da poboljšaju sigurnost računala ohrabrujući korisnike da koriste jake lozinke i da ih pravilno koriste. Politika lozinke je često dio službenih propisa organizacije i može se podučavati kao dio obuke za podizanje svijesti o sigurnosti.

Politika lozinke definira pravila jačine lozinke koja se koriste za određivanje da li je nova lozinka važeća.

Pravilo jačine lozinke je pravilo kojem lozinka mora biti usklađena. Na primjer, pravila jačine lozinke mogu specificirati da minimalni broj znakova lozinke mora biti 5. Pravilo također može specificirati da maksimalni broj znakova mora biti 10 (1).

Politika lozinke postavlja pravila koja lozinke za uslugu moraju zadovoljiti, kao što su dužina i tip znakova dozvoljenih i nedozvoljenih. Osim toga, politika lozinke može specificirati da je unos zabranjen ako se termin nalazi u rječniku neželjenih termina. Da izaberete ovaj izbor u korisničkom sučelju, prvo morate učitati datoteku dictionary.ldif u IBM® Security Privileged Identity Manager (1).

Možemo odrediti sljedeće standarde i druga pravila za lozinke(1):

- Minimalna i maksimalna dužina
- Ograničenja karaktera
- Učestalost ponovne upotrebe lozinke
- Nedozvoljena korisnička imena ili korisnički ID-ovi
- Navedite minimalnu starost lozinke

Kreiranje politike lozinke

Administrator može kreirati politiku lozinke za korištenje sa jednom ili više usluga. Na primjer, možete kreirati politiku lozinke koja specificira pravilo da se znak može ponoviti najviše tri puta u lozinki.

Kreiranje pravila politike lozinke

Kao administrator, možete kreirati pravilo za postojeću politiku lozinki. Na primjer, možete kreirati pravilo koje specificira minimalni broj numeričkih znakova za lozinku.

Promjena politike lozinke

Administrator može promijeniti politiku lozinke kako bi zadovoljio zahtjeve vaše organizacije za lozinkama. Na primjer, možete promijeniti politiku lozinke da postavite minimalne i maksimalne znakove koji su potrebni za lozinku.

Promjena pravila politike lozinke

Administrator može promijeniti pravilo politike lozinke. Na primjer, možete promijeniti ili ukloniti postavke za postojeće pravilo.

Brisanje politike lozinke

Administrator može izbrisati politiku lozinke koja više nije potrebna za kontrolu unosa lozinki.

Lozinke su najčešći oblik autentifikacije koji se koristi za kontrolu pristupa informacijama, u rasponu od ličnih identifikacijskih brojeva koje koristimo za bankomate, kreditne kartice, telefonske kartice i sisteme govorne pošte do složenijih alfanumeričkih lozinki koje štite pristup datotekama. , računare i mrežne servere. Lozinke se široko koriste jer su jednostavne, jeftine i pogodne za upotrebu i implementaciju. U isto vrijeme, lozinke su također prepoznate kao izuzetno loš oblik zaštite. U ovom radu analiziraju se sistemi autentifikacije zasnovani na lozinki sa politikom lozinki i daju se preporuke za poboljšanje problema vezanih za lozinku

2. OSIGURAVANJE LOZINKE KORIŠTENJEM DINAMIČKOG ALGORITMA ZA GENERIRANJE POLITIKE LOZINKE

Većina web stranica koristi lozinke za autentifikaciju korisnika i omogućavajući im pristup resursima web stranice koji sadrže osjetljive informacije. Izbor lozinki korisnika nije jako jak i zbog toga su mnogi korisnici weba podložni hakiranju njihovih informacija. Generalno, ljudi koriste riječi iz rječnika da kreiraju lozinku ili bilo koju jednostavnu lozinku koju mogu zapamtiti.

Lozinke se stavljaju kroz jednosmjerne hash funkcije, a zatim se pohranjuju u bazu podataka kao odgovarajuće hash vrijednosti umjesto običnog teksta. Potencijalni haker može koristiti brute-force napad, napad na dugu tabelu, napad na rječnik, napad phishing-a, napad društvenog inženjeringa kako bi dohvatio ulaznu lozinku iz hash vrijednosti, a napadi uglavnom u stvarnom životu su učinjeni probijanjem heševa lozinki korištenjem napada rječnika.

