CryptTalk
www.crypttalk.com

Biztonságos mobilalkalmazás-fejlesztés a gyakorlatban

A CryptTalk fejlesztése során alkalmazott módszerek

Dr. Barabás Péter

Arenim Technologies

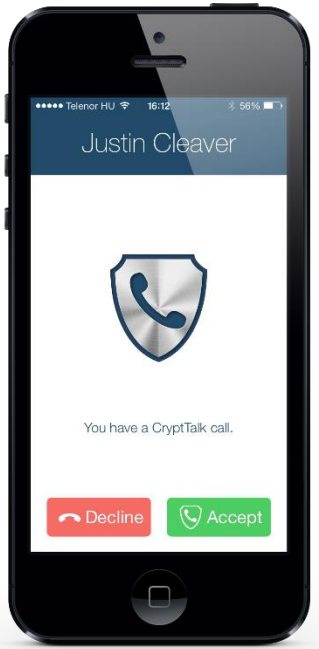
Agenda

- CryptTalk
- Hálózati kommunikáció
- Authentikált kérések
- Adatvalidáció
- Kliens adattárolás
- Jailbreak detekció
- Memóriavédelem
- Eredmények

ARENIM

CryptTalk

- Kliens oldal
  - Saját fejlesztésű kiforrott VoIP motor, SIP
  - Több mint 100 millió sikeres hívás 2013-ig
  - Peer-to-peer hívásfelépítés
  - Platform független kód
  - Software alapú megoldás, nincs szükség speciális hardware-re
- Szerver oldal
  - Presence, Regisztráció és kontakt kezelés
  - CA, Tanusítvány kezelés
  - OTP Autentikáció: a szerver végzi jelszó nincs tárolva a kliensen



ARENIM

Hálózati kommunikáció - SSL

- SSL certificate pinning
  - Szerver tanúsítvány → Bundle
    - Előny: támadó nem tudja a bináris hozzáférés nélkül lecserélni
    - Hátrány: tanusítvány megújítása esetén újrafordítás, publikálás
- Kliens authentikáció
  - Kliens tanúsítvány → Bundle
  - Jelszó kezelés:
    - Ahogyan NE: normál sztring konstansként
    - Ahogyan IGEN: valamilyen algoritmus rakja össze és adja vissza

ARENIM

Hálózati kommunikáció II. - SSL

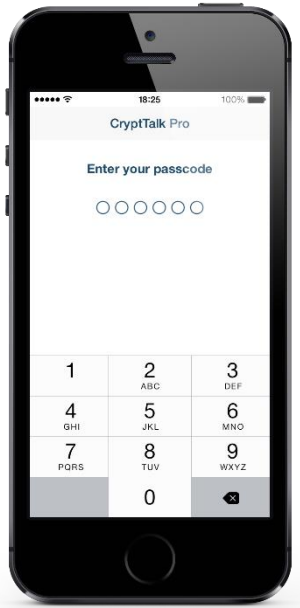
- Példa kliens tanúsítvány jelszavának tárolására
  - Jelszó: A1b2C3d4E5f6G7h8

1. Vegyünk egy nevezetes sorozatot, pl. Recamán, Fibonacci
2. Számítsuk ki a letárolandó byte tömb értékeit a következőképpen:
   1. T[i] = Sorozat[i] + ASCII(jelszo[i])
3. Jelszó generálásnál végezzük az előző lépéseket fordítva:
   1. PWD[i] = T[i] – Sorozat[i]
   2. Vegyük a PWD byte tömböt, mint jelszó sztringet
4. Végül, amikor már nincs szükség rá, írjuk felül a memóriában a PWD tömböt.

ARENIM

Authentikált kérések - OTP

- Authentikált kérések
  - statikus jelszó
  - Dinamikus jelszó + PIN védelem
    - One-Time Password (OTP) mechanizmus
    - HOTP
      - OTP = HOTP_ALG(OTP-kulcs, counter)
- Azonosítás: userId + OTP
- Problémák:
  - OTP-kulcs, counter tárolás
  - Brute-force támadás
  - User blokkolás



ARENIM

Authentikált kérések II. - OTP

- OTP-kulcs tárolás:
  - Fájlban, titkosítva (ECB mód)
  - Titkosítás kulcsa: user PIN + salt
    - Mindez PBKDF2-vel pár 1000x megpörgetve
  - Minden PIN próbálkozásra kapunk OTP-t eredményül
    - Az OTP validálás a szerver dolga
- Counter tárolása pl. keychain-ben
- Counter elcsúszás elleni védelem (időablak)

ARENIM

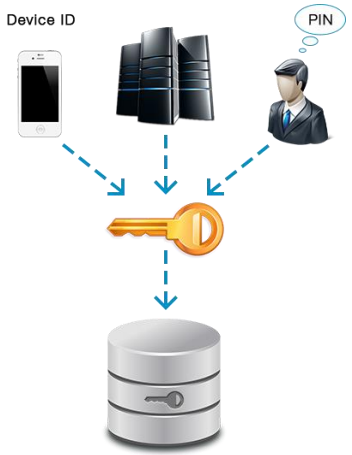
Authentikált kérések III. – OTP

- Brute-force támadás:
  - userId + OTP pár kipörgetése
  - Megoldás:
    - a szerver a userID-t X db sikertelen próbálkozás után blokkolja
  - Következmény:
    - Egy valós user könnyen kiblokkolható néhány fals userID+OTP kéréssel

ARENIM

Authentikált kérések IV. - OTP

- UserID blokkolás kivédése
  - „Device-függő” kérések
  - Aktuális deviceID generálás + regisztrálás a user-hez
  - DeviceID küldése minden kérésben
- Authentikált kérés paraméterek:
  - UserID + DeviceID + OTP
- Következmény:
  - Hibás userID + OTP-vel nem blokkoljuk a user-t X db próbálkozás után
  - Csak a userID-hoz regisztrált deviceID-val fogadható el a kérés



ARENIM

Adatvalidáció

- Szerver oldalon
  - Kérés feldolgozása
  - Paraméterek vizsgálata
    - Szigorú validációs szabályok
    - Hossz korlátozás, valid karakterek, értékek, regexp, stb.
    - Whitelist alapon
- Kliens oldalon
  - Ugyanazok a szabályok, mint szerver oldalon
  - Mit validáljunk?:
    - Minden user inputot
    - Minden szerver kérést + választ

ARENIM

Kliens adattárolás

- Fájl, adatbázis, keychain (iOS), memória, … ?
- Keychain jó lehet, de!
  - Jailbreak esetén könnyen dumpolható
- Fájl
  - Egyszerű adatokra, titkosítva
- Adatbázis
  - Összetett, strukturált adatokra, titkosítva
- Memória
  - Alkalmazás futása idejéig, ideiglenes adatokra

ARENIM

Kliens adattárolás II. – Adatbázis példa

- Adatbázis: sqlite + sqlcipher
- Kérdések:
  - Adatbázis kulcs mi legyen?
  - Hol tároljuk az adatbázis kulcsát?

ARENIM

Kliens adattárolás III. – DB kulcs

- Két komponens
  - Szerver oldali kulcsrészlet (Ks)
  - Kliens oldali kulcsrészlet (PIN_hash + salt)
- DB kulcs:
  - PBKDF2(Ks, PBKDF2(PIN_hash, salt, 4096), 4096)
  - Ks authentikált kérés válaszában kerül a kliensre
  - Töröljük a memóriából, amint nincs rá szükség
- Tárolandók:
  - Szerver oldalon DB-ben: Ks
  - Kliens oldalon keychain-ben: salt

ARENIM

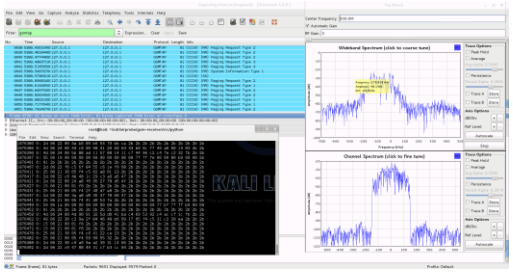
Jailbreak detekció

- Nincs tökéletes módszer
- Néhány népszerű módszer:
  - Bash test - fopen(„/bin/bash”,”r”)
  - Hosts test - fopen(„/etc/hosts”,”a”)
  - FileExistsAtPath tests - @”/bin/apt”, @”/usr/sbin/sshd”, @”/Applications/Cydia.app”
  - Fstab test - stat(„/etc/fstab”, &sb) → result>=0 || size != 80
  - Shell test - system(0)
  - SignerIdentity test
  - Dyld test
  - Fork test

ARENIM

Memóriavédelem

- Érzékeny adatokat, amint nincs rá szükség töröljünk
  - Nem elég nil-lé tenni
  - WIPE!!! → írjuk felül random értékkel
- Debugging detekció (PTRACE)



```
void* handle = dlopen(0, RTLD_GLOBAL | RTLD_NOW);
ptrace_ptr_t ptrace_ptr = dlsym(handle, "ptrace");
ptrace_ptr(PT_DENY_ATTACH, 0, 0, 0);
dlclose(handle);
```

ARENIM

Összegzés

- Biztonság fontossága
- Alkalmazásonként változhatnak a biztonsági szintek, igények
- Legfontosabb védendő területek
  - Felhasználói interakció
  - Hálózati kommunikáció
  - Adattárolás
  - Fizikai védelem
- Amiről még lehetne beszélni
  - Szerver infrastruktúra védelem
    - Tűzfalszabályok, route-ok
  - Tanúsítvány kiállító működése, konfigurálása
  - Hangkommunikáció titkosítása

ARENIM

Eredmények

- **CryptTalk 2.3.1**
  - **2014. november 6. : Ready for Sale**
  - Publikus verzió
  - 1 havi ingyenes „trial” időszak
- CryptTalk 2.4.0 (Pro verzió)
  - 2014. október 30. : Ready for Sale
  - Üzleti verzió
  - Konferencia funkcióval

ARENIM

Köszönöm a figyelmet!

ARENIM TECHNOLOGIES

CryptTalk
www.crypttalk.com

Kapcsolat:

Dr. Barabás Péter

Director of Software Development

peter.barabas@arenim.com

+36 70 314 56 57