hyväksymispäivä arvosana

arvostelija

Tunkeutumisen havaitseminen

Antti Rantasaari

Helsinki 3. maaliskuuta 2003

Seminaari

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Sisältö

1 Johdanto

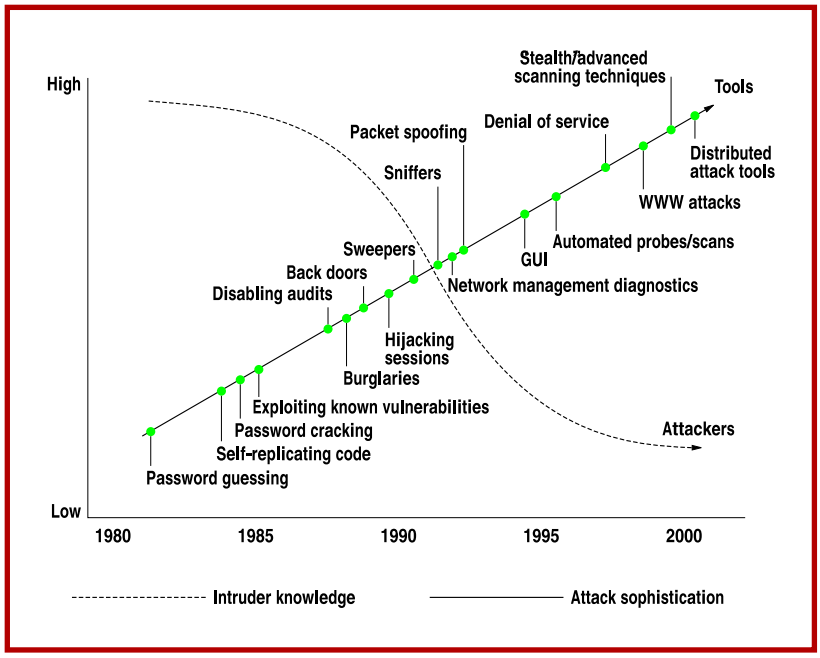
Tietotekniikan, niin laitteiden, ohjelmistojen kuin verkkojenkin, nopea kehitys tarjoaa lukemattomia uusia mahdollisuuksia uuden tekniikan hyödyntämiseen ja väärinkäyttöön. Tietojärjestelmien tulisi tarjota käyttäjille luottamuksellista, eheää ja varmaa palvelua. Tämän saavuttamiseksi järjestelmistä on pyritty kehittämään mahdollisimman turvallisia. Tyypillisiä turvatoimia ovat mm. salasanat, palomuuri ja VPN (Virtual Private Network). Vaikka näillä toimilla palvelun luvatonta käyttöä pystytään vaikeuttamaan, täysin turvallisen järjestelmän kehittäminen on käytännössä mahdotonta. Lisäksi edellämainitut turvatoimet eivät suojaa tietojärjestelmiä järjestelmän sisältä tulevia hyökkäyksiä, joiden on todettu olevan paljon ulkoisia hyökkäyksiä yleisempiä ja vaarallisempia, vastaan.

2 Tunkeutumisen havaitseminen

Turvajärjestelmät, jotka torjuvat luvatonta pääsyä järjestelmään, ovat tärkeitä, mutta tarvitaan myös keinoja havaita tunkeutumisyrityksiä ja korjata mahdollisen hyökkäyksen aiheuttamia vahinkoja. Anderson [A80] ehdotti vuonna 1980 kirjausketjujen käyttöä uhkien tarkkailemiseen ja hyökkäysten paljastamiseen. Ennen Andersonin artikkelia tälläisen datan tärkeyttä ei ymmärretty ja kaikki tietoturvan parantamiseen liittyvät menetelmät keskittyivät pääsyn estämiseen arkaluonteiseen dataan. Andersonin artikkelin katsotaan olleen synty *tunkeutumisen havaitseminen*-käsitteelle ja artikkelin jälkeen on tutkittu ja kehitetty useita tekniikoita sen toteuttamiseen.

2.1 Tarve tunkeutumisen havaitsemiseen

Viime vuosikymmenen aikana tietomurrot ovat kasvaneet nopeaa vauhtia. Täysin luotettavaa tietoa tietomurtojen määrästä ei ole saatavilla, mutta Computer Security Instituten ja FBI:n vuonna 2002 tekemän tutkimuksen mukaan noin 90% yrityksistä oli murron kohteena - vastaava luku vuonna 1996 oli 42% [P02]. Monien asiantuntijoiden mielestä todellisuudessa tapahtuu murtoja kuitenkin vielä enemmän, koska yritykset haluavat vaieta niitä vastaan kohdistuneista tietomurroista. Samalla kun tietomurrot ovat yleistyneet, on hyökkäysyritysten tekemistä helpotettu. 80-luvulla ammattitaitoiset murtautujat käyttivät yksinkertaisia ja yksilöllisiä keinoja murtautumiseen, nykyään lähes kuka tahansa voi yrittää tunkeutua luvatta tietojärjestelmään käyttämällä avukseen kehittyneitä, valmiiksi tehtyjä työkaluja [AMC00]. Kuvassa 1 näkyy kehitys tunkeutujien ammattitaidon ja hyökkäysten hienouden muutoksesta.



