Access control

Leereenheid 2

Access control

INTRODUCTIE

Access control (toegangscontrole) is het proces dat regelt welke gebruikers, machines of processen toegang krijgen tot welke systeembronnen, en wat de operaties zijn die de gebruikers kunnen uitvoeren op deze bronnen. Access control stelt ons in staat bronnen tegen ongewenste toegang te beschermen en is dan ook een belangrijk onderdeel van de systeembeveiliging.
Access control bestaat uit twee stappen: authenticatie en autorisatie. Authenticatie verifieert of de gebruiker die toegang vraagt daadwerkelijk is wie hij beweert te zijn. Autorisatie bepaalt vervolgens welke rechten (lezen, schrijven, uitvoeren, enzovoort) deze gebruiker heeft op de verschillende systeembronnen.
Deze leereenheid geeft een introductie in access control, en beschrijft de methoden waarmee de rechten van gebruikers op bronnen vastgelegd kunnen worden. Vervolgens beschrijft deze leereenheid het gebruik van wachtwoorden voor authenticatie: wat zijn goede wachtwoorden en welke technieken gebruiken aanvallers om wachtwoorden te achterhalen?

LEERDOELEN
Na het bestuderen van deze leereenheid wordt verwacht dat u
- de termen object en subject kunt beschrijven
- de verschillende access-controlstructuren (access control matrix, access control list, capability list) kunt beschrijven en de voor- en nadelen van iedere structuur kunt opsommen
- kunt uitleggen wat role-based access control inhoudt
- kunt uitleggen wat een wachtwoord veilig maakt
- de verschillende manieren waarop aanvallers aan wachtwoorden proberen te komen kunt beschrijven
- kunt bepalen hoelang een brute-force aanval op wachtwoorden met bepaalde eigenschappen duurt
- kunt uitleggen wat social engineering inhoudt.

Studeeraanwijzing
In deze leereenheid gebruiken we sectie 2 'Access Control Models' (pagina 19 tot en met 24) en sectie 4 'Implementation and Usability Issues' (pagina 39 tot en met 45) uit hoofdstuk 1 'Introduction' van het tekstboek. Dit is een inleidende leereenheid. Details en implementaties van beschreven technieken en methoden komen later uitvoerig aan bod in de leereenheden over Operating systems security.

De studielast van deze leereenheid bedraagt circa 3 uur.

LEERKERN

2 Access Control Models

2.1 ACCESS CONTROL MATRICES

Vanwege de nadelen van de access control matrix wordt deze structuur in de praktijk niet gebruikt.

2.2 ACCESS CONTROL LISTS

Zowel Linux, UNIX als Windows gebruiken een vorm van access control lists om toegangsinformatie bij objecten op te slaan.

2.3 CAPABILITIES

OPGAVE 2.1
Waarom wordt in besturingssystemen zoals Linux en Windows wel gebruikgemaakt van access control lists en niet van capability lists?

2.4 ROLE-BASED ACCESS CONTROL

Het tekstboek noemt als belangrijkste nadeel van role-based access control het feit dat deze methode niet geïmplementeerd is in de huidige besturingssystemen. Dit is echter geen nadeel van role-based access control zelf, maar in feite een tekortkoming van de huidige besturingssystemen. Role-based access control wordt wel steeds meer toegepast in commerciële applicaties, onder andere in databasemanagementsystemen. Het biedt namelijk de mogelijkheid om de complexiteit en kosten van het beheer van de beveiliging te verminderen.

4 Implementation and Usability Issues

4.1 EFFICIENCY AND USABILITY

Studeeraanwijzing

Het voorbeeld in de eerste alinea verwijst naar public-key en symmetrische encryptie. Dit voorbeeld kunt u hier negeren. In de leereenheden over cryptografie komt dit nader aan de orde.

An Example Scenario Involving Usability and Access Control

Het voorbeeld verwijst naar access control in Linux. Aan een object kunnen read, write en execute-rechten worden toegekend. Voor een bestand betekent read dat het bestand mag worden gelezen, write dat het bestand mag worden gewijzigd, en execute dat het bestand mag worden uitgevoerd (wat alleen zinvol is als het bestand executeerbare programmacode bevat). Voor een map (directory) betekent read dat de inhoud van de map bekeken mag worden, write dat een bestand in de map gecreëerd of verwijderd mag worden of een bestandsnaam gewijzigd mag worden, en execute dat een gebruiker naar deze map mag gaan (via een commando waarbij de naam van de map expliciet wordt vermeld). Deze rechten worden afzonderlijk aangegeven voor drie groepen subjects: voor de eigenaar (‘owner’) van het object, voor een groep van subjects (‘group’) die dezelfde group-id hebben als het object, en voor alle andere subjects (aangeduid als ‘everyone’, ‘other’ of ‘world’).

