Securitatea Reţelelor (ROL) - Examen: iunie 2020

EXAMEN ONLINE - Instrucţiuni generale

1. Transmiteţi examenul **prin Moodle** până la termenul limită: **16 iunie, ora 09:55**.

   - Transmiterea corectă a examenului este strict în responsabilitatea voastră.
   - Transmiteţi în timp util, NU aşteptaţi ultimele minute pentru a încărca examenul. Examenul poate fi transmis de oricâte ori doriţi până la deadline, se ia în considerare doar ultima variantă transmisă. NU se acceptă ca motivaţie pentru netransmiterea examenului niciun fel de probleme tehnice (încetinirea platformei, utilizarea incorectă, nesincronizări ale ceasului, etc.).
   - Studenţii care nu transmit rezolvarea examenului scris sunt consideraţi absenţi.

2. Răspunsul trebuie să fie în **format .pdf, încărcat prin contul instituţional Moodle** în secţiunea corespunzătoare sub numele **grupa_nume_prenume.pdf**. Prima pagină a fişierului de răspunsuri trebuie să conţină **nume, grupă, o listă a subiectelor netratate** (ex.: *Subiecte netratate: 1(a), 1(c), 3(b).* sau -).

   - Este la latitudinea fiecărui student cum redactează examenul: scan al foilor scrise de mână (citeţ / lizibil!), Word / LaTeX exportat în pdf, etc.
   - Aveţi grijă ca fişierul final .pdf să fie valid şi rezolvările să fie uşor identificabile!

3. Se acordă punctaje parţiale. Răspunsurile greşite la examenul scris NU depunctează suplimentar.

4. Pentru promovare, **este obligatoriu să participaţi la ambele probe (examen scris şi oral) şi să obţineţi minim 22,5 puncte în final şi minim 45 de puncte** ca notă finală (include punctele obţinute în timpul anului, fără bonus, care se acordă doar în caz de promovare).

5. Pentru examenul oral:

   - Este strict în responsabilitatea voastră să verificaţi repartizarea pe zile / ore (aprox.) şi alte informaţii necesare referitoare la susţinerea examenului oral.
   - Trebuie să vă conectaţi **audio-video, folosind contul instituţional Teams**.
   - Trebuie să arătaţi **un act de identitate** (CI, paşaport, permis de conducere, etc.) **sau legitimaţie de student cu poză**. Este în responsabilitatea voastră să ascundeţi alte informaţii (altele decât numele şi poza) de pe documentul prezentat, pe care nu doriţi să le faceţi publice!
   - Fiecare subiect rezolvat în scris, dar pe care nu ştiţi să îl explicaţi (i.e., să arătaţi că l-aţi rezolvat individual sau înţeles), **se depunctează cu dublul punctajului alocat subiectului respectiv**.
   - Studenţii care transmit rezolvarea examenului scris dar nu participă la susţinerea orală obţin nota finală 4.
   - Dacă există studenţi care nu au posibilitatea unei conexiuni audio şi video, trebuie să anunţe în prealabil, pe e-mail (*ruxandra.olimid@fmi.unibuc.ro*).

- Specificaţi pe prima pagină a examenului scris dacă aveţi intervale orare în care nu puteţi susţine examenul oral.

Dacă în timpul examenului aveţi întrebări, le puteţi posta pe forum, secţiunile *Examen* sau *Întrebări exerciţii şi probleme examen*. Urmăriţi forumul pentru informaţii. **NU postaţi indicii sau soluţii!**

SUCCES!

EXAMEN ONLINE - Probleme

1. Răspundeţi cu adevărat sau fals. Dacă afirmaţia este falsă, scrieţi în locul acesteia o afirmaţie adevărată, modificând minimal afirmaţia iniţială (i.e., păstraţi contextul), dar nu corectaţi printr-o simplă negaţie.

   (a) Sistemele WPA/WPA2 enterprise folosesc o parolă comună pentru toţi utilizatorii. **(2p)**

   (b) Un sistem ar putea să ofere protecţie la integritate prin utilizarea unui Cyclic Redundancy Check (CRC). **(2p)**

   (c) Una dintre problemele grave ale WEP referitoare la confidenţialitate pentru care nu ar trebui utilizat este este complexitatea procesării. **(2p)**

   (d) În TKIP, rolul cheile pairwise sunt folosite pentru comunicaţia 1-la-1, iar cheile de grup pentru comunicaţia de tip broadcast. **(2p)**

   (e) Pentru a se putea realiza autentificarea utilizatorului prin 4G-AKA, serving network primeşte de la home network un hash al cheii K stocată pe SIM-ul utilizatorului. **(2p)**

   (f) În 5G, protecţia identităţii utilizatorului este realizată prin criptare simetrică. **(2p)**

   (g) Principiul separării cheilor se referă la faptul că utilizatori diferiţi pot genera chei de lungimi diferite. **(2p)**

   (h) Pentru a realiza un atac de tip DoS asupra dronei, autorii articolului *Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things* au injectat pachete ARP. **(2p)**

   (i) Pentru anumite variante de Android, atacul KRACK conduce la instalarea cheii 0-peste-tot din cauza unui bug in *wpa_authenticator*. **(2p)**

   (j) VLAN realizează un canal de comunicaţie sigur între noduri situate la distanţă. **(2p)**

2. **Incidente în reţeaua GSM**

   Un operator mobil a identificat o problemă în reţeaua GSM proprie. Aţi fost angajat ca şi consultant de securitate pentru analizarea incidentului. După o analiză iniţială aţi determinat că adversarul a dobândit acces neautorizat (wireless) la un BTS al operatorului de câteva luni, dar nu a acţionat activ.

   (a) Exemplificaţi ce acţiuni ar fi putut să realizeze adversarul, dacă este vorba despre un adversar pasiv. **(5p)**

   (b) Conexiunea dintre BTS şi BSC este wireless. Explicaţi la ce tip de date (criptate sau plaintext, ce tip de informaţii / mesaje, etc.) a avut acces adversarul. **(5p)**

   (c) Înaintaţi cu analiza şi descoperiţi că adversarul a reuşit să acceseze şi să descarce toate informaţiile stocate în AuC/HLR. Discutaţi impactul asupra securităţii. **(5p)**

   (d) Pe baza observaţiilor făcute până acum, daţi recomandări pentru a îmbunătăţii securitatea. **(5p)**

3. **WPA3 modificat**

Unul dintre colegi afirmă că a modificat WPA3 într-un mod sigur, protocolul modificat fiind ilustrat în figura de mai jos. Clientul şi Access Point-ul (AP) partajează parolă PWD care este codată printr-o funcţie f într-un punct P pe o curbă eliptică EC (i.e., $P = f(PWD)$, cu f publică). Curba eliptică EC şi numărul prim mare q folosite în cadrul protocolului sunt de asemenea publice.

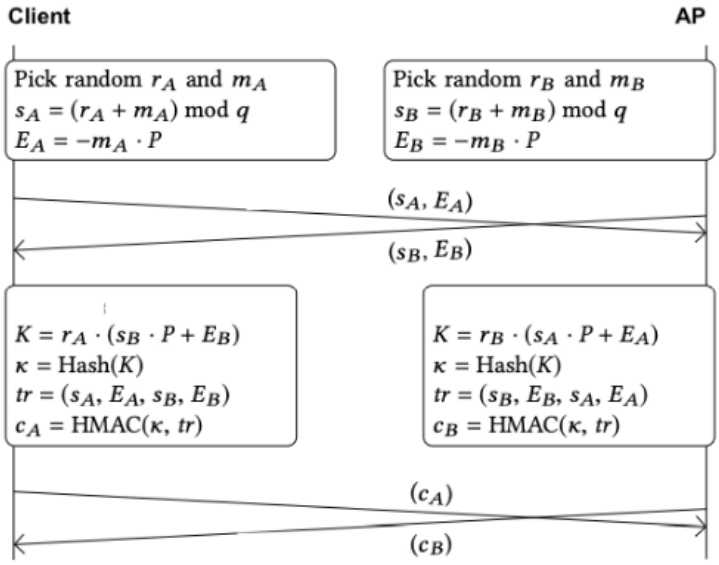

Figure 1: Sursă (înainte de modificare): M.Vanhoef and E. Ronen, Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd, Cryptology ePrint Archive: Report 2019/383

(a) Arataţi că AP-ul şi clientul calculează aceaşi cheie K. **(5p)**

(b) Clientul şi AP-ul folosesc o parolă PWD des întâlnită. Poate un adversar (care nu cunoaşte nimic despre parolă în afară de faptul că este o parolă des întâlnită) să determine cheia K? Consideraţi că Discrete Logarithm Problem (DLP) e uşoară pentru EC şi P, adică fiind date y şi P este uşor de calculat x astfel încât $y = xP$. **(5p)**

(c) Software-ul clientului şi al AP-ului au fost infectate de un program maliţios care afectează generatorul de numere pseudo-aleatoare. Aceasta conduce la faptul că m_A şi m_B sunt cu o probabilitate mare egale cu o valoare constantă VAL. Ce puteţi afirma despre securitatea sistemului? Discuţie. (Notă: acest punct este independent de punctul anterior, PWD poate fi o parolă puternică şi EC poate fi o curbă eliptică pentru care DLP este sigură.) **(5p)**

(d) Momentan propunerea se află în etapa de testare, dar colegul doreşte să o implementeze pentru comunicaţia internă (în cadrul companiei) săptămâna viitoare. Daţi un sfat (argumentat) colegului vostru. **(5p)**

TOTAL disponibile: 60p