Bevezetés a kiberbiztonságba és biztonságtudatosság

Digitális identitás

Szarvák Anikó

2023. Tavasz

Jogosultság kezelési módszerek, megoldások

- Access Control List – ACL,
- Discretionary Access Control – DAC,
- Mandatory Access Control – MAC,
- Role Based Access Control – RBAC,
- Attribute Based Access Control – ABAC,
- Bell-LaPadula modell
- Clark-Wilson modell

+ Megvalósítások.

ACL

A számítógépes biztonságban a hozzáférés-vezérlési lista (ACL) a rendszererőforráshoz (objektumhoz) társított engedélyek listája.

Az ACL meghatározza, hogy mely felhasználók vagy rendszerfolyamatok kapnak hozzáférést az objektumokhoz, valamint hogy milyen műveletek engedélyezettek az adott objektumokon.

A tipikus ACL minden bejegyzése meghatároz egy tárgyat és egy műveletet. Például, ha egy fájlobjektum rendelkezik ACL-lel, amely tartalmazza

DAC

A számítógépes biztonságban a diszkrecionális hozzáférés-szabályozás (DAC) egyfajta hozzáférés-szabályozás, amelyet a Trusted Computer System Evaluation Criteria (TCSEC) határoz meg, amely eszközként korlátozza az objektumokhoz való hozzáférést az alanyok és/vagy csoportok identitása alapján tartoznak.

Az ellenőrzések diszkrecionálisak abban az értelemben, hogy egy bizonyos hozzáférési engedéllyel rendelkező alany képes ezt az engedélyt (talán közvetetten) átadni bármely más alanynak (hacsak nem korlátozza a kötelező hozzáférés-szabályozás).

MAC

A számítógépes biztonságban a kötelező hozzáférés-szabályozás (MAC) a hozzáférés-szabályozás egy olyan típusát jelenti, amellyel az operációs rendszer vagy az adatbázis korlátozza az alany vagy a kezdeményező azon képességét, hogy hozzáférjen egy objektumhoz vagy célhoz, vagy általában valamilyen műveletet hajtson végre azokon.

Az operációs rendszerek esetében az alany általában egy folyamat vagy szál; Az objektumok olyan konstrukciók, mint a fájlok, könyvtárak, TCP/UDP portok, megosztott memória szegmensek, IO-eszközök stb.

Az alanyok és objektumok mindegyike rendelkezik biztonsági attribútumokkal.

RBAC

A számítógépes rendszerek biztonsága, a szerepkör-alapú hozzáférés-vezérlés (RBAC) vagy a szerepalapú biztonság egy olyan megközelítés, amely a rendszerhez való hozzáférést az engedélyezett felhasználókra korlátozza.

Ez egy megközelítés a kötelező hozzáférés-vezérlés (MAC) vagy a diszkrecionális hozzáférés-vezérlés (DAC) megvalósítására.

A szerepkör alapú hozzáférés-vezérlés egy házirend-semleges hozzáférés-vezérlési mechanizmus, amely szerepkörök és jogosultságok köré épül.

ABAC

Az attribútum-alapú hozzáférés-vezérlés (ABAC), más néven IAM szabályzatalapú hozzáférés-vezérlés, egy hozzáférés-vezérlési paradigmát határoz meg, amelyben az alany jogosultságát egy műveletkészlet végrehajtására az alanyhoz, objektumhoz, kért műveletekhez társított attribútumok kiértékelése határozza meg, és bizonyos esetekben a környezeti jellemzők is.

Az ABAC egy olyan hozzáférés-vezérlési házirendek megvalósítási módja, amely nagymértékben adaptálható, és az attribútumok széles skálájával testreszabható, így alkalmas elosztott vagy gyorsan változó környezetben való használatra.

Bell-Lapadula modell

A Bell–LaPadula Modell (BLP) egy állapot-gép-modell, amelyet kormányzati és katonai alkalmazások hozzáférés-szabályozásának kikényszerítésére használnak.

David Elliott Bell és Leonard J. LaPadula fejlesztette ki Roger R. Schell határozott útmutatása nyomán az US Védelmi Minisztérium (DoD) többszintű biztonsági (MLS) szabályozására.

A modell a számítógépes biztonsági politika formális állapot-átmeneti modellje, amely olyan hozzáférés-szabályozási követelményeket ír le, amelyek biztonsági címkéket használnak az objektumokon és engedélyeket az alanyok számára.

A biztonsági címkék a legérzékenyebbtől (pl. "Szigorúan titkos"), egészen a legkevésbé érzékenyekig (pl. "Nem minősített" vagy "Nyilvános") terjedhetnek.

A Bell–LaPadula modell egy olyan modell példája, ahol nincs egyértelmű különbség a védelem és a biztonság között.

Clark-Wilson modell

A Clark–Wilson integritási modell alapot biztosít egy számítástechnikai rendszer integritási szabályzatának meghatározásához és elemzéséhez.

A modell elsősorban az információs integritás fogalmának formalizálására irányul. Az információk integritását azáltal tartják fenn, hogy megakadályozzák a rendszerben lévő adatelemek sérülését hiba vagy rosszindulatú ok esetén.

Az integritási szabályzat leírja, hogy a rendszerben lévő adatelemeket hogyan kell érvényben tartani a rendszer egyik állapotától a másikig, és meghatározza a rendszerben lévő különféle állapotok követelményeit.

A modell biztonsági címkéket használ, hogy hozzáférést biztosítson az objektumokhoz átalakítási eljárásokon és egy korlátozott interfész modellen keresztül.

Megoldások

- LDAP
- Kerberos
- AD
- SAML
- OpenID

LDAP

Az LDAP a Lightweight Directory Access Protocol rövidítése. Ez a protokoll directory szolgáltatások elérését szabályozza.

LDAP RFC: https://ldap.com/ldap-related-rfcs/

Az LDAP-protokollnak számos megvalósítása van, mint például:

- OpenLDAP,
- Apple Open Directory,
- Microsoft Active Directory.

AD

Az Active Directory, röviden AD a Microsoft egyes hálózati szolgáltatásainak gyűjtőneve, ezek:

- X.500-alapú, LDAPv3 protokollal lekérdezhető, elsősorban Microsoft Windows-környezetben használatos címtárszolgáltatás;
- Kerberos protokoll-alapú autentikáció;
- DNS-alapú névszolgáltatás és egyéb hálózati információk.

AD (folyt.)

Egy Active Directory-címtár legmagasabb szintje az erdő (forest), ami egy vagy több bizalmi kapcsolatokkal (trust) összekötött tartományt (domain) magába foglaló egy vagy több fa (tree) összessége. A tartományokat DNS-beli névterük azonosítja. A címtár objektumait a Directory Information Tree (címtárinformációs fa, DIT) adatbázisa tárolja, ami három partícióra bomlik, ezek:

- az objektumok tulajdonságait leíró sémapartíció (schema partition),
- az erdő szerkezetét (tartományokat, fákat, helyeket) leíró konfigurációs partíció(configuration partition) és
- a tartomány objektumait tartalmazó tartományi partíció (domain partition). Ezeken kívül létezhetnek alkalmazáspartíciók (application partition) is.

Kerberos

A Kerberos egy számítógépes hálózati hitelesítési protokoll, amely egy nem biztonságos hálózaton keresztül úgy teszi lehetővé a csomópontok közötti kommunikációt, hogy biztonságos módon igazolják személyazonosságukat egymás felé.

Tervezőinek elsődleges célja egy kliens-szerver modell volt, amely kölcsönös hitelesítést nyújt mind a kliens, mind a szerver számára, hogy egymás személyazonosságát megállapíthassák.

A Kerberos protokoll üzenetei védve vannak a lehallgatások és az ismétlődő támadások ellen (replay attacks). A Kerberos a szimmetrikus kulcsú titkosításonalapszik, amelyhez egy „megbízható harmadik fél” szükséges: opcionálisan, a hitelesítés egyes fázisaiban – az aszimmetrikus kulcsú titkosítást felhasználva – publikus kulcsú titkosítást is választhatunk.

(A Kerberos a Massachusetts Institute of Technology (MIT) által kiadott és alkalmazott protokoll, amely egy ingyenes szoftvercsomag is egyben. A Kerberos alapértelmezettként a 88-as portot használja.)

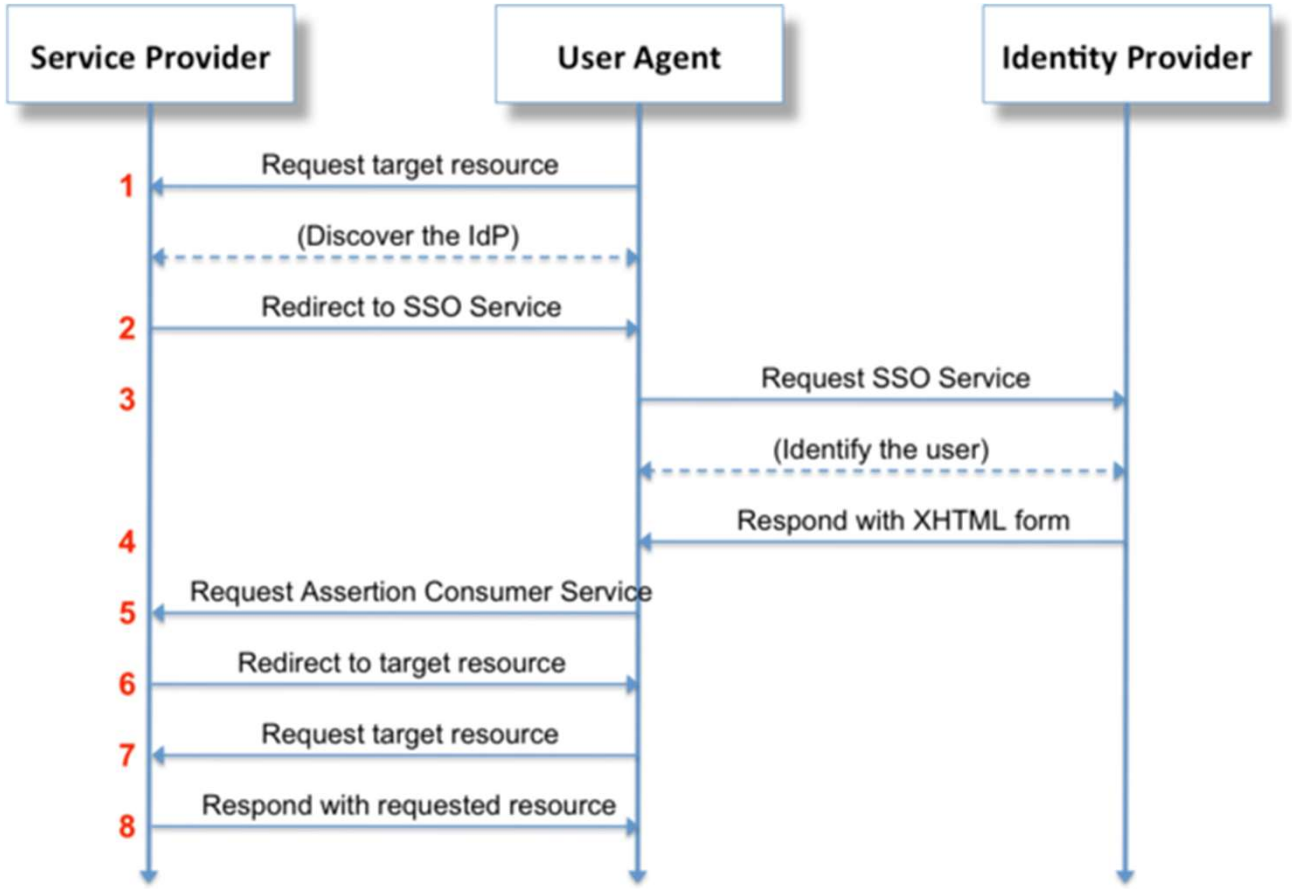
SAML

A SAML a Security Assertion Markup Language rövidítése.

Ez egy XML-alapú nyílt szabvány az identitásadatok átvitelére két fél között: egy identitásszolgáltató (IdP) és egy szolgáltató (SP) között.

Identity Provider — Hitelesítést hajt végre, és átadja a felhasználó identitását és jogosultsági szintjét a szolgáltatónak.

Single Sign On – SAML



https://commons.wikimedia.org/wiki/File:Saml2-browser-sso-redirect-post.png

OpenID

Az OpenID egy nyílt szabványú és decentralizált hitelesítési protokoll, amelyet a non-profit OpenID Foundation támogat.

Lehetővé teszi a felhasználók hitelesítését együttműködő webhelyek (úgynevezett támaszkodó felek, vagy RP) által harmadik féltől származó identitásszolgáltató (IDP) szolgáltatással, így nincs szükség arra, hogy saját, ad hoc bejelentkezési rendszert biztosítsanak.

Lehetővé teszi a felhasználók számára, hogy bejelentkezzen több, nem kapcsolódó webhelyre anélkül, hogy mindegyikhez külön azonosítóval és jelszóval kellene rendelkeznie.

A felhasználók egy OpenID identitásszolgáltató kiválasztásával hoznak létre fiókokat, majd ezekkel a fiókokkal bejelentkezhetnek bármely olyan webhelyre, amely elfogadja az OpenID hitelesítést.

Számos nagy szervezet ad ki vagy fogad el OpenID-t a webhelyén.

https://openid.net/specs/openid-authentication-2_0.html