

Securitatea și confidențialitatea datelor în contextul aplicațiilor mobile

Ghimpu Lucian Eduard

April 18, 2019

CONDUCĂTOR ȘTIINȚIFIC

DR. CZIBULA ISTVAN, PROFESOR UNIVERSITAR

Contents

| | | |
|----------|-----------------------------------------------------------------------------------|-----------|
| 1 | Introducere | 3 |
| 1.1 | Introducere | 3 |
| 1.2 | Ecosistemul aplicațiilor mobile | 3 |
| 1.3 | GDPR | 3 |
| 2 | Securitatea și confidențialitatea datelor în contextul aplicațiilor mobile | 3 |
| 2.1 | Autentificarea și înregistrarea | 3 |
| 2.1.1 | Ceva introducere * | 4 |
| 2.1.2 | JWT | 5 |
| 2.1.3 | Autentificare prin senzori biometrici | 7 |
| 2.1.4 | Autentificare prin factori multipli | 8 |
| 2.2 | Canale de comunicare | 10 |
| 2.2.1 | HTTP și HTTPS | 10 |
| 2.2.2 | SMS | 11 |
| 2.2.3 | WebSocket | 12 |
| 2.3 | Persistența datelor | 13 |
| 2.3.1 | Metode de persistare a datelor | 13 |
| 2.3.2 | Criptografie | 13 |
| 2.3.3 | Gestionarea datelor sensibile | 13 |
| 2.4 | Alți factori | 13 |
| 2.4.1 | Permițiuni | 13 |
| 2.4.2 | Webviews | 13 |
| 2.4.3 | Distribuirea aplicației | 13 |
| 2.4.4 | Probleme specifice pe anumite platforme | 13 |
| 3 | Medicarium | 13 |
| 3.1 | Analiza aplicației | 13 |
| 3.1.1 | Problematica | 13 |
| 3.1.2 | Cazuri de utilizare | 13 |
| 3.2 | Proiectarea aplicației | 13 |
| 3.2.1 | Arhitectura | 13 |
| 3.2.2 | UML ceva??? | 13 |
| 3.3 | Implementarea aplicației - Serverul și serviciile | 13 |
| 3.3.1 | Server REST | 13 |
| 3.3.2 | Node.js | 13 |

| | | |
|-------|-----------------------------------------------------|----|
| 3.3.3 | MongoDB | 13 |
| 3.3.4 | Rute disponibile | 13 |
| 3.3.5 | Autentificare in doi pași | 13 |
| 3.4 | Implementarea aplicației - Clientul mobil | 13 |
| 3.4.1 | Android Jetpack | 13 |
| 3.4.2 | Kotlin | 13 |
| 3.4.3 | Autentificarea | 13 |
| 3.4.4 | Securitatea aplicației | 13 |
| 3.4.5 | Gestionarea permisiunilor | 13 |
| 3.4.6 | Gestionarea fișierelor | 13 |
| 3.5 | Testarea | 13 |
| 4 | Manual de utilizare | 13 |
| 5 | Concluzii | 13 |
| 6 | Bibliografie | 14 |

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 și înregistrarea

2.1.1 Ceva introducere *

Indiferent că vorbim de aplicații web, desktop sau mobile, majoritatea folosesc o metodă de autentificare. Autentificarea 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 necorespunzătoare sunt clasate pe locul 4, respectiv 6.

Unicitatea aplicațiilor mobile este dată de faptul că un dispozitiv mobil poate deveni accesibil oricărui persoane datorită portabilității 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 senzori 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 utilizator, 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 îl definește pe utilizator (amprenta, retina)

3. Ceva ce utilizatorul deține (parole generate temporal)

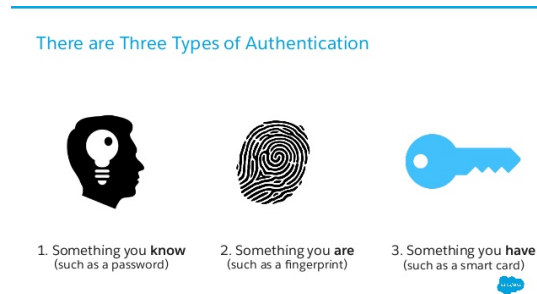


Figure 1: Metode de autentificare [3]

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 creează cont pentru o anumită aplicație, folosește credentialele pentru a se loga, cererea de autentificare ajunge la server unde se verifică credentialele 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 transferului de informații între două părți [5], de obicei 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 următoarea formă 11111.22222.33333 și este alcătuit din 3 părți:

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

HEADER: ALGORITHM & TOKEN TYPE

```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}
```