Glavne web stranice i aplikacije pružaju sigurnosnu politiku zajedno s mjerom jačine lozinke i od korisnika se traži da se registruju na web lokacijama sa lozinkama koje slijede politiku lozinki. Lozinke koje prate određene obrasce prihvaćene su kao jake postojećim politikama, ali su ipak podložne napadu rječnika, napadu duginih tablica, napadu grube sile itd. na osnovu tih obrazaca. Provjera autentičnosti bilo koje informacije je najkritičniji zahtjev. Postoje različiti načini autentifikacije prema pogodnostima korisnika kao što su captcha, PIN-ovi, OTP, biometrijski otisci prstiju, itd. Generalno, sistemi zasnovani na lozinki se najčešće koriste i lako se implementiraju među postojećim metodama. [2]

Sigurnost pohranjenih lozinki je glavni problem zbog curenja lozinki sa velikih web lokacija kao što su Linked-In, G-mail, Yahoo, itd. Ovo curenje lozinke dalo je napadačima mnogo skupova podataka za obuku njihovih algoritama za razbijanje lozinki. Stobert i Biddle su rezultirali da se slabe metode skladištenja lozinki koriste na mnogim web stranicama na osnovu nedavnog curenja lozinki.

U drugoj studiji, u sistemu e-Harmony lozinke su pohranjene korištenjem MD5 heševa bez soli, a također su i Linked-In lozinke pohranjene korištenjem SHA-1 algoritma bez vrijednosti soli. Napadač može izvesti potpuno automatizirani napad kako bi provalio korisničku lozinku upoređujući vrijednost heša sa kriptografskim hešovima vjerojatnih nagađanja lozinke. Napadač van mreže ima ograničene resurse, ali on/ona može isprobati onoliko pogađanja lozinki koje želi. Dogodili su se neki incidenti s curenjem lozinke koji su pogoršali stvari. Sada, napadač ima veliki skup podataka procurjelih lozinki koje mogu uvelike poboljšati sposobnost napadača da razbiju što više lozinki.

Većina web stranica i aplikacija koristi provjeru jačine lozinke za provjeru jačine lozinki u trenutku registracije korisnika. Primarni cilj provjere snage lozinke je da usmjeri korisnike da kreiraju sigurnu lozinku, ali smo primijetili i ispitali da postoji nedostatak konzistentnosti i tačnosti u statičkoj provjeri jačine lozinke.

Postojeći uređaji za provjeru jačine lozinki ne izvode uniformnu karakterizaciju jakih lozinki . U drugoj studiji, istraživač je otkrio da postoji kompromis između upotrebljivosti i složenosti lozinke. Također, složene lozinke imaju manju upotrebljivost. Stoga, provjere snage lozinke ne mogu zahtijevati od korisnika da kreiraju vrlo složenu lozinku. [2]

Također je jednostavno ciljati provjeru jačine lozinke, tj. provjeru jačine lozinke također može biti ranjivost. Provjera jačine lozinke pruža statičku politiku lozinke za svakog korisnika. Kao rezultat toga, lozinka generirana korištenjem ove politike lozinke ima jake predrasude u pogledu karakteristika lozinke.

U ovom radu je razvijen algoritam za dinamičko generisanje politika lozinki u zavisnosti od učestalosti znakova u bazi podataka. Algoritam kreira efikasne politike koje su različite za svakog korisnika. Koristi skoro sve znakove u prostoru za lozinku koji se uglavnom ne koristi. Lozinka koju je kreirao korisnik koristeći dinamičku politiku je jaka i složena. Za napadača je teže provaliti te lozinke.

3. ANALIZA POPULARNE FUNKCIJE HEŠIRANJA

MD5 (Message-Digest Algoritam 5) je pojednostavljena kriptografska heš funkcija koja generiše 128-bitnu heš vrijednost. MD5 se koristi u većini sigurnosnih aplikacija, a koristi se i za provjeru integriteta datoteka. Heš MD5 je izražen kao heksadecimalni broj od 32 cifre

MD5, koji je izumio profesor Ronald Rivest, sa MIT-a je ažurirana verzija MD4 i koristi se kao model za SHA-1. SHA-1 i MD5 su dva najčešće korišćena hash algoritma danas, ali je upotreba MD5 vremenom odbijena jer se sada smatra neispravnim. Prema Stevens et al., čak ni SHA-1 nije bezbedan za upotrebu.

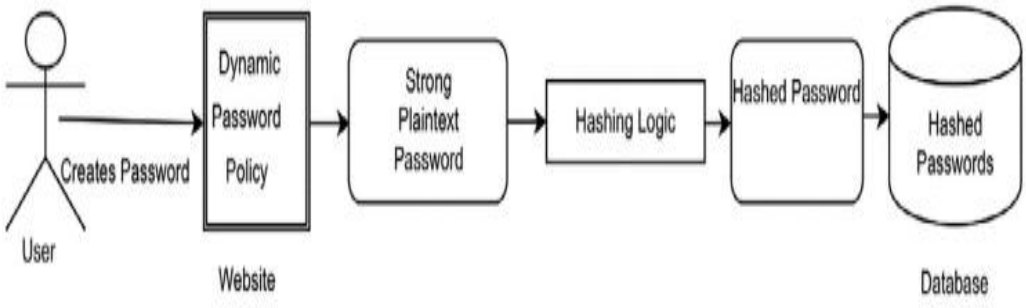
Da bi se osigurala sigurnost lozinki, programeri pohranjuju slane hash vrijednosti u svoje baze podataka umjesto običnog teksta. Napadači mogu pristupiti unosima tabela unutar baze podataka web stranica putem ranjivosti SQL injekcije. Napadač može koristiti napad grubom silom, napad na Rainbow tablicu, napad na rječnik za probijanje otvorenog teksta za unos lozinke iz njegove hash vrijednosti. Većina web stranica i aplikacija insistira na tome da korisnici dodaju posebne znakove, znamenke i simbole kako bi svoju lozinku učinili složenijom. Houshmand i Aggarwal su doveli do toga da neki korisnici biraju lozinku ponavljajući riječ iz rječnika više puta (npr. pronepronepronе, crackcrack, itd.) kako bi je učinili jakom i dugom. Haker je sposoban da identifikuje uobičajene obrasce lozinki i generiše novu rečničku datoteku na osnovu zajedničke datoteke rječnika koristeći standardne obrasce lozinki. Ove lozinke zasnovane na uzorcima nisu dovoljno jake da izbjegnu napade i sklone su takvim napadima. Stoga je izazovno osigurati slabe lozinke koristeći čak i moćne algoritame za heširanje. Offline napadi su postali vrlo opasni iz sljedećih razloga:

- Poboljšanje računarskog hardvera iz dana u dan, kako navodi Mooreov zakon, čini jeftinijim probijanje lozinki,
- Uglavnom korisnici biraju lozinke sa vrlo malom entropijom,
- Sada, napadač ima dovoljno podataka o lozinkama iz prethodnih provala, tako da posjeduju vrlo precizno znanje o obrascu popularnih lozinki.

Različite funkcije heširanja lozinki kao što su PKDF2, Bcrypt i Scrypt primjenjuju tehniku istezanja ključeva kako bi oflajn napadačima otežali i skupljili probijanje heširanih lozinki. Proširivanje ključa smanjuje broj pokušaja koje napadač poduzima da razbije heširanu lozinku, ali je također kompromis za legitimni server jer povećava cijenu autentifikacije svaki put kada se korisnik autentifikuje. [2]

4. IMPLEMENTACIJA FUNKCIJE HEŠIRANJA

Ovaj odjeljak ilustruje rad registracije korisnika i prijavljivanja na bilo koju web stranicu. **Slika 1** pokazuje kako se lozinka čuva u bazi podataka.



Slika 1. Prikazuje pohranjivanje lozinke u bazi podataka.

