# Model de securitare a aplicațiilor mobile în baza analizei STRIDE

Rodica BULAI, Nelu SNEGUR
*Technical University of Moldova*
rodica.bulai@mail.utm.md, nelu.snegur@ati.utm.md

***Abstract* — STRIDE is a threat classification model developed by Microsoft for thinking about computer security threats. It provides a mnemonic for security threats in six categories: Spoofing of user identity, Tampering, Repudiation, Information disclosure (privacy breach or data leak), Denial of service (D.o.S) and Elevation of privilege. Based on this methodology, a pattern of threats and vulnerabilities for all of mobile applications which are developed, as well as security measures that prevent identified threats.**

***Index Terms* — STRIDE, threats, vulnerabilities, mobile applications, security measures.**

## I. INTRODUCERE

Dispozitivele mobile au devenit tot mai răspîndite în ziua de azi. Telefoanele mobile și tabletele sunt dotate cu putere de calcul similare calculatoarelor, ceea ce favorizează dezvoltarea aplicațiilor pentru dispozitive mobile cît mai complexe. Aceste aplicații procesează și stochează date confidențiale ale utilizatorilor precum date despre starea sănătății, date financiare, poziția geografică și date cu caracter personal. Dezvoltarea aplicațiilor mobile implică și crearea serviciilor web cu care aplicațiile comunică pentru procesarea și stocarea datelor, care la rîndul său, necesită măsuri de securitate. Din aceste motive, asigurarea securității aplicațiilor mobile trebuie să fie preocuparea primară a oricărui programator.

Pentru analiza și identificarea amenințărilor și vulnerabilităților unei aplicații mobile, este utilizată metodologia STRIDE: **S**poofing of user identity - Falsificarea identității utilizatorului; **T**ampering - Fraudarea datelor; **R**epudiation – Repudierea; **I**nformation disclosure - Dezvăluirea informațiilor; **D**enial of service - Întreruperea funcționării serviciilor; **E**levation of privilege - Ridicarea nivelului de privilegii [1]. În baza acestei metodologii este elaborat un model de amenințări și vulnerabilități caracteristice aplicațiilor mobile și măsurile de securitate care previn amenințările identificate.

## II. MODELUL DE SECURITATE

**Falsificarea identității utilizatorului**

*Amenințări:*

- gestionarea incorectă a sesiunii de autentificare;
- traficul de rețea necriptat.

O aplicație mobilă, de regulă, permite autentificarea utilizatorilor în baza unui nume de utilizator și parolă. Aceste date sunt transmise prin rețea către serviciul de autentificare pentru identificarea utilizatorului și oferirea accesului în cadrul sistemului informațional. Întrucît traficul de rețea nu este criptat, toate datele ce sunt transmise între aplicația mobilă și serviciul de autentificare pot fi interceptate cu ușurință și utilizate pentru autentificarea în cadrul sistemului informațional sub identitatea unui alt utilizator.

*Soluții:*

Pentru înlăturarea acestor amenințări, este necesară securizarea comunicării între aplicația mobilă și serviciile web, prin utilizarea corectă a protocoalelor OAuth2 [2] și OpenID Connect [3], care asigură securitatea procesului de autentificare și autorizare în cadrul sistemului informațional.

**Fraudarea datelor**

*Amenințări:*

- atac de tip ”man in the middle” care permite modificarea datelor aflate în tranzit.

Pentru securizarea traficului între aplicația mobilă și server se utilizează un certificat TLS. Însă există riscul ca datele aflate în tranzit între aplicație și server să fie modificate, datorită unui atac de tipul ”man in the middle”. Cînd are loc o conexiune HTTPS între client și server, clientul verifică dacă certificatul este semnat de către o autoritate de certificare și dacă numele serverului corespunde cu numele comun specificat în certificat, însă nu se verifică dacă certificatul respectiv este certificatul pe care serverul îl utilizează. Această vulnerabilitate permite realizarea unui atac de tipul ”man in the middle” și interceptarea datelor confidențiale.

*Soluții:*

Soluția împotriva acestei amenințări constă în aplicarea unei măsuri de securitate, numită ”Certificate and public key pinning” [4]. Ea presupune încorporarea cheii publice a certificatului în aplicația mobilă, și întrucît doar un certificat predefinit este utilizat pentru a asigura o comunicare securizată, conexiunile cu alte certificate vor eșua. Un atacator va trebui să decompileze aplicația, să modifice codul sursă, și să asambleze din nou aplicația, pentru a face din nou, posibilă interceptarea datelor transmise prin rețea, acest lucru fiind dificil de realizat.

