



Fișa disciplinei:

“Securitatea aplicațiilor mobile și cloud”

Domeniul / Specializarea: CALCULATOARE / SECURITATEA INFORMAȚIILOR ȘI A SISTEMELOR CIBERNETICE

Anul I / Semestrul I

Titularul cursului: s.l. dr. ing. Daniel Iercan, prof. dr. ing. Marius Marcu					
Colaboratori:					
Număr de ore total/Verificarea/Credite					
Curs	Seminar	Laborator	Proiect	Examinare	Credite
28	-	-	28	E	3

A. Obiectivele cursului

- ❖ Însușirea de către cursanți a cunoștințelor teoretice și aplicative, necesare pentru proiectarea, configurarea și operarea unei aplicații de tip cloud care să respecte standardele de securitate;
- ❖ Însușirea de către cursanți a cunoștințelor teoretice și aplicative, necesare pentru proiectarea, implementarea și testarea unei aplicații de mobile care să respecte standardele de securitate și protecție a datelor;
- ❖ Studiul acestei discipline are ca rezultat o pregătire de specialitate a cursanților punându-le la dispoziție cunoștințe din domeniul securității aplicațiilor mobile și cloud, cu ajutorul cărora să se poată alinia la progresul științei, să își dezvolte abilități de stocare și transfer în siguranță a datelor, de minimizare a suprafeței “expuse” a aplicațiilor de tip mobile și cloud și de gestionare în siguranță a secretelor (parole, chei de acces, etc.); să devină competenți pentru proiectarea și implementarea aplicațiilor de tip mobile și cloud la un standard ridicat de securitate.

B. Subiectele cursului

1. Introducere (2 ore)
 - 1.1. Noțiuni elementare despre cloud.
 - 1.2. Protocolul HTTPS
 - 1.3. Riscurile de securitate la care sunt expuse aplicațiile de tip cloud
 - 1.4. Avantajele și dezavantajele platformelor de cloud public din punctul de vedere al securității
2. Securitatea datelor unei aplicații de tip cloud (2 ore)
 - 2.1. Securitatea datelor stocate.
 - 2.2. Securitatea datelor în tranzit.
 - 2.3. Soluțiile oferite de o platforma cloud pentru stocarea cheilor de criptare
3. Protocoale de autentificare și autorizare (6 ore)
 - 3.1. Noțiuni elementare de autentificare și autorizare pentru protocolul HTTP
 - 3.2. Protocolul OAuth 2.0
 - 3.3. Protocolul OpenID Connect
 - 3.4. Furnizori externi de identitate
4. Izolarea și segmentarea rețelelor de calculatoare virtuale pentru a restrânge suprafața unei aplicații de tip cloud expusă atacurilor (2 ore)
 - 4.1. Noțiuni elementare de rețele de calculatoare virtuale.
 - 4.2. Principii de segmentare și izolare a rețelelor de calculatoare virtuale.
 - 4.3. Direcționarea traficului prin „reverse proxy”
5. Securitatea parametrilor de configurare, separarea și controlul accesului la resursele din producție. (2 ore)
6. Introducere în programarea aplicațiilor mobile (2 ore)

- 6.1. Arhitectura si componentele sistemului de operare Android
- 6.2. Concepte si modele de programare specifice Android
- 7. Proiectarea nivelului de securitate al aplicatiilor mobile (2 ore)
 - 7.1. Arhitecturi de aplicatii mobile si cloud
 - 7.2. Probleme de securitate al aplicatiilor mobile
 - 7.3. Securitatea datelor
 - 7.4. Securitatea comunicatiilor
- 8. Protectia datelor utilizatorilor aplicatiilor mobile (2 ore)
 - 8.1. Cadrul legal pentru protectia datelor (GDPR)
 - 8.2. Sistemul de permisiuni pentru aplicatiile mobile
 - 8.3. Modele si metode pentru colectarea si analiza datelor utilizatorilor
- 9. Implementare nivelului de securitate al aplicatiilor mobile (4 ore)
 - 9.1. Mecanismul de login
 - 9.2. Mecanisme de criptare pentru date
 - 9.3. Mecanisme de securizare a comunicatiei
 - 9.4. Tratarea sigură a notificărilor
 - 9.5. Eficientizarea utilizării mecanismelor de securitate
- 10. Testare nivelului de securitate al aplicatiilor mobile (2 ore)
 - 10.1. Metode si unelte pentru testarea aplicațiilor mobile
 - 10.2. Acoperirea codului prin testare
 - 10.3. Asigurarea calității codului
- 11. Publicarea si mentenanta aplicatiilor mobile (2 ore)
 - 11.1. Unelte pentru publicarea si mentenanta aplicatiilor mobile
 - 11.2. Soluții pentru semnarea, împachetarea și „obfuscarea” aplicațiilor
 - 11.3. Analiza și rezolvarea crash-urilor și ANR-urilor

C. Subiectele aplicațiilor (laborator, seminar, proiect)

Proiect:

Dezvoltarea unei aplicații mobile Android sau iOS cu backend de tip cloud pentru platforma de cloud public Microsoft Azure care să asigure securitatea datelor în tranzit și la stocare, să folosească Google ca furnizor de identități, să stocheze și să gestioneze parametrii de configurare criptat folosind Azure Key Vault. Datele aplicației vor fi stocate pe servere aflate într-o rețea virtuală separată față de rețeaua virtuală în care se află aplicația.

D. Bibliografie

1. Thomas Erl, Cloud Computing: Concepts, Technology & Architecture, Mai 2013, Prentice Hall
2. Advanced API Security: Securing APIs with OAuth 2.0, OpenID Connect, JWS, and JWE, August 2014, Apress
3. Alexandru Topirceanu, Marius Marcu, Introducere în programarea ANDROID, Editura Politehnica Timisoara, 2015.
4. Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse, The Mobile Application Hacker's Handbook, Wiley, 2015.

E. Evaluarea

Examen oral + aplicație pe calculator

Nota finală este compusă din media celor două note obținute: nota la examenul oral și nota obținută la evaluarea aplicației.

Data: 10.09.2018

Director de program de studii postuniversitare,

Prof. dr. ing. Bogdan GROZA

Titular de disciplină,

**S.I. dr. ing. Daniel Iercan,
Prof. dr. ing. Marius Marcu**