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

PAYLOAD: DATA

```
{  
  "numar": "1234567890",  
  "nume": "John Doe",  
  "admin": false  
}
```

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

VERIFY SIGNATURE


```
HMACSHA256(  
  base64UrlEncode(header) + "." +  
  base64UrlEncode(payload),  
  your-256-bit-secret  
)  secret base64 encoded
```

Figure 4: Semnătura unui JWT este alcătuită din antetul encodat, datele encodeate, 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

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJudW1hcnI6IjEyMzQ1Njc4OTAiLCJudW11IjoieSm9obiBEb2UiLCJkYXRhIjoxNTE2MjM5MDIyfQ.uEE41yzcc12Z1Tp0J20NwLbg_js4sMq6ikJRue87QUo
```

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 (Shared-Preferences 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 către client. Un alt aspect important îl reprezintă faptul că în spate, totul se produce folosit obiecte de tipul JSON, fapt ce îl face extrem de ușor de implementat și folosit în 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 aprență 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, capacitățile hardware ale dispozitivelor mobile a crescut exponențial, telefoanele vin încorporate cu diferinți 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 necesită hardware în 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. [6]
- Cererea de permisiunea pentru folosirea senzorilor.
- Verificarea datele biometrice asociate dispozitivului să nu se modifice de la prima autentificare. Această măsură trebuie luată pentru a împiedica cazuri în care se adaugă noi date biometrice (amprenta nouă).

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

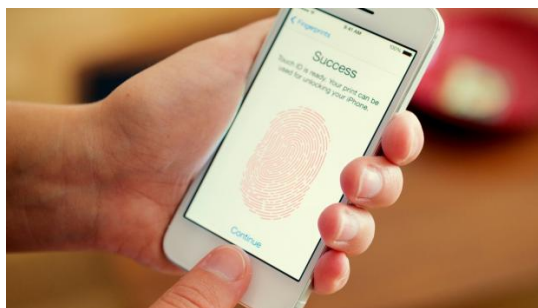


Figure 6: Autentificare prin senzor de amprentă

2.1.4 Autentificare prin factori multipli

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

Autentificare prin factori multipli 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 multipli este acela de a crea 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 autentificării prin factori multipli îl reprezintă autentificarea în doi pași sau OTP (one time password). Rolul autentificării în doi pași este acela de a crea o barieră în plus în sistemul de securizare al autentificării prin creare 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, de obicei prin SMS, email sau aplicații special făcute pentru generarea de coduri unice. Utilizatorul este apoi nevoit să introducă codul primit pentru a își confirma identitatea. Utilizarea sa nu se limitează doar la autentificare, ci poate fi folosită în mod general pentru a confirma identitatea persoanei. Un exemplu îl reprezintă aplicațiile financiare care atunci când se încearcă o plată, vor trimite un cod unic pentru a verifica identitatea persoanei care a inițiat acțiunea.

Deși folosirea autentificării 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 redirectionate, la fel și apelurile telefonice. În astfel de cazuri se poate limita valabilitatea codului primit la un interval scurt de timp (5-10 minute).

Utilizarea unui sistem de autentificare multiplu precum autentificare în doi pași este de altfel recomandată și de ENISA [7] într-un studiu făcut în vederea siguranței procesării datelor personale de către companii mari.

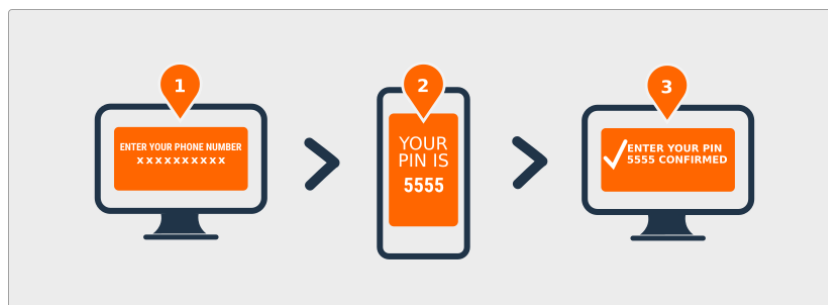


Figure 7: Autentificare în doi pași

2.2 Canale de comunicare

2.2.1 HTTP și HTTPS

