Securitatea și confidențialitatea datelor în contextul aplicațiilor mobile

Ghimpu Lucian Eduard

April 13, 2019

Conducător științific
Dr. CZIBULA Istvan, Profesor Universitar

Contents

1 Introducere

1.1 Introducere

1.2 Ecosistemul aplicațiilor mobile

1.3 GDPR

2 Securitatea și confidențialitatea datelor în contextul aplicațiilor mobile

2.1 Autentificarea si înregistrarea

2.1.1 Ceva introducere *

Indiferent că vorbim de aplicații web, desktop sau mobile, majoritatea folosesc o metodă de autentificare. Auntentificarea și înregistrarea stau la baza problematicii securității datelor. În clasamentul OWASP Top 10 din 2017 [1], problemele legate de autentificare și gestiunea sesiunii, sunt clasate pe locul 2. Iar în clasamentul OWASP top 10 Mobile din 2016 [2], autentificare nesigură și autorizarea necurespunzatoare sunt clasate pe locul 4, respectiv 6.

Unicitatea aplicaților mobile este dată de faptul că un dispozitiv mobil poate devenii accesibil oricărui persoane datorită portabilitatii lor. Un dispozitiv mobil poate fi furat, pierdut sau accesat temporal de o persoană necunoscută fără permisiunea posesorului. Prin urmare nevoia de un sistem de autentificare robust este mandatorie atunci când vorbim de aplicații care gestionează date sensibile (aplicații financiare, sociale, medicale, etc. . .).

În cadrul aplicațiilor mobile, autentificarea se poate face prin mai multe metode. De la simpla autentificare prin utilizator și parolă, până la utilizarea de sezori biometrici. Mitigari clasice precum impunerea unei parole sigure rămân valabile și în contextul aplicațiilor mobile.

Pentru alegerea metodei de autentificare trebuie să ne punem în primă instanța următoarele două întrebări:

- Care este scopul aplicației? O aplicație care notifica utilizatorul despre starea meteo poate că nu ar avea nevoie de autentificare prin senzori biometrici.
- Aplicația gestionează date confidențiale? Un exemplu potrivit ar fi o aplicație precum BT pay, care gestionează contul curent al unui utilizatorul, se folosește de mai multe metode de autentificare, o dată prin datele de logare, iar apoi prin senzori biometrici.

După ce ne este clar care este scopul aplicației și cu ce fel de date lucrează, putem include una sau mai multe metode de autentificare bazate după următorii factori:

1. Ceva ce utilizatorul știe (parolă, pin etc. . .)
2. Ceva ce il definește pe utilizator (amprenta, retina)
3. Ceva ce utilizatorul deține (parole generate temporal)

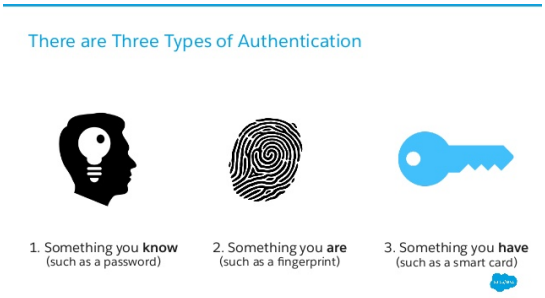

Figure 1: Metode de autentificare [3]

2.1.2 JWT

Majoritatea aplicațiilor de azi se folosesc de cea mai simplă formă de autentificare, prin folosirea de credentiale (ceva ce utilizatorul știe) și unui token de acces (ceva ce utilizatorul deține). Utilizatorul își creeza cont pentru o anumită aplicație, folosește credeințalele pentru a se loga, cererea de autentificare ajunge la server unde se verifică credențialele iar apoi se generează un token care va fi folosit de utilizator pentru a accesa diferite resurse în aplicație.

Scenariu descris anterior se referă la folosirea de JWT (JSON Web Token), un standard (RFC 7519) [4] adoptat de multe aplicații mobile în zilele noastre. JSON Web Token este o metodă sigură de autorizare a trasferului de informații între două părți [5], deobicei clientul mobil și serverul la care se face cererea. Clientul revendică de la server o dovadă, un token, care apoi este folosit de client pentru a accesa diferite resurse.

Din punct de vedere tehnic, un JWT are urmatoarea forma 11111.22222.33333 și este alcătuit din 3 parți:

1. Antetul (Header)
2. Datele utile (Payload)
3. Semnătura (Signature)

Figure 2: Antetul unui JWT, alcatuit din tipul de algoritm de înregistrare (HS256) și tipul de token (JWT).