**Repudierea**

*Amenințări:*

- infectarea dispozitivelor mobile cu aplicații malițioase;
- atac de tip ”man in the middle” care permite modificarea datelor aflate în tranzit.

*Soluții:*

Repudierea poate fi evitată prin prevenirea amenințărilor și vulnerabilităților enumerate în acest articol.

**Dezvăluirea informațiilor**

*Amenințări:*

- lipsa accesului restricționat la datele utilizatorului;
- ingineria inversă a aplicației mobile;
- injectarea de cod malițios;
- pierderea depozitului mobil.

Lipsa accesului restricționat asupra datelor prelucrate de aplicația mobilă poate conduce la dezvăluirea informațiilor confidențiale persoanelor neautorizate. O altă amenințare este decompilarea aplicației mobile, ceea ce permite analiza codului sursă, modificarea acestuia, și injectarea codului malițios.

*Soluții:*

Aplicația mobilă trebuie să permită setarea unei parole, astfel încît pentru a avea acces la aplicația mobilă, este necesar de introdus parola setată. În așa mod nici un alt utilizator nu va putea avea acces la datele personale ale utilizatorului. Parola nu este stocată în clar, ci este stocată doar valoarea hash a parolei. Astfel, dacă se obțin drepturi privilegiate asupra dispozitivului mobil, parola nu va putea fi identificată.

Decompilarea codului sursă nu poate fi evitată, dar poate fi aplicată o măsură de protecția împotriva analizei codului sursă și modificării acestuia prin ofuscarea codului sursă înainte de generarea fișierului de distribuire a aplicației. Astfel, codul decompilat de către atacator va fi foarte dificil de analizat și modificat.

**Întreruperea funcționării serviciilor**

*Amenințări:*

- atacuri de tip DDoS;
- erori ale aplicației mobile;

*Soluții:*

Întrucît sistemului informațional are o arhitectură de tipul client-server, este necesar de asigurat disponibilitatea serverului. Aceasta poate fi realizat prin instalarea în fața serverului un server de tip reverse proxy, pe care este configurat un load balancer și un firewall.

**Ridicarea nivelului de privilegii**

*Amenințări:*

- obținerea drepturilor privilegiate asupra dispozitivului mobil.

Sistemele de operare pentru dispozitivele mobile au vulnerabilități care permit ridicarea nivelului de privilegii, ce permite utilizatorilor să acceseze orice informație stocată pe aceste dispozitive.

*Soluții:*

Datele confidențiale care sunt păstrate pe dispozitivele mobile trebuie să fie criptate utilizînd API expus de fiecare platformă. Sistemul de operare Android pune la dispoziție Keystore API [5], care permite stocarea cheilor criptografice într-un container făcînd accesarea acestora mult mai dificilă. Android Keystore diminuează accesul neautorizat asupra cheilor criptografice, prin prevenirea extragerii datele care formează cheia de criptare, fiindcă aceste chei sunt asociate cu dispozitivul mobil, astfel chiar dacă aceste chei sunt compromise, ele nu pot fi utilizate pe alte dispozitive mobile asupra aceleași aplicații moile. Sistemul de operare iOS oferă un mecanism similar de protecție a datelor criptate, utilizînd Keychain API [6].

## III. CONCLUZII

Managementul riscurilor aplicațiilor mobile reprezintă procesul de identificare, evaluare și control al riscurilor de securitate prezente într-o aplicație mobilă. Toate modelele de management al riscurilor urmează pași similari care formează procesul de modelare a riscurilor: identificarea, analiza, evaluarea, atenuarea și monitorizarea riscurilor. După ce are loc acest proces, există cîteva strategii care sunt aplicate riscurilor: reducerea riscurilor, partajarea riscurilor și acceptarea riscurilor.

## BIBLIOGRAFIE

[1] The STRIDE threat model. [Resursă electronică] - Regim de access: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx.

[2] OAuth 2 – OAuth. [Resursă electronică] - Regim de access: https://oauth.net/2/.

[3] OpenID Connect. OpenID. [Resursă electronică] - Regim de access: http://openid.net/connect/.

[4] Certificate and public key pinning. [Resursă electronică] - Regim de access: https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning.

[5] Android Keystore System. [Resursă electronică] - Regim de access: https://developer.android.com/training/articles/keystore.html.

[6] Keychain services. [Resursă electronică] - Regim de access: https://developer.apple.com/library/content/documentation/Security/Conceptual/keychainServConcepts/01introduction/introduction.html.