Jegyzőkönyv

Biztonság és védelem az informatikában c. tárgy

13. feladat

Készítette:

Csomor Bence, TVIK4I

2021.05.12.

**Tanúsítványok**

Tanúsítvány általános feladata:

Publikus kulcsú infrastruktúrában a tanúsítványok feladata elsősorban egy adott publikus kulcs és az ahhoz tartozó titkos kulcs összekapcsolása. Ugyanakkor a tanúsítványoktól elvárjuk, hogy rendelkezzen mindazokkal a tulajdonságokkal, amikkel mondjuk egy személyi igazolvány vagy egy bankkártya. Elvárjuk, hogy az egyes személyek szervezetek azonosítását, kezelését épp olyan, de inkább nagyobb biztonsággal el tudjuk végezni, mint ahogy azt az offline megfelelőikkel természetesen és magától értetődően tesszük. Elvárjuk tőlük mindazt a biztonságot és kényelmet és természetesen azt, hogy ezt a modern hálózati környezetben hajtsa végre.

Három verziója létezik ezeknek a tanúsítványoknak:

Az X509-es tanúsítvány az 1988-ban kiadott CCITT X509 -es ajánlásról kapta a nevét. Ebben az ajánlásban definiálták ugyanis a szabvány első verzióját. Ez a tanúsítvány még kizárólag az X500 Directory -hoz készült, annak az azonosítását volt hivatott kezelni. Később a hangsúly eltolódott egy általánosabb megközelítés felé. Idővel két a szabvány két további verziója látott napvilágot. A második verzió egyetlen újítást hozott, mégpedig a nevek újrafelhasználhatóságát. Napjainkban a legtöbb alkalmazás a harmadik verziót használja (X509v3). A harmadik verzió több kiterjesztést is definiál a formátumhoz, amelyek különböző plusz információk feltűntetését teszik lehetővé a tanúsítványban. Ezeknek a kiterjesztéseknek a használatát az egyes alkalmazások hivatottak kezelni és a vonatkozó megoldások alkalmazásról alkalmazásra változnak.

Tanúsítvány felépítése:

A szabvány szerint az X509 tanúsítvány három részből áll. A teljes tanúsítványt magában foglalja egy úgynevezett "módosításjelző boríték". Ez a gyakorlatban annyit jelent, hogy mindent, ami ezen a borítékon belül van, azt digitálisan aláírunk. A borítékon belül van a tanúsítvány tartalom és ez pedig opcionálisan tartalmazhat egy vagy több tanúsítvány kiegészítést.

Hierarchia:

A nyilvános kulcsú infrastruktúrában kiemelt fontossággal bír a bizalom. Az infrastruktúra feladata, hogy a bizalmat, a megbízhatóságot továbbítsa és kezeskedjen az egyes szereplőkért, illetve tanúsítványokért. A nyilvános kulcsú infrastruktúra kapcsán alapvetően kétféle bizalomról beszélhetünk. Egyrészt a bizalom jelentheti egy adott tanúsítvány megbízhatóságát, azt a tényt, hogy a vonatkozó titkos kulcs valóban annak a birtokában van, akinek az adatai a tanúsítványban szerepelnek. Másrészt egy teljesen általános értelemben vett bizalomról is szó lehet, ahol egy adott entitástól egy meghatározott viselkedést várunk el. Az ebben az értelemben vett bizalom természetesen nem lehet teljes bizonyosságú, amikor emberi tényezőkről van szó.

A Szigorú hierarchia moddeljének sok változata, bővítése van.

Szigorú hierarchia:

A szigorú hierarchiánál az egyes hitelesítő szervezetek (CA - Certificate Authority) egy fa-struktúrába vannak rendezve. A fa gyökerében álló hitelesítő szervezet a gyökér CA, vagy más néven a bizalmi horgony. A modell alapja, hogy a rendszer minden szereplője megbízik a gyökérben. Ebből indul ki a bizalom továbbadása a tanúsítványláncon. A modell működésének előfeltétele, hogy a hierarchia minden résztvevője birtokában legyen a bizalmi horgony saját maga által aláírt tanúsítványának. Ezt a biztonság érdekében nem internetes csatornákon kell továbbítani vagy ellenőrizni. Tipikus megoldás a gyökér tanúsítványának valamilyen digitális ujjlenyomattal, ellenőrző összeggel való megerősítése. Ebben az esetben természetesen az ellenőrző összeget kell nem elektronikus csatornákon felülvizsgálni.

Tanúsítvány kiszolgáló és szerepe:

A tanúsítvány egy nyilvános kulccsal, kiszolgálóval és az azért felelős szervezettel kapcsolatos egyéb információk terjesztésére használt módszer.

Biztonságos kiszolgáló nyilvános kulcsú titkosítás használatára való beállításához a legtöbb esetben el kell küldenie a hitelesítési kérést, a cég azonosságának bizonyítékát, valamint a CA díjazását. A CA ellenőrzi a hitelesítési kérést és az azonosságot, majd visszaküldi a biztonságos kiszolgálóhoz használható tanúsítványt.

Certificate Revocation List (Tanúsítvány visszavonási lista):

A Certificate Revocation List (CRL) olyan tanúsítványok listája, amelyek az érvényességi idejük alatt lettek törölve és ma már nem megbízhatóak. Az idő előtti törlés oka az esetek többségében a nyilvános kulcs rossz hírbe kerülése, kompromittálódása. Ezt a listát minden hitelesítő hatóság kiadja a tanúsítványai számára és elérhetővé teszi a saját weboldalán. A lista a tanúsítvány érvényességének ellenőrzésére szolgál.

Hash szerepe tanúsítványok esetében:

A hasht a biztonságos adathasználatra használják az interneten, digitális aláírások és cripto valuták esetében is. A digitális aláírás egy bonyolult matematikai és kriptográfiai megoldás. Az ezt lehetővé tevő eljárás igen fontos eleme az un. HASH függvény alkalmazása.

Lényege, hogy egy tetszőleges hosszúságú dokumentumhoz egy belőle létrehozott, állandó hosszúságú un. stringet, srítményt fznek. Az eredeti dokumentum a bemenet (input), a srítmény a kimenet (output). Minden dokumentumhoz más-más string tartozik és a string létrehozása gyors, egyszer folyamat. A HASH a következő tulajdonságok miatt alkalmas aláírás („digitális ujjlenyomat”) készítésére:

* gyakorlatilag nem létezik két olyan input, ami azonos outputot generál,
* egy létező outputhoz az eredeti inputtól eltérő inputot nem lehet konstruálni úgy, hogy a HASH függvény ahhoz is azonos outputot rendeljen,
* a dokumentumban eszközölt egy bit módosítás a kimenet több bitjét módosítja.

A leggyakrabban alkalmazott HASH függvény a Standard Hash Algoritmus, SHA. Itt az input tetszőleges hosszúságú (maximum 2^64 bit), a kimenet pedig 160 bit hosszú. Ez a hash érték.

Az aláírási folyamat tekintetében a dokumentum létrehozásakor és annak feldolgozásakor (olvasás) végzett tevékenység vizsgálandó. Ebben a folyamatban három fél vesz részt:

a dokumentum aláírója, a dokumentum olvasója, a hitelesítés szolgáltató.

Aláírónak nevezzük azt a személyt, aki saját aláírását az elektronikus iraton elhelyezi.

Az olvasó az a személy, aki az elektronikus iratot megkapja, és a más által elhelyezett aláírást ellenőrzi.

A hitelesítés szolgáltató (certificate provider, CP) az a személy vagy szervezet, amely az aláírás létrehozásához szükséges eszközök (software, hardware) és kulcsok kiadását végzi. Ezek kiadásakor az aláíró személyazonosságát ellenőrzi, és ennek eredményeként egy un. tanúsítványt állít ki.

források:

<https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0046_informatikai_biztonsag_es_kriptografia/ch11s07.html>

<https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0046_informatikai_biztonsag_es_kriptografia/ch11s05.html>

<http://sugo.ubuntu.hu/10.04/html/serverguide/hu/certificates-and-security.html>

<https://www.sslmarket.hu/ssl/help-szojegyzek>

<https://www.jogiforum.hu/files/publikaciok/szk_meh_ea_tv.pdf>