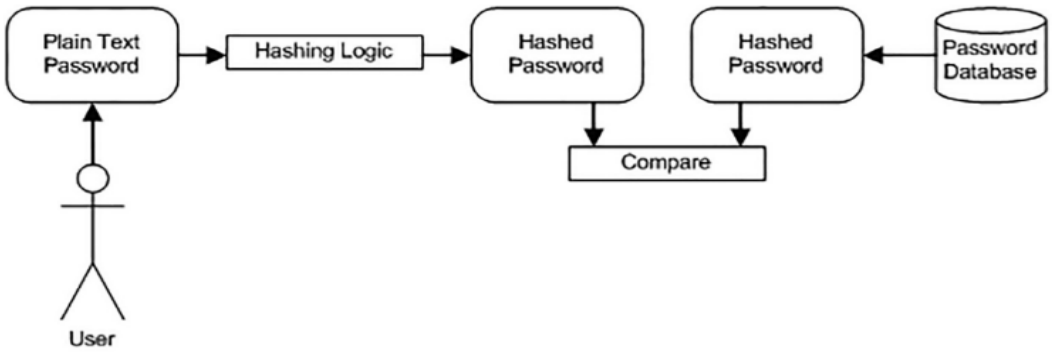
Prvo, korisnik se registruje na web stranici u kojoj korisnik mora unijeti različite detalje poput korisničkog imena, nove lozinke, sigurnosnog koda itd. Fokusirani smo na lozinku koju korisnik bira na osnovu politike lozinke koju generiše algoritam, a koji dinamičan. Politika lozinke je skup pravila koji je dizajniran da poveća sigurnost ohrabrujući korisnike da kreiraju jake lozinke. Na primjer, slijede pravila lozinki za kreiranje jake i dinamičke lozinke[2]:

- Najmanje 8 znakova u dužini.
- Maksimalna dužina od 20 znakova.
- Birajte između datih dobrih likova.
- Izbjegavajte loše karaktere.

Kreirana lozinka je jaka i složena jer slijedi politiku koja je dinamička. Generirana jaka lozinka u obliku običnog teksta se raspršuje korištenjem hash algoritma koji je spora hash funkcija, a zatim se pohranjuje u bazu podataka. [2]

Nakon uspješne registracije na web stranicu, kada se registrirani korisnik prijavi na web stranicu, data lozinka se ponovo hešira koristeći istu hash funkciju i budući da je korisnički ID primarni ključ (pošto je jedinstven) u bazi podataka, koristeći ovu , traži pohranjenu heširanu lozinku u bazi podataka. [2]

Nakon dobijanja željene heširane lozinke u bazi podataka, ona se upoređuje sa proizvedenim hešom i ako se oba poklapaju, korisniku je dozvoljen pristup resursima web stranice. To je prikazano na **slici 2**.



Slika 2. Prikazuje poređenje heša ulazne lozinke sa hešom pohranjene lozinke u bazi podataka.

Pošto je metodologija kombinacija generisanja jake lozinke primenom politike dinamičke lozinke i heširanja sa standardnom funkcijom izvođenja ključa zasnovanom na lozinki-2, ona čini predloženi sistem sigurnijim u odnosu na druge.

5. ANALIZA SISTEMA ZA AUTENTIFIKACIJU ZASNOVANU NA LOZINKI SA POLITIKOM LOZINKE

Upotreba lozinki je i dalje najširi mehanizam za online autentifikaciju. To je razumljivo, s obzirom da je jedini zahtjev da svi upamte svoje korisničko ime i lozinku, umjesto da je neugodnost da nosi digitalni certifikat, USB token, inteligentnu karticu, specijalizovani hardver ili softver, itd. [3]

Međutim, beskrajni slučajevi krađe lozinki i kompromisa su, u najmanju ruku, pokazatelj da je potrebno posvetiti veliku pažnju prilikom implementacije jednog ili drugog mehanizma. Posebno imajući na umu da se od korisnika ne može očekivati da slijede adekvatna pravila za upravljanje svojim lozinkama.

Stoga je u ovom članku izvršena analiza sistema provjere autentičnosti zasnovanih na lozinki zasnovanih na politici lozinke.

5.1. Analiza lozinke zasnovana na politici

Politika lozinki je skup pravila dizajniranih da poboljšaju sigurnost računala ohrabrujući korisnike da koriste jake lozinke i da ih pravilno koriste. Politika lozinke je često dio službenih propisa organizacije i može se podučavati kao dio obuke za podizanje svijesti o sigurnosti [4]. Svrha politike lozinki je uspostavljanje standarda za kreiranje jakih lozinki, zaštitu tih lozinki i učestalost promjene. [5]

Mnoge organizacije su usvojile politike sastavljanja lozinki [6], koje definiraju zahtjeve za kreiranje lozinke, uključujući dužinu znakova (npr. najmanje osam znakova) i kategorije znakova (npr. simboli, cifre, velika i mala slova). U određenoj mjeri, politike sastavljanja lozinki podstiču korisnike da kreiraju jače lozinke. Mnogo je politika lozinki koje su predložene u prošlogodišnjim [7]. U Tabeli 1 su data pravila i rezultati za korištenje na politikama lozinki.

№	Rules	Scores
1.	Minimum password length less than 6 characters.	- 1
2.	The minimum password length is 6-8 characters.	- 0,5
3.	Minimum length more than 8 characters.	+ 1
4.	Maximum length less than 20 characters.	-0,5
5.	Maximum length more than 20 characters.	+1
6.	Password must contain numbers.	+0,5
7.	Password must contain letters.	+0,5
8.	Password must contain capital letters.	+0,5
9.	Password must contain special characters.	+0,5
10.	Password must not be the same as login.	+1
11.	Password must not match mail.	+1
12.	The password cannot be similar to login and / or mail (login + year).	+2
13.	Password must not be dictionary.	+2
14.	The service makes recommendations explicitly.	+1
15.	Preventing the use of special characters.	-1
16.	The service strictly adheres to its recommendations.	+0,5
17.	The service allows you to set a weak password.	-1

Slika 1. Prikazuje točke o politici za lozinke

U ovom slučaju, 1 rezultat se uklanja za svaki nedostatak koji može dovesti do ranjivosti lozinke, i obrnuto, usluge s najboljim zahtjevima dobivaju odgovarajuće bodove. Što više poena skupi usluga, to je politika lozinke bolja.

Naravno, najgore je ako uopće ne postoje pravila za kreiranje lozinki, a mali broj tačaka ovdje je sam po sebi razumljiv. Međutim, pristup, u kojem usluga zahtijeva kreiranje kombinacije od najviše 20 znakova ili zabranjuje korištenje posebnih znakova, također „slabi“ lozinke [8]. Stoga je u ovom slučaju oduzimanje bodova sasvim opravdano.

Na osnovu gore navedene politike lozinki, procijenjene su sljedeće usluge: usluge e-pošte; društvene mreže; elektronska trgovina; usluge plaćanja; Usluge igara; kriptovaluta; pohrana podataka; zajednički razvoj; hosting. Procjena politike lozinki usluga e-pošte na osnovu gornjih definicija i ocjena data je u Tabeli 2.

Password requirements	Gmail	Outlook	Yandex	Mail.ru	Rambler	Yahoo
Minimum password length less than 6 characters						
The minimum password length is 6-8 characters			-0,5	-0,5	-0,5	-0,5
Minimum length more than 8 characters	+1	+1				
Maximum length less than 20 characters						
Maximum length more than 20 characters	+1	+1	+1	+1	+1	+1
Password must contain numbers	+0,5	+0,25*	+0,5	+0,5	+0,5	
Password must contain letters	+0,5	+0,25*	+0,5	+0,5	+0,5	
Password must contain capital letters		+0,25*	+0,5		+0,5	
Password must contain special characters	+0,5	+0,25*				
Password must not be the same as login	+1	+1	+1	+1		+1
Password must not match mail	+1	+1	+1	+1		+1
The password cannot be similar to login and / or mail (login + year)		+2		+2		+2
Password must not be dictionary	+2	+2	+2	+2		+2
The service makes recommendations explicitly	+1	+1	+1	+1	+1	+1
Preventing the use of special characters			-1	-1	-1	-1
The service strictly adheres to its recommendations		+0,5	+0,5	+0,5	+0,5	+0,5
The service allows you to set a weak password			-1	-1	-1	
2FA	+0,5	+0,5	+0,5	+0,5		+0,5
	sms, app, codes, e-key	sms, app	sms, app	sms, app		sms

Slika 2 prikazuje evaluaciju politike lozinke, e-mail usluge

Rezultati eksperimenata jasno pokazuju da pristupne fraze pružaju najbolju opciju za odabir lozinke, budući da je rezultujuće lozinke relativno teško razbiti, ali ih je lako zapamtiti [6, 7, 8]. Na primjer, „FSa7Yago“ može izgledati kao da se nalazi u kategoriji teško pogodnoj, ali preteškoj za pamćenje. Međutim, postoji trik koji pomaže korisniku da ga zapamti—zasnovan je na pristupnoj frazi. To jest, "FSa7Yago" je izvedeno iz fraze "prije četiri desetine i sedam godina". Shodno tome, legalnom korisniku bi ovu lozinku trebalo biti relativno lako za pamćenje, a opet relativno teško za napadača da pogodi.

6. ZAKLJUČAK

U ovom radu je razvijen algoritam koji generiše politike lozinki dinamički u zavisnosti od učestalosti karaktera. Izračunali smo vremensku složenost algoritma i utvrđeno je da algoritam radi brzo. Pošto algoritam generiše politike lozinki dinamički, za napadača će biti izazov da pogodi karakteristike baze podataka lozinki. Ovaj algoritam takođe povećava prostor za lozinku jer se većina specijalnih znakova poput !%$# nikada ne koristi u kreiranju lozinke. Uključivanje ovih znakova u lozinku će učiniti lozinku složenijom i težim za probijanje napadaču.

Cilj ovog generatora politike lozinki (password policy) je da osigura postojeće web-stranice koje su ranjive na razne napade kao što su brute-force, napad na rainbow table, napad na rječnik, itd. (kao PBKDF-2, Bcrypt, Scrypt, itd.) otežavaju probijanje lozinke čak i ako je napadač provalio server i kompromitovao bazu podataka.

Kako koristimo algoritam koji detektuje učestalost znakova i potom generiše politiku lozinke u skladu sa tim, napadaču će biti veoma teško analizirati karakteristike distribucije lozinki u bazi podataka. Stoga će napadaču biti vrlo skupo da provali te dinamički generirane lozinke. Stoga se naš dinamički generator politike lozinki može koristiti za smanjenje prijetnje oflajn napada.

7. LITERATURA

[1] https://www.ibm.com/docs/hr/i/7.1?topic=tasks-setting-password-policy-properties

[2] Journal of King Saud University - Computer and Information SciencesOpen AccessVolume 34, Issue 4, Pages 1357 – 1361 April 2022

[3] „Provjera autentičnosti zasnovana na lozinki“, INCIBE-CERT, 2021. [Online]. Dostupno: https://www.incibe-cert.es/en/blog/password-basedauthentication. [Pristupljeno: 07. maj 2022.].

[4] „Politika lozinki – Wikipedia“, En.wikipedia.org, 2021. [Online]. Dostupno: https://en.wikipedia.org/wiki/Password_policy. [Pristupljeno: 7. maj 2022.].

[5] Međunarodna konferencija o informacionim naukama i komunikacijskim tehnologijama: primjene, trendovi i mogućnosti, ICISCT 20212021 2021 Međunarodna konferencija o informacionim naukama i komunikacijskim tehnologijama, ICISCT 2021 Virtual.

[6] A. Singh i S. Raj, „Osiguranje lozinke pomoću dinamičkih lozinke algoritam generatora politike“, Journal of King Saud University - Računarske i informatičke nauke, 2019. [Pristupljeno: 7. maj 2022.].

[7] K. M. Malikovich, K. Z. Turakulovich i A. J. Tileubajevna, „A Metoda efikasnog generisanja OTP-a korišćenjem pseudoslučajnog broja Generatori“, Međunarodna konferencija o informacionim naukama 2019 i komunikacijske tehnologije (ICISCT), 2019, str. 1-4, doi: 10.1109/ICISCT47635.2019.9011825.

[8] K. Tashev, Z. Khudoykulov i J. Arzieva, "Poboljšanje poboljšanja sigurnosti jednokratna međusobna autentikacija i ključ Agreement Scheme", Međunarodni časopis za inovativnu tehnologiju i Exploring Engineering, vol. 8, br. 12, str. 5031-5036, 2019. Dostupno: 10.35940/ijitee.l3761.1081219 [Pristupljeno: 7. maj 2022.]

Slika 1. 2021 POINTS ON PASSWORD POLICY/International Conference on Information Science and Communications Technologies (ICISCT)

Slika 2. 2021 THE EVALUATION OF THE PASSWORD POLICY OF EMAIL SERVICES/International Conference on Information Science and Communications Technologies (ICISCT)