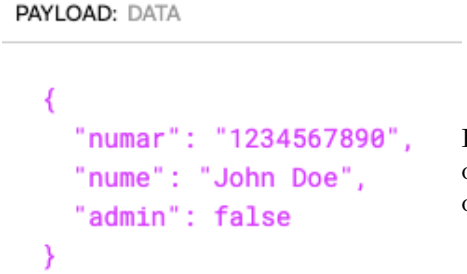

Figure 3: Partea utilă al unui JWT conține date sau permisiuni pe care clientul le are.

Figure 4: Semnătura unui JWT este alcătuită din antetul encodat, datele encodate, algoritmul folosit în antet și un secret. Semnătura are rolul de a oferi o metodă de verificare pentru a asigura ca conținutul nu a fost modificat

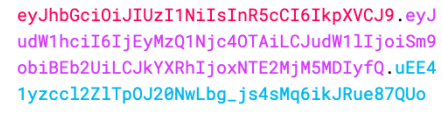

Figure 5: JWT va fi format în final de 3 siruri de caractere de tip Base64-URL separate prin punct.

O dată ce clientul deține un token, acesta trebuie tratat cu multă grijă în cadrul unei aplicații. Acesta poate fi folosit mai apoi în antetul tuturor cererilor de tip HTTP sub formă "Authorization: Bearer ¡token¿", din acest motiv cel mai probabil se dorește salvarea token-ului în memoria locală a dispozitivului pentru a putea fi apoi folosit în viitor. Acesta poate fi criptat iar la rândul lui la nivelul clientului, deși în mod nativ atât pe android cât și pe ios există metode sigure de stocare a datelor de tip primitiv (SharedPreferences în mod private pe Android și keychain pe iOS).

Pentru un nivel și mai mare de siguranță, se poate limita durata de timp pe care este valabil un token. Spre exemplu aplicația BT Pay folosește un token care este valid tip de 10-15 minute. După ce token-ul expiră, utilizatorul este nevoit să se autentifice din nou.

Avantajul principal pe care îl oferă JWT este facilitatea prin care se demarează tot procesul de revendicare a datelor sau drepturile de la un server de catre client. Un alt aspect important îl reprezintă faptul că în spate, totul se produce folosit obiecte de tipul JSON, fapt ce il face extrem de ușor de implementat și folosit in orice limbaj de programare.

2.1.3 Autentificare prin senzori biometrici

Biometria este termenul tehnic folosit pentru măsurătorile și calculele făcute legate de corpul uman. Se folosește de metrici legate de caracteristicile umane. În cazul dezvoltării de software, biometria este folosită pentru autentificare.

Autentificarea prin senzori biometrici se folosește de un factor moștenit, ceva ce îl definește pe utilizator și prin urmare este una dintre cele mai comode și rapide metode de autentificare. Mai mult decât atât, datele biometrice precum aprentă sunt greu de furat sau compromis.

Din ce în ce mai multe aplicații încep să folosească autentificare prin senzori biometrici, un factor major îl joacă faptul că în ultimi ani, capabilitățile hardware ale dispozitivelor mobile a crescut exponențial, telefoanele vin încorporate cu diferinti senzori biometrici precum: senzori de amprenta și recunoaștere facială (iris și rețină).

Metricile biometrice pot varia de la caracteristici fizice până la aspecte ale comportamentului unei persoane. În cea ce privește dispozitivele mobile putem

idetifica trei tipuri de autentificari biometrice:

1. Senzor de amprentă, extrem de sigur deoarece fiecare individ are o amprentă unică.
2. Recunoașterea vocii, avantajoasă deoarece nu necesitâ hardware in plus dar nepotrivit pentru situații unde utilizatorul trebuie să păstreze liniștea.
3. Recunoaștere facială, la fel ca cea a vocii, nu necesită hardware adițional dar nepotrivit pentru locuri în care luminozitatea este scăzută.

Utilizarea senzorilor biometrici implică anumite aspecte de care un dezvoltator de aplicații mobile trebuie să țină cont:

- Verificarea ca dispozitivul mobil este încorporat cu senzorii folosiți, în cazul în care un dispozitiv nu are senzorii biometrici, dezvoltator trebuie să ofere o metodă alternativă de autentificare. [9]
- Cererea de permisiunea petru folosirea senzorilor.
- Verificarea datele biometrice asociate dispozitivului să nu se modifică de la prima autentificare. Această măsură trebuie luată pentru a împiedică cazuri în care se adaugă noi date biometrice (amprenta nouă).

Deși autentificare prin senzori biometrici este mai rapidă și comodă, această nu ar trebuii să înlocuiască în mod complet autentificare făcută la nivel de server. Ambele metode pot coexista în funcție de context.

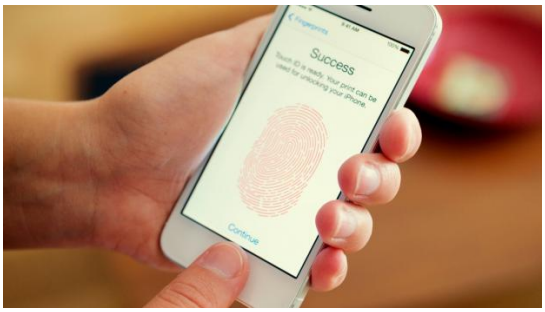

Figure 6: Autentificare prin senzor de amprentă

2.1.4 Autentificare prin factori multiplii

Autentificare prin factori multiplii (MFA) este un sistem de securizare a autentificării prin impunerea a mai multor metode de verificare a identității unui utilizator.

Autentificare prin factori multiplii combină mai multe metode independente de autentificare. Așa cum am văzut în capitolul anterior, autentificarea prin senzori biometrici și autentificarea prin credentiale lucrează cel mai bine împreună. Pe această idee, rolul autentificării prin factori multiplii este acela de a creea un sistem greu de compromis în vederea asigurării siguranței și confidentialității datelor utilizatorului. Astfel dacă unu din componentele sistemului este compromis, atacatorul este oprit de restul barierelor. În cazul în care cineva are acces

la credentialele unui utilizator și la dispozitivul sau mobil, atacatorul poate fi oprit prin folosirea senzorului de amprenta.

Un alt caz de utilizare al autentificarii prin factori multiplii îl reprezintă autentificarea în doi pași sau OTP (one time password). Rolul autentificarii în doi pași este acela de a crea o barieră în plus în sistemul de securizare al autentificarii prin creeare de coduri/parole temporare unice.

După ce un utilizator se loghează folosind credențialele valide, un cod unic și temporar este generat și trimis utilizatorului prin diferite canale, deobicei prin SMS, email sau aplicații special făcute pentru generarea de coduri unice. Utilizatorul este apoi nevoit să introducă codul primit pentru a își confirmă identitatea. Utilizarea sa nu se limitează doar la autentificare, ci poate fi folosită în mod general pentru a confirmă identitatea persoanei. Un exemplu îl reprezintă aplicațiile financiare care atunci când se încearcă o plata, vor trimite un cod unic pentru a verifică identitatea persoanei care a inițiat acțiunea.

Deși folosirea autentificarii prin doi pași este destul de comună în cadrul aplicațiilor mobile, această metodă prezintă și anumite vulnerabilități, mai ales când canalul de comunicare a parolei este prin SMS sau prin apel telefonic. SMS-urile pot fi interceptate și redirecționate, la fel și apelurile telefonice. În astfel de cazuri se poate limita valabilitatea codului primit la un iterval scurt de timp (5-10 minute).

Utilizarea unui sistem de autentificare multiplu precum autentificare în doi pași este de altfel recomandată și de ENISA [8] într-un studiu făcut în vederea siguranței procesării datelor personale de către companii mari.

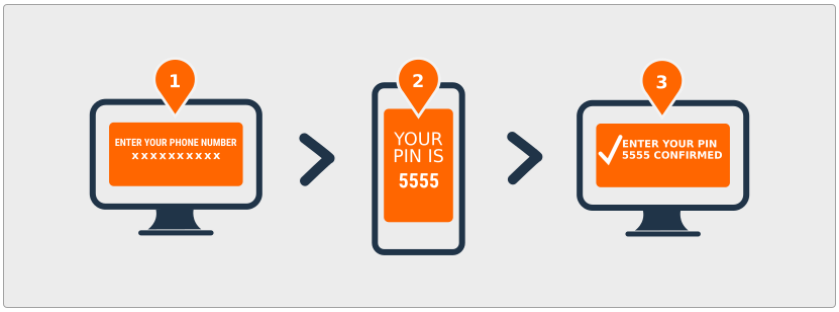

Figure 7: Autentificare în doi pași

List of Figures

References

[1] OWASP Top 10 2017
https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

[2] OWASP Top 10 Mobile 2016
https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

[3] 3 types of Authentication
https://www.slideshare.net/awesomeadmin/secure-your-salesforce-org-with-twofactor-authe

[4] RFC 7519 JWT
https://tools.ietf.org/html/rfc7519

[5] JSON Web Token (JWT)
https://tools.ietf.org/html/rfc7519

[6] ENISA, Privacy and data protection in mobile applications, 29.01.2019
https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applicat

[7] ENISA, Smartphone Secure Development Guidelines, 27.02.2017,
https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016

[8] ENISA, Guidelines for SMEs on the security of personal data processing, 27.01.2017
https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-persona

[9] OWASP Mobile Application Security Verification Standard,
https://github.com/OWASP/owasp-masvs

[10] amprenta
https://engineering.nyu.edu/news/so-you-think-you-can-secure-your-mobile-phone-fingerpr

[11] What is Two-Factor Authentication?
https://blog.templatetoaster.com/wordpress-two-factor-authentication/