Majoritatea aplicațiilor mobile se folosesc de unul sau mai multe servere pentru a își aduce date sau pentru a prelucra date preluate de la utilizator. Această practică este folosită pentru a evita stocarea de date pe dispozitivele utilizatorului având în vedere memoria limitată pe care o dețin. Din acest motiv este necesar folosirea unor protocoale de comunicare. Cele mai folosite protocoale de comunicare în ecosistemul mobil sunt HTTP și HTTPS.

Aceste protocoale de comunicare sunt un set de reguli care descriu modalitatea prin care datele sunt trimise și primite. În mediul mobil, HTTP și HTTPS sunt cele mai folosite protocoale pentru a trimite text, imagini și sunete.

HTTPS este varianta sigură a lui HTTP, pe tot parcursul comunicării, datele sunt criptate de la un capăt la altul. Deși HTTP este mai frecvent folosit, este recomandată folosirea protocolului HTTPS mai ales pentru aplicații care gestionează date sensibile.

Dezavantajul folosirii protocolului HTTPS îl reprezintă performanța. Criptare și decriptarea datelor transmise sunt operații costisitoare. Deși există o pierdere de performanță, există studii [8] care demonstrează că diferența de performanță este modestă, și încurajează folosirea protocolului mai sigur. Un alt studiu [9] arată că pe anumite sisteme de operare mobile, precum Android, rata de adopție pentru HTTPS este în urmă față de rata de adopție pe desktop.

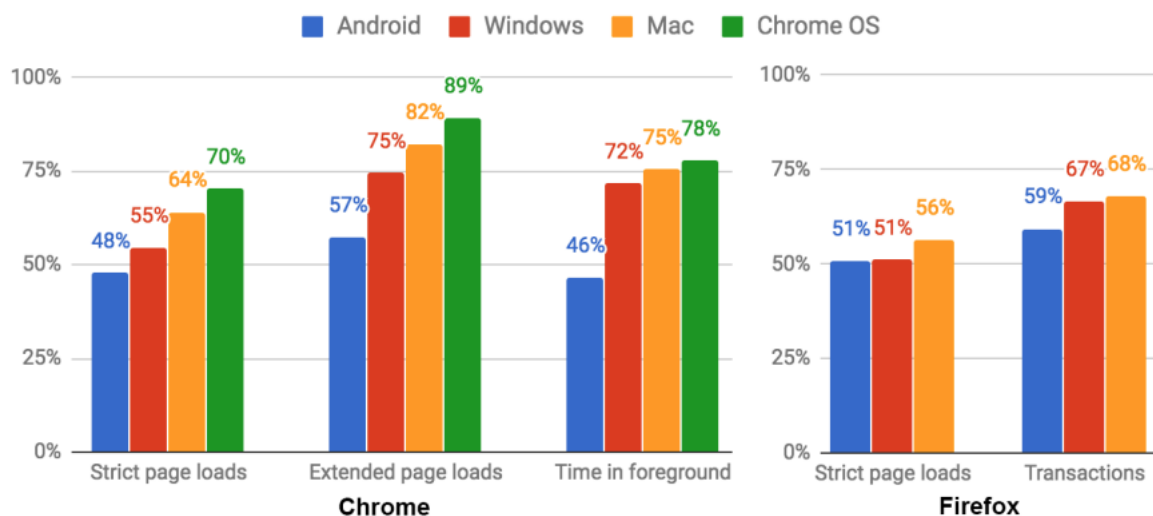


Figure 8: Procentul de utilizare HTTPS pe diferite sisteme de operare la sfarsitul unei saptamani din Februarie 2017 [9]

2.2.2 SMS

SMS (Short Message Service) este un serviciu folosit de majoritatea dispozitivelor mobile. Cazurile de utilizare ale serviciului variază de la simpla folosire pentru a comunica mesaje scurte, până la autentificare cu parolă unică. În 2010, 6.1 trilioane de mesaje au fost trimise cu o medie de 193.000 de SMS-uri pe secundă [10].

Din punct de vedere tehnic, SMS este un protocol de comunicare care permite schimbul de mesaj scurte. Un SMS poate fi format din 160 de caractere alfanumerice, mesajele mai mari de 160 de caractere sunt sparte în mai multe mesaje. Un mesaj trimis este mai întâi interceptat de SMSC (Short Message Service Center) care de cele mai multe ori este menținut de providerii de rețele telefonice. SMSC-ul trimite mai apoi mesajul către un alt SMSC (al receptorului) mesaj pe care în final îl trimite receptorului.

În ciuda popularității sale, comunicare prin SMS prezintă anumite vulnerabilități. Cel mai periculoasă vulnerabilitate este "SMS spoofing". Aceasta are loc când un atacator manipulează adresa mesajului pentru a impersona pe cineva. Aceste tipuri de atacuri pot fi prevenite prin verificarea datelor

emittătorului înainte ca mesajul să ajungă la receptor. O altă metodă de protejare, adoptată mai ales în cadrul autentificării prin 2 pași, este folosirea unui SMS gateway, servicii special dedicate pentru astfel de operații, dotate cu diverse măsuri de protecție.

2.2.3 WebSocket

Standardizat în 2011 în RFC 6455 [11], WebSocket este un protocol de comunicare bidirecțional bazându-se de fapt o conexiune de tip TCP.

Principalul avantaj pe care îl oferă protocolul WebSocket este facilitatea prin care se permite transferul de date în mod bidirecțional. În comparație cu protocolul HTTP, un server poate transmite date unui client fără ca acesta să fie făcut o cerere.

La fel ca HTTP, protocolul WebSocket (WS) este dublat de variată protejată WSS, oferind criptare de la un capăt la altul al comunicării.

