

EXAMEN ONLINE - Probleme

1. Răspundeți cu adevărat sau fals. Dacă afirmația este falsă, scrieți în locul acesteia o afirmație adevărată, modificând minimal afirmația inițială (i.e., păstrați contextul), dar nu corectați printr-o simplă negație.
 - (a) Sistemele WPA/WPA2 enterprise folosesc o parolă comună pentru toți utilizatorii. **(2p)**
 - (b) Un sistem ar putea să ofere protecție la integritate prin utilizarea unui Cyclic Redundancy Check (CRC). **(2p)**
 - (c) Una dintre problemele grave ale WEP referitoare la confidențialitate pentru care nu ar trebui utilizat este complexitatea procesării. **(2p)**
 - (d) În TKIP, rolul cheile pairwise sunt folosite pentru comunicația 1-la-1, iar cheile de grup pentru comunicația de tip broadcast. **(2p)**
 - (e) Pentru a se putea realiza autentificarea utilizatorului prin 4G-AKA, serving network primește de la home network un hash al cheii K stocată pe SIM-ul utilizatorului. **(2p)**
 - (f) În 5G, protecția identității utilizatorului este realizată prin criptare simetrică. **(2p)**
 - (g) Principiul separării cheilor se referă la faptul că utilizatori diferiți 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 Wi-Fi 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 în *wpa_authenticator*. **(2p)**
 - (j) VLAN realizează un canal de comunicație sigur între noduri situate la distanță. **(2p)**

2. Incidente în rețeaua GSM

Un operator mobil a identificat o problemă în rețeaua GSM proprie. Ați fost angajat ca și consultant de securitate pentru analizarea incidentului. După o analiză inițială ați determinat că adversarul a dobândit acces neautorizat (wireless) la un BTS al operatorului de câteva luni, dar nu a acționat activ.

- (a) Exemplificați ce acțiuni ar fi putut să realizeze adversarul, dacă este vorba despre un adversar pasiv. **(5p)**
- (b) Conexiunea dintre BTS și BSC este wireless. Explicați la ce tip de date (criptate sau plaintext, ce tip de informații / mesaje, etc.) a avut acces adversarul. **(5p)**
- (c) Înaunțați cu analiza și descoperiți că adversarul a reușit să acceseze și să descarce toate informațiile stocate în AuC/HLR. Discutați impactul asupra securității. **(5p)**
- (d) Pe baza observațiilor făcute până acum, dați recomandări pentru a îmbunătății 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 și Access Point-ul (AP) partajează parolă PWD care este codată printr-o funcție f într-un punct P pe o curbă eliptică EC (i.e., $P = f(PWD)$, cu f publică). Curba eliptică EC și numărul prim mare q folosite în cadrul protocolului sunt de asemenea publice.

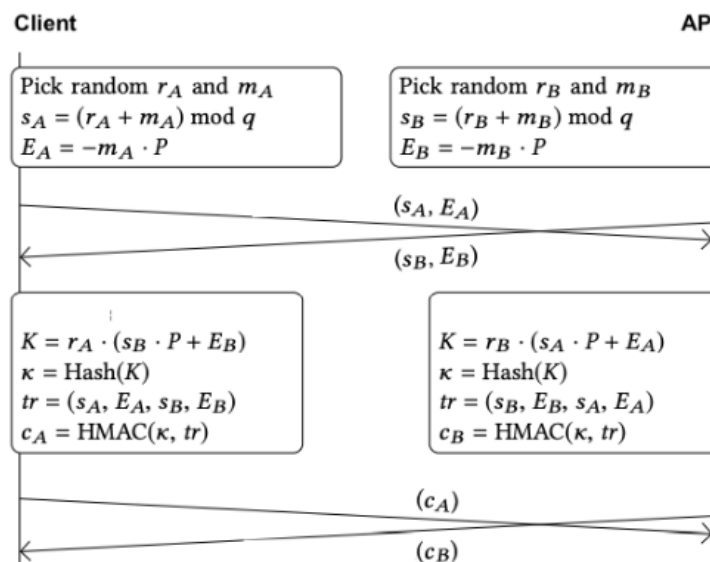


Figure 1: Sursă (înainte de modificare): M.Vanhoef and E. Ronen, Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd, Cryptology ePrint Archive: Report 2019/383

- Aratați că AP-ul și clientul calculează aceeași cheie K . (5p)
- Clientul și AP-ul folosesc o parolă PWD des întâlnită. Poate un adversar (care nu cunoaște nimic despre parolă în afară de faptul că este o parolă des întâlnită) să determine cheia K ? Considerați că Discrete Logarithm Problem (DLP) e ușoară pentru EC și P , adică fiind date y și P este ușor de calculat x astfel încât $y = xP$. (5p)
- Software-ul clientului și al AP-ului au fost infectate de un program malițios care afectează generatorul de numere pseudo-aleatoare. Aceasta conduce la faptul că m_A și m_B sunt cu o probabilitate mare egale cu o valoare constantă VAL . Ce puteți afirma despre securitatea sistemului? Discuție. (Notă: acest punct este independent de punctul anterior, PWD poate fi o parolă puternică și EC poate fi o curbă eliptică pentru care DLP este sigură.) (5p)
- Momentan propunerea se află în etapa de testare, dar colegul dorește să o implementeze pentru comunicația internă (în cadrul companiei) săptămâna viitoare. Dați un sfat (argumentat) colegului vostru. (5p)

TOTAL disponibile: 60p