Possible Solutions

OPGAVE 2.2
Maak opgave C-20 op pagina 52 van het tekstboek.

4.2 PASSWORDS

Password checker
Weblink

U kunt met behulp van een *password checker* zelf testen of de wachtwoorden die u gebruikt 'sterk' zijn. In de elektronische leeromgeving vindt u referenties naar een aantal password checkers. Het is echter onverstandig om blind vertrouwen te stellen in zulke password checkers: in de praktijk blijken vaak ook wachtwoorden die door password checkers als sterk worden aangeduid, in een mum van tijd via een dictionary attack te achterhalen.

Wanneer we voor wachtwoorden alle mogelijke karakters (letters, cijfers, leestekens) kunnen gebruiken, dan zal de kans van slagen van een dictionary-aanval zeer klein worden. De kans dat een willekeurige string met karakters in de woordenlijst voorkomt, is natuurlijk erg klein. In zo'n geval zal een aanvaller alle mogelijke strings van karakters moeten uitproberen als wachtwoord. Dit wordt een *brute-force-aanval* genoemd.

Brute-force-aanval

OPGAVE 2.3
Stel dat wachtwoorden een lengte van exact 6 alfanumerieke karakters (hoofd- en kleine letters en cijfers) hebben. Hoelang duurt dan gemiddeld een brute-force aanval als het testen van een wachtwoord
a een tiende van een seconde duurt?
b een microseconde (miljoenste van een seconde, 10^{-6} s) duurt?
c een nanoseconde (miljardste van een seconde, 10^{-9} s) duurt?

OPGAVE 2.4
Welke van de volgende wachtwoorden zijn geschikt: FV94KZ, mffitwoo (afgeleid van 'mijn favoriete film is The Wizard of Oz'), 12345678, legovfoor, MtL+DoM15?

4.3 SOCIAL ENGINEERING

Bij social engineering probeert een aanvaller vertrouwelijke informatie te verzamelen door een legitieme gebruiker te manipuleren. Niet het systeem wordt aangevallen, maar een gebruiker, omdat gebruikers gemakkelijker voor de gek te houden zijn dan systemen. De aanvaller exploiteert de menselijke neiging om behulpzaam en nieuwsgierig te zijn en om snel te handelen in geval van een crisis.

4.4 VULNERABILITIES FROM PROGRAMMING ERRORS

Bij deze sectie is het alleen van belang te beseffen dat fouten in programmacode kunnen leiden tot onveilige situaties. De buffer overflow-aanval is een voorbeeld van een aanval die mogelijk wordt gemaakt door een programmeerfout. In de leereenheid Operating systems security II zal hieraan uitgebreid aandacht worden besteed.

ZELFTOETS

1 Wat is het verschil tussen een object en een subject in de context van access control? Geef een voorbeeld van beide.

2 Waarom is de access control matrix geen handige structuur om toegangsrechten vast te leggen?

3 Geef voor elk van onderstaande operaties aan met welke structuur deze het meest efficiënt kan worden uitgevoerd, met een access control list of met capabilities:
   a bepalen welke subjecten toegang hebben tot een gegeven object
   b bepalen tot welke objecten een gegeven subject toegangsrechten heeft
   c verwijderen van een gebruiker van een systeem
   d verwijderen van een bestand van een systeem.

4 Voor welk type aanval zijn gebruikers die als wachtwoord eenvoudige en betekenisvolle termen gebruiken, zoals namen van huisdieren of geboortedata, extra gevoelig?

5 Gegeven is dat alleen de 26 karakters van het alfabet mogen worden gebruikt om een wachtwoord te vormen. Hoeveel verschillende wachtwoorden zijn dan mogelijk
   a als een wachtwoord exact 4 karakters lang en niet hoofdlettergevoelig is (er wordt dus geen onderscheid gemaakt tussen hoofdletters en kleine letters)?
   b als een wachtwoord maximaal 4 karakters lang en wel hoofdlettergevoelig is?

TERUGKOPPELING

1 Uitwerking van de opgaven

2.1 In de praktijk is het gebruik van access control lists het efficiëntst. Linux en Windows zijn weliswaar multi-user-besturingssystemen, maar het aantal subjects per systeem is vele malen kleiner dan het aantal objects: het gaat meestal slechts om enkele gebruikers, versus tien- tot honderdduizenden mappen en bestanden. Een capability list per gebruiker is daarom enkele ordes groter dan een access control list per object. Bij de meest voorkomende operaties, zoals lezen, schrijven, creëren of verwijderen van een bestand of map, is het dan ook vele malen efficiënter om de access control list bij het object te raadplegen dan een capability list. De operaties waarbij een capability list handiger is, zijn beperkt tot het creëren of verwijderen van een gebruiker, wat echter relatief weinig voorkomt.