Când vine vorba de aplicații mobile, WebSocket-urile sunt folosite predominant de aplicații care au nevoie de o comunicare de tip broadcast. Aplicațiile de mesagerie în grup precum WhatsApp folosesc WebSocket-uri pentru a notifica toți utilizatorii unui grup de mesaje noi primite.

Deși WebSocket rezolvă probleme de conectivitate, nu rezolvă și problemele de securitate [12]. vulnerabilități la nivelul acestui protocol variază de la simple interceptări ale datelor în rețea, atunci când se folosește varianta neprotejată a protocolului, până la vulnerabilități mai severe precum blocarea serviciului (DDos) [13]. Pentru a evita astfel de probleme este sugerată folosirea variantei protejate (wss) și limitarea conexiunilor sau verificarea conexiunilor când provin din aceeași sursă.

Fiind o tehnologie încă tânără, WebSocket încă nu este la fel de răspândit precum HTTP sau SMS, dar că orice sistem de comunicare, includerea lui într-o soluție soft necesită atenție sporită pentru a prevenii eventuale probleme de securitate.

2.3 Persistența datelor

2.3.1 Metode de persistare a datelor

2.3.2 Criptografie

2.3.3 Gestionarea datelor sensibile

2.4 Alți factori

2.4.1 Permisuni

2.4.2 Webviews

2.4.3 Distribuirea aplicației

2.4.4 Probleme specifice pe anumite platforme

3 Medicarium

3.1 Analiza aplicației

3.1.1 Problematica

3.1.2 Cazuri de utilizare

3.2 Proiectarea aplicației

3.2.1 Arhitectura

3.2.2 UML ceva???

3.3 Implementarea aplicației - Serverul și serviciile

3.3.1 Server REST

3.3.2 Node.js

3.3.3 MongoDB

3.3.4 Rute disponibile

3.3.5 Autentificare in doi pași

3.4 Implementarea aplicației - Clientul mobil

3.4.1 Android Jetpack

3.4.2 Kotlin

13

3.4.3 Autentificarea

3.4.4 Securitatea aplicației

3.4.5 Gestionarea permisiunilor

3.4.6 Gestionarea fișierelor

6 Bibliografie

Bibliografie

- [1] OWASP. *OWASP Top 10 2017*. URL: https://www.owasp.org/images/7/72/OWASP%5C_Top%5C_10-2017%5C_%5C%28en%5C%29.pdf.pdf.
- [2] OWASP. *Top 10 Mobile 2016*. URL: https://www.owasp.org/index.php/Mobile%5C_Top%5C_10%5C_2016-Top%5C_10.
- [3] *3 types of Authentication*. URL: <https://www.slideshare.net/awesomeadmin/secure-your-salesforce-org-with-twofactor-authentication>.
- [4] *RFC 7519 JWT*. URL: <https://tools.ietf.org/html/rfc7519>.
- [5] *JSON Web Token (JWT)*. URL: <https://tools.ietf.org/html/rfc7519>.
- [6] ENISA. *Smartphone Secure Development Guidelines*. 2017. URL: <https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016>.
- [7] ENISA. *Guidelines for SMEs on the security of personal data processing*. 2017. URL: <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing>.
- [8] Arthur Goldberg, Robert Buff, and Andrew Schmitt. “A comparison of HTTP and HTTPS performance”. In: *Computer Measurement Group, CMG98* 8 (1998).
- [9] Adrienne Porter Felt et al. “Measuring {HTTPS} Adoption on the Web”. In: *26th {USENIX} Security Symposium ({USENIX} Security 17)*. 2017, pp. 1323–1338.
- [10] “The rise of 3G”. In: URL: <http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf>.
- [11] Ian Fette and Alexey Melnikov. *The websocket protocol*. Tech. rep. 2011.
- [12] Jussi-Pekka Erkkilä. “Websocket security analysis”. In: *Aalto University School of Science* (2012), pp. 2–3.

- [13] *Testing WebSockets*. URL: [https://www.owasp.org/index.php/Testing_WebSockets_\(OTG-CLIENT-010\)](https://www.owasp.org/index.php/Testing_WebSockets_(OTG-CLIENT-010)).