Kuva 1: Tunkeutujien ammattitaidon ja hyökkäyksien hienouden muutos [AMC00]

Tunkeutumisyritysten käsittelyyn on olemassa kaksi lähestymistapaa [S96]. Yksi tapa on rakentaa järjestelmä, johon tunkeutuminen on estetty. Voidaan ottaa käyttöön esimerkiksi hyvin tiukka pääsynvalvonta, salata luottamuksellinen tieto ja vaatia käyttäjiä yksilöimään ja varmantamaan itsensä. Lähtökohta ei kuitenkaan yksistään riitä eikä ole toteuttamiskelpoinen, koska

- ei ole käytännössä mahdollista kehittää täysin turvallista järjestelmää mm. ohjelmistoissa ja käyttöjärjestelmissä olevien ohjelmavirheiden takia.
- erilaisten tietojärjestelmien valtava määrä hidastaa siirtymistä turvallisempiin järjestelmiin.
- salaamisessa on omat ongelmansa. Salasanoja voidaan murtaa ja kadottaa sekä kokonaisia salausjärjestelmiä voidaan rikkoa.
- kaikki erittäin hyvinkin suojatut järjestelmät ovat haavoittuvaisia järjestelmän sisältä tulevia hyökkäyksiä vastaan.

Tämän takia perinteisen suojautumisen tueksi tarvitaan muita järjestelmiä. Jos on oletettavaa, että tietomurtoja tapahtuu, on tarpeellista saada niistä mahdollisimman nopeasti tieto, jotta murto pystyttäisiin keskeyttämään tai ainakin murron aiheuttamat vahingot voitaisiin selvittää ja korjata nopeasti. Tunkeutumisen havaitsemisjärjestelmät (Intrusion Detection System, IDS) on kehitetty tätä varten.

2.2 Tunkeutumisen havaitsemisjärjestelmät

IDS-järjestelmät toimivat tutkimalla järjestelmän kirjausketjuja. Koska lähes kaikki järjestelmässä tehtävät toiminnot tallettuvat lokitiedostoihin, voidaan niitä lukemalla selvittää järjestelmään tehdyt tunkeutumisyritykset. Datan valtavan määrän, mahdollisesti satojen megatavujen, takia manuaalinen tutkiminen ei ole järkevää, mutta ennalta määriteltyjen ohjeiden perusteella IDS-järjestelmät voidaan

automatisoida analysoimaan dataa ja tunkeutumisyrityksen havaitessa toimimaan halutulla tavalla. Reaaliaikainen lokien seuraaminen on tärkeää, koska ammattitaitoinen tunkeutuja pyrkii peittämään tunkeutumisesta aiheutuneet jäljet, jolloin tunkeutujan havaitseminen on mahdollista vain tunkeutumisen aikana.

Tunkeutujan havaitseminen perustuu oletukseen, että tunkeutujan käytös poikkeaa järjestelmän normaalista käytöstä. Ero normaalin käyttäjän, ylläpitäjän ja tunkeutujan käytöksessä ei välttämättä ole kovinkaan suuri. Mitä tiukemmin kirjausketjuja tulkitaan, sitä suurempi mahdollisuus IDS-järjestelmällä on huomata tunkeutuminen, mutta toisaalta tiukka tulkinta johtaa suureen määrään vääriä hälytyksiä, jolloin IDS-järjestelmä tulkitsee luvallisen käyttäjän toimet tunkeutumisena.

2.3 IDS-järjestelmän toteutustavat

IDS-järjestelmät voidaan toteuttaa joko verkkoasemakohtaisesti tai verkkokohtaisesti [SD02]. Luvussa 3 käydään selvitetään tarkemmin, miten IDS-järjestelmät havaitsevat tunkeutumisen.

Verkkoasemakohtaisessa ratkaisussa IDS-järjestelmä asennetaan koneille, joiden toimintaa halutaan tarkastella. Koneen lokitiedostoja ja järjestelmän tarkistusagentteja hyväksikäyttäen IDS tarkkailee koneen verkkoliikennettä ja toimintaa epäilyttävien prosessien havaitsemiseksi. Verkkoasemakohtainen ratkaisu on erityisen tehokas sisältä tulevien hyökkäyksien havaitsemiseksi, mutta huonona puolena IDS-järjestelmä täytyy asentaa jokaiseen koneeseen, jonka halutaan kuuluvan tarkkailun piiriin. Lisäksi IDS-järjestelmä käyttää koneella samoja resursseja kuin muutkin ohjelmat, joten kuormitetulla koneella IDS voi aiheuttaa suorituskyvyn voimakasta laskua.

Verkkokohtainen IDS-järjestelmä (Network Intrusion Detection System, NIDS)

on asemakohtaista ratkaisua uudempi. Sen ideana on, että verkossa on haluttu määrä koneita, joiden tehtävänä on tarkkailla verkkoliikennettä. NIDS-järjestelmän toteutus vaatii, että verkkomonitorina toimiva kone pystyy nappaamaan kaiken verkossa liikkuvan datan ja tutkimaan sen sisällön etsien datan seasta mahdollisia tunkeutumisyrityksiä. NIDS-järjestä on suosittu, koska se on verkkoasemakohtaiseen ratkaisuun verrattuna helppo ottaa käyttöön sekä ylläpitää eikä valvottavien koneiden teho kulu IDS-järjestelmän ajamiseen. Verkkokohtaisen ratkaisun suurin ongelma on, että verkkojen nopeutuessa valvontakoneelle käsiteltäväksi tulevan datan määrä kasvaa huomattavasti. Valvontakoneen resurssit ei välttämättä riitä verkkoliikenteen tehokkaaseen valvontaan ja verkkoa joudutaan osittamaan pienempiin segmentteihin, joilla jokaisella on oma valvontakone.

3 IDS-järjestelmien toiminta

IDS-järjestelmän täytyy kyetä havaitsemaan tunkeutumisyritykset tietojärjestelmän normaalin käytön seasta. Kaksi käytetyintä tunkeutujan havaitsemistapaa ovat sääntöpohjainen 3.1 ja tilastollinen 3.2 havaitseminen. Molemmilla niistä on vahvