Felhő alapú mobilalkalmazások biztonsága

Budai Péter, Mikó Norbert
Vezető szoftverfejlesztők, Tresorit Kft.

Miről lesz szó?

- **A Tresorit szolgáltatás és platformjainak gyors bemutatása**
- **A Tresorit szoftver architektúrája**
  - Hogyan épül fel?
  - Miért?
- **Mobilalkalmazások biztonsági kérdései**
  - Mit kell védeni? Mi ellen kell védekezni?
  - Milyen megoldásokat nyújtanak a készülékgyártók, illetve a Tresorit?
- **Összefoglalás**

Tresorit - biztonságos kollaboráció 8 platformon

- **Biztonságos kollaborációs szoftver**
  - Fájlok tárolása, szinkronizációja és megosztása a felhőben
  - Magas szintű biztonság, kliens oldali titkosítás

- **8 platform**
  - Desktop
    - Windows, Mac OS X, Linux
  - Mobil
    - Android, iOS, BlackBerry, Windows Phone
  - Web

tresorit

A Tresorit háromszintű architektúrája

- **Kliens alkalmazások**
  - Platform "natív" eszközkészlet és nyelv
- **Kriptográfiai köztes réteg**
  - "Core" library
  - C++
  - Beépül a kliensekbe
  - Szerver elérés
- **Tároló és kiszolgáló szerverek**
  - Microsoft Azure szolgáltatások

tresorit

Miért így épül fel?

- **Kliens oldali titkosítás**
  - Számításigényes műveletek
    - Gyorsabb működés
    - Jobb üzemidő
- **Fejlesztés gyorsítása**
  - Jelentős kliensoldali logika
  - Hibalehetőségek minimalizálása
- **Könnyű kezelés és fejlesztés**
  - Natív, megszokottabb felhasználói felület
    - A operációs rendszer összes szolgáltatása elérhető a platform natív nyelvéből
  - Egyszerűbb szerver-kliens kommunikáció

Mobilalkalmazások biztonsági kérdései

- Mit védünk?
  - Felhasználó személyes adatai
  - Alkalmazás, mint szellemi tulajdon
- Mi ellen védekezünk?
  - Ellopott, elvesztett eszközök
  - A készüléken futó más alkalmazások
  - Készülékgyártók
  - Telefon- és internetszolgáltók
  - Rosszindulatú támadók

Ellopott, elvesztett eszközök

- Platformok megoldásai
  - Passcode, PIN, unlock jelszó
  - Biometrikus azonosítás a kényelmesebb használat kedvéért
    - Lehetséges az alkalmazásokkal is integrálni
    - iOS - Minden újabb készülék (iPhone 4+)
    - Android - Kezdenek megjelenni az új készülékekben
  - Minden platformon összekötve a háttértár titkosítással
    - iOS - Full storage encryption
    - Android - 5.0+ Full disk encryption
    - WP – BitLocker
  - Távoli törlés
    - Szintén mindhárom platformon létezik (Find My Phone / Device Manager)
    - Aktív hálózati kapcsolat szükséges
    - Egyéb funkciók: távoli lezárás, üzenet kiírása a kijelzőre (Android)

Ellopott, elvesztett eszközök

- Mit tehetünk még?
- A Tresorit megoldásai
  - Lokálisan titkosított adatok
    - Az operációs rendszertől független kulcsokkal
    - Figyelni kell rá, hol tároljuk ezeket a fájlokat
  - Eszközkezelési lehetőségek
    - Elhagyott eszközök letiltása - kliens és szerver oldalon is
    - Bizonyos platformok, IP címtartományok, országok tiltása vagy engedélyezése

A készüléken futó más alkalmazások

- Platformok megoldásai
  - Sandboxing
    - Az alkalmazás csökkentett jogosultságokkal fut
    - Külön jogosultság kérés: Contacts, Location, Photos, Internet
  - Védi mind a rendszert mind pedig a felhasználót, illetve az alkalmazásokat egymástól
    - Adatok megosztásához appok között különböző lehetőségek vannak, sokkal formálisabb
  - Apponként ki- és bekapcsolható
    - Android 6.0+ és iOS – Futás közben kér jogosultságot az alkalmazás, egyszeri alkalomra vagy örökre, később letiltható
    - Android 6.0- és Windows Phone – Telepítéskor engedélyezzük a jogosultságokat, mindent vagy semmit alapon
- Jailbreak/rooting problémát jelent

Készülékgyártók

- Kényelmi szolgáltatások
  - Meglehetősen szabadon kezelik adatainkat
- Backup/restore
  - iOS - iCloud Backup
    - Automatikus biztonsági mentés a felhőbe
    - Figyelni kell, érzékeny adatokat hova helyezünk
      - Az alkalmazás sandboxából némely mappákat nem backupol
      - Illetve explicit kikapcsolni is lehet barmely mappára vagy fájlra
  - Android
    - Nincs alapértelmezett biztonsági mentés
    - Erre a célra léteznek alkalmazások, illetve fejlesztői eszközökkel oldható meg
      - Fejlesztő tilthatja, hogy ezek a backup solutionok láthassák az alkalmazás adatait
      - Sajnos gyakoriak a root jogot igenylő backup szoftverek, ahol ez nem segít
  - WP
    - Ki- és bekapcsolható központi biztonsági mentés OneDrive tárhelyre
    - Nagyon hasonlít az iOS megoldásához, de opt-out helyett opt-in jellegű

Telefon-, internet- és felhőszolgáltatók

- A hálózaton átmenő forgalom hozzáférhető
  - Mobilszolgáltatók, nyilvános Wi-Fi hotspotok
  - Titkosított hálózati kapcsolatot használujunk
    - A Tresorit a TLS 1.2 csatornán kommunikál minden esetben
    - Szerver és kliens oldali authentikáció X.509 tanúsítványok segítségével
- A felhőben tárolt adatok is hozzáférhetőek a szolgáltató felé
  - Felhasználják a szokásaink elemzésére
  - Esetleges hacker támadás esetén ők is hozzáférnek
    - Nem segít a szerver oldali titkosítás
  - A Tresorit megoldása a kliens oldali titkosítás
    - Még feltöltés előtt
    - A mi adminisztrátoraink sem férnek a felhasználó adataihoz

Rosszindulató támadók

- Az eddig felsorolt elemek ez ellen is védenek
  - Jelkódok
  - Kliens oldali titkosítás
    - Lokálisan tárolt és feltöltött adatokra is
  - Sandboxing
  - Titkosított adatkapcsolat
- A felhasználónak meg kell bíznia az operációs rendszerben
  - Egy hiba mindig kihasználható
  - Érdemes a saját alkalmazásunkba is védelmet beépíteni
    - Az operációs rendszertől független megvalósítással
- A felhasználónak meg kell bíznia az alkalmazásban

Rosszindulató támadók

- Alkalmazás aláírás
  - A cél, hogy a felhasználó meggyőződhessen, hogy az alkalmazás megbízható forrásból érkezik
  - iOS
    - Nagyon jól kitalált, komplex rendszer
      - Certificates, Provisioning Profiles, Signing identites
    - Apple által kiállított tanúsítványokkal
    - Egy app aláírása csak addig él amíg a fejlesztő feltölti az AppStore-ba
      - Utána ők egy saját tanúsítvánnyal irják alá, ezt fogadja csak el az iOS
    - Adhoc Distribution rendszer enterprise alkalmazásokhoz
  - Android
    - Publikus/privát kulcspár a fejlesztőnél, azzal kell digitálisan aláírni az alkalmazást
      - Ha kompromittálódik, nem lehet visszavonni, egy teljesen új alkalmazást kell létrehozni a Play Store-ban.
  - Windows Phone
    - Fejlesztő nem, csak a Microsoft írja alá a Store-ban feltöltött alkalmazást
    - Itt is létezik enterprise distribution

Köszönöm a figyelmet! Kérdések?