VULNERABILITĂȚILE SISTEMELOR DE AUTENTIFICARE CU DOI FACTORI (2FA)

Maria CERNEI

Departamentul Tehnologii și Sisteme Electronice, SISRC 211M, Facultatea Electronică și Telecomunicații, Universitatea Tehnică a Moldovei, Chișinău, Republica Moldova

Autorul corespondent: Cernei Maria, maria.cernei@tse.utm.md

Rezumat. *În lucrare este prezentată analiza vulnerabilităților sistemelor de autentificare cu 2 factori, aspectele de ocolire a factorilor de securitate pe calculatoare și dispozitivele pe baza de Android și identificate metodele de îmbunătățire a protecției sistemelor de autentificare cu 2 factori.*

Cuvinte cheie*: sistem de autentificare cu doi factori, 2FA, securitate cibernetică, phishing, brute-force.*

Introducere

Autentificarea cu doi factori (2FA) a fost inventată pentru a adăuga un nivel suplimentar de securitate la procedura simplă de autentificare, considerată acum de modă veche și nesigură, care constă în introducerea unui nume de utilizator și a unei parole.

Unul dintre cele mai cunoscute exemple de 2FA este atunci când se realizează conectarea la un site web cunoscut dintr-o altă locație, ceea ce duce la un IP diferit. În cazul procedurilor de conectare cu 2FA, mai întâi se introduce numele de utilizator și parola pe computer, iar apoi se primește un mesaj text de tip SMS pe telefon care oferă un cod de verificare. Acel cod de verificare trebuie introdus pe calculator pentru a finaliza procedura de conectare [1].

Factori de autentificare

Autentificarea cu doi factori este o versiune mai puțin complexă a autentificării cu mai mulți factori (MFA), care utilizează mai mulți factori pentru a determina autenticitatea. Există trei categorii principale de factori posibili într-o configurație de autentificare multifactorială.

Factor cunoscut

Categoria "factor cunoscut" este factorul cu care suntem cel mai familiarizați. Aceasta presupune ca o persoană să introducă informații pe care le cunoaște pentru a obține acces la contul său, de exemplu combinația dintre un nume de utilizator și o parolă.

Factor posedat

Primirea unui cod de verificare precum cel menționat mai devreme înseamnă că procedura utilizată este "factorul posedat" al autentificării 2FA sau MFA. Factorul posedat poate fi un cont de e-mail separat sau un telefon la care se trimite un cod de verificare, sau soluții hardware specializate, cum ar fi chei USB.

Factor de identitate

Categoria "factorilor de identitate" este încă în curs de dezvoltare, dar se axează pe anumiți markeri fizici care pot fi analizați de tehnologie, sau biometrie, pentru a dovedi identitatea. Aceste date biometrice includ: amprentele digitale, scanarea retinei, recunoașterea vocală, recunoașterea facială.

Majoritatea acestor metode trebuie să devină suficient de fiabile pentru a fi utilizate în viața de zi cu zi, deși industriile pentru care securitatea este imperativă au început să le adopte, inclusiv instituțiile medicale, băncile și companiile de comunicații. Totuși ele sunt încă prea costisitoare pentru a fi implementate sau pur și simplu prea complexe pentru a fi utilizate la moment pe telefoanele mobile.

Vulnerabilitățile 2FA la atac

În ciuda intențiilor de a îngreuna accesul infractorilor, autentificarea 2FA și chiar MFA poate fi vulnerabilă. Infractorii o ocolesc prin faptul că se află deja în posesia unui factor de autentificare, prin forțare brută sau prin utilizarea instrumentului împotriva căruia nicio tehnologie nu poate proteja – ingineria socială (social engineering). Iată care sunt cele mai frecvente moduri în care poate fi abuzată 2FA:

Phishing-ul

Phishing-ul poate fi folosit pentru a atrage victimele către o pagină de autentificare falsă. Atunci când victima introduce datele sale de identificare, atacatorul le redirecționează către pagina de autentificare reală, declanșând astfel procedura 2FA care îi solicită victimei codul numeric care i-a fost trimis prin SMS sau prin poștă sau, în unele cazuri, produs de o aplicație de autentificare. Atacatorul prinde din nou acest cod pe pagina falsă de autentificare pe care victima o folosește în continuare și obține un set complet de autentificare. Evident, din cauza utilității limitate a codului numeric, atacatorul va trebui să fie rapid. Dar, odată ce reușește să se conecteze cu succes, nimic nu-l împiedică să schimbe numărul de telefon la care va fi trimis următorul cod - sau orice altceva din cont dorește.

Resetarea parolei

Unele proceduri de autentificare pot fi ocolite prin efectuarea unei proceduri de "parolă pierdută" dacă atacatorul este în posesia unui "factor posedat". De exemplu, să presupunem că atacatorul a obținut acces la contul de e-mail al victimei, iar în acel cont a fost trimis un link de verificare pentru o anumită autentificare. Într-un astfel de caz, atacatorul ar putea folosi adresa "am uitat parola" de pe site și ar putea folosi următoarea interacțiune prin e-mail pentru a schimba parola cu un „factor cunoscut” [2].

Forța brută (Brute force)

Unele token-uri 2FA sunt atât de scurte și limitate în caractere încât pot fi obținute cu ușurință prin forță brută. Cu excepția cazului în care există sisteme de siguranță, un token (jeton) de patru cifre este destul de inutil dacă atacatorul are timp să aplice forța brută. Jetoanele care au o valabilitate limitată în timp (TOTP) oferă o protecție mai bună împotriva acestui tip de atac.

Conform studiilor companiei de securitate cibernetică Hive Systems, parolele personale ar trebui să aibă cel puțin 16 caractere amestecate pentru o securitate maximă. Compania a analizat cifrele și a calculat cât timp le-ar lua hacker-ilor pentru a intra prin forță brută în contul personal al unei victime, pe baza lungimii și complexității caracterelor (majuscule, numere și simboluri).

Parolele de regulă sunt păstrate sub formă de „date hash” și, respectiv, atacul de forță brută este bazat pe compararea hash-urilor ale unor parole deja cunoscute dintr-o bază de date creată preventiv utilizând tehnică de calcul destinată pentru mineritul de cripto-valută (crypto mining) [3].

O aplicație populară pentru hash-ing se numește *Hashcat*. În tabelul 1 este prezentat timpul necesar soft-ului *Hashcat* pentru forțarea brută a parolelor în care se utilizează diverse combinații de caractere.

Autentificarea prin părți terțe (Third-party Login)

În cadrul unor procese de autentificare, utilizatorului i se oferă opțiunea de a se autentifica folosind un cont terț, iar utilizarea acestei opțiuni permite ocolirea procedurii 2FA. Cel mai cunoscut exemplu este "autentificarea cu contul de Facebook", care este utilizat pentru anumite site-uri și aplicații. În acest caz, un atacator poate prelua alte conturi odată ce cunoaște datele de identificare de pe Facebook.

Tabelul 1

Parole cu hash MD5 sparte utilizând GPU RTX 2080 [3]

Număr de caractere	Doar numere	Litere minuscule	Litere minuscule și majuscule	Numere, litere minuscule și majuscule	Numere, litere minuscule și majuscule, simboluri
6	instantaneu	instantaneu	instantaneu	1 secundă	5 secunde
7	instantaneu	instantaneu	25 secunde	1 min	6 min
8	instantaneu	5 secunde	22 minute	1 ora	8 ore
9	instantaneu	2 minute	19 ore	3 zile	3 săptămâni
10	instantaneu	58 minute	1 lună	7 luni	5 ani
11	2 secunde	1 zi	5 ani	41 ani	400 ani
12	25 secunde	3 săptămâni	300 ani	2000 ani	34000 ani
13	4 minute	1 an	16000 ani	100000 ani	2 mil ani
14	41 minute	51 ani	800000 ani	9 mil ani	200 mil ani
15	6 ore	1000 ani	43 mil ani	600 mil ani	15 mrd ani
16	2 zile	34000 ani	2 mrd ani	37 mrd ani	1 tm ani

Vulnerabilitatea SMS în cadrul 2FA

Companiile cum ar fi Microsoft, au îndemnat utilizatorii să renunțe la soluțiile 2FA care utilizează SMS-uri și apeluri vocale. Acest lucru se datorează faptului că SMS-ul este renumit printr-o securitate infamantă, lăsând-o deschisă pentru o serie de diverse atacuri.

A fost demonstrat că schimbul de SIM-uri (SIM Swapping) este o modalitate de eludare a 2FA. Schimbul de SIM presupune ca un atacator să convingă furnizorul de servicii mobile al victimei că el însuși este victima, iar apoi să solicite ca numărul de telefon al victimei să fie schimbat pe un dispozitiv la alegerea sa. Deasemenea, s-a demonstrat, că codurile de unică folosință bazate pe SMS pot fi compromise prin intermediul unor instrumente ușor accesibile, cum ar fi soft-ul *Modlishka*, prin utilizarea unei tehnici numite „reverse proxy". Aceasta facilitează comunicarea între victimă și un serviciu care pretinde a fi un serviciu.

Astfel, în cazul softului *Modlishka*, acesta va intercepta comunicațiile dintre un serviciu autentic și o victimă și va urmări, înregistra interacțiunile victimei cu serviciul, inclusiv orice date de autentificare pe care le-ar putea folosi).

O vulnerabilitate adițională în 2FA bazat pe SMS reprezintă un atac special care exploatează o funcție oferită de Google Play Store pentru a instala automat aplicații de pe web pe dispozitivul Android. Dacă un atacator obține acces și reușește să se conecteze la contul Google Play de pe un laptop, acesta poate instala automat orice aplicație dorește pe smartphone-ul victimei.

Vulnerabilitățile dispozitivelor Android

Un actor rău intenționat poate accesa de la distanță 2FA bazat pe SMS al unui utilizator prin utilizarea unei aplicații concepută pentru a sincroniza notificările utilizatorului pe diferite dispozitive.

Mai exact, atacatorii pot profita de o combinație compromisă de e-mail și parolă conectată la un cont Google (cum ar fi username@gmail.com) pentru a instala în mod nefast o aplicație de oglindire (replicare) a mesajelor disponibilă pe smartphone-ul victimei prin intermediul Google Play. Acest scenariu este destul de real, deoarece utilizatorii folosesc, de regulă, aceleași date de acces în cadrul mai multor servicii. Utilizarea unui „manager de parole" este o modalitate eficientă de a face mai sigură prima linie de autentificare - autentificarea cu nume de utilizator/parolă.

Odată ce aplicația este instalată, atacatorul poate aplica tehnici simple de inginerie socială pentru a convinge utilizatorul să activeze permisiunile necesare pentru ca aplicația să funcționeze corect. De exemplu, acesta poate pretinde că sună de la un furnizor de servicii legitim pentru a convinge utilizatorul să activeze permisiunile. După aceasta, pot primi de la distanță toate comunicațiile trimise pe telefonul victimei, inclusiv codurile unice utilizate pentru 2FA.

Acest atac nu necesită capacități tehnice de vârf. Este nevoie doar de o înțelegere a modului în care funcționează aceste aplicații specifice și a modului de a le utiliza în mod inteligent (împreună cu ingineria socială) pentru a ținti o victimă. Amenințarea este și mai reală atunci când atacatorul este o persoană de încredere (de exemplu, un membru al familiei) cu acces la telefonul victimei.

Metode de îmbunătățire a protecției 2FA

Unele metode de păstrare a informației personale în siguranță sunt:

- Atenție sporită la e-mailurile care spun că un cont a fost folosit de pe un dispozitiv nou sau necunoscut și necesitatea să verificați dacă ați fost chiar dumneavoastră. De asemenea, este necesară o atenție sporită la alte semnalele de alarmă evidente, cum ar fi e-mailurile care notifică încercările de autentificare eșuate sau cererile de resetare a parolei care nu provin de la noi.
- Dacă există un cont de Facebook, este necesar de verificat în compartimentul setărilor Setări > Aplicații și site-uri web (Settings > Apps and Websites) dacă tot ceea ce este listat acolo este folosit de noi și dacă ar trebui să fie acolo. Un cont de Facebook "dezactivat" poate fi restabilit atunci când undeva se utilizează opțiunea "Autentificare cu contul de Facebook".
- Dacă există posibilitatea selectării procedurilor de autentificare, este important de analizat vulnerabilitățile cunoscute. De exemplu, algoritmii slabi ai token-urilor pot fi folosiți de un atacator pentru a prezice următorul token, în cazul disponibilității celor anterioare. Sau utilizarea unor token-uri scurte, fără o valabilitate limitată, poate expune utilizatorul la un atac.
- Pregătirea personală și a eventualilor angajați ai unei companii pentru a recunoaște tentativele de phishing.

Concluzii

Adevărul este că până și autentificarea cu mai mulți factori (MFA) are soluții de ocolire. Metodele de autentificare prin "factor de identitate" utilizate în prezent pe dispozitivele noastre sunt încă destul de ușor de eludat - nu este nevoie de un hacker geniu pentru a împiedica recunoașterea vocală.

Având în vedere că actual sunt înregistrate din ce în ce mai multe încălcări masive de date ale unor companii populare, autentificarea 2FA devine rapid o procedură standard. Și chiar dacă există modalități de a ocoli 2FA, aceasta este totuși mai sigură decât utilizarea combinației de modă veche – nume de utilizator și parolă. Pentru a ocoli 2FA, atacatorul ar trebui să spargă două cicluri de autentificare, față de unul singur.

Referințe

1. Roger Grimes. The many ways to hack 2FA. Journal Network Security, Vol. 2019, Issue 9, pp.1-20. https://www.sciencedirect.com/science/article/abs/pii/S1353485819301072
2. Thanasis Petsas, Giorgos Tsirantonakis, lias Athanasopoulos, Sotiris Ioannidis. Two-factor authentication: is the world ready? Quantifying 2FA adoption. https://dl.acm.org/doi/abs/10.1145/2751323.2751327.
3. Looking at Passwords in 2022. https://www.hivesystems.io/blog/are-your-passwords-in-the-green?utm_source=tabletext&fbclid=IwAR0-cG7B6VRJ-UMq7L7nuMZT3RlFXNkOLjhp4M6oJUV5XbFrsCpyhDNhQ7Q