2.2 Maak een directory, bijvoorbeeld met een willekeurige naam 'foo', in de home directory van een van de groepsleden, zonder read-rechten voor iedereen, maar wel met execute-rechten voor iedereen. Maak vervolgens in de directory foo een subdirectory met een willekeurig gekozen naam die alleen bekend wordt gemaakt aan de groepsleden. Geef deze subdirectory read, write en execute-rechten voor iedereen.
Omdat de directory foo geen leesrechten heeft, kan niemand de inhoud (en dus de naam van de subdirectory) bekijken. Maar omdat de groepsleden de naam van de subdirectory wel kennen, kunnen zij zich verplaatsen naar deze subdirectory en daar hun werk doen.
Ook deze oplossing is echter een vorm van security by obscurity, omdat iedereen die de naam van de subdirectory kent erbij kan. Als die naam bekend wordt bij niet-teamleden, is de security doorbroken.
Een oplossing die daadwerkelijk veilig is, is teamleden in een aparte groep onderbrengen en hun in de group-permissies bij deze directory read-, write- en execute-rechten verlenen. In de world-permissies bij deze directory worden dan geen read-, write- en execute-rechten aan alle andere gebruikers verleend. Dit vereist echter meestal de tussenkomst van een systeembeheerder om de groep aan te maken en gebruikers aan die groep toe te wijzen.

2.3 Er zijn 62 verschillende alfanumerieke karakters: 26 hoofdletters + 26 kleine letters + 10 cijfers. Dus er zijn 62^6 verschillende wachtwoorden van 6 alfanumerieke karakters. Gemiddeld moet de helft van het aantal mogelijke wachtwoorden getest worden voordat het juiste wachtwoord is gevonden, dus $62^6/2 = 28.400.117.792$. Het zoeken duurt daarom ongeveer
a 90 jaar
b 8 uur
c 28 seconden.

2.4 Als FV94KZ het nummer van een nummerbord is, dan is het niet geschikt. Ongeschikt zijn ook: 12345678 (zeer ongeschikt zelfs) en legovfoor (hier staat roofvogel achterstevoren). Geschikter is mffitwoo, maar deze valt bij de meeste checkers door de mand. Het is veel beter om tevens hoofdletters en andere tekens te gebruiken, zoals in MtL+DoM15.

2 Uitwerking van de zelftoets

1 Een subject is een actieve entiteit die toegang kan krijgen tot objecten. Voorbeelden zijn gebruikers en processen. Een object is een passieve entiteit waar toegang tot verkregen kan worden. Voorbeelden zijn bestanden, programma's en delen van de geheugenruimte.

2 De access control matrix schaalt niet goed. Als er veel subjecten en objecten zijn, wordt de matrix erg groot zonder dat deze veel informatie bevat. Veel cellen in de matrix zullen leeg zijn, omdat een subject over het algemeen slechts rechten heeft op een beperkt aantal objecten in het systeem. De access control matrix vraagt dan veel geheugen en voor een systeembeheerder is het onmogelijk om alle cellen van de matrix te beheren.

3 a access control list
b capabilities
c capabilities
d access control list
De access control list is handig voor operaties die uitgaan van een object (bepalen welke subjecten rechten hebben op het object, en het verwijderen van een object van het systeem). De capability list is handig voor operaties die uitgaan van een subject (bepalen van objecten en hun rechten bij een subject, en het verwijderen van een subject).

4 Een dictionary-aanval. Het is goed mogelijk een dictionary met bestaande bekende namen te maken en al deze namen uit te proberen als wachtwoord. Er zijn zelfs complete dictionaries (met veelgebruikte namen) op internet voor hackers beschikbaar. Omdat veel gebruikers eenvoudige namen gebruiken, maken hackers eerst gebruik van deze dictionaries, voordat ze een brute-force-aanval uitvoeren omdat die veel langer duurt.

5 a Dat is gelijk aan: $26 \times 26 \times 26 \times 26 = 26^4 = 456.976$ (voor elk karakter zijn er 26 keuzemogelijkheden).
b Het totaal aantal wachtwoorden dat maximaal 4 karakters heeft, is gelijk aan de som van het aantal wachtwoorden bestaande uit 1, uit 2, uit 3, en uit 4 karakters. Het aantal verschillende wachtwoorden is daarom gelijk aan $52^1 + 52^2 + 52^3 + 52^4$, en dat is meer dan 7,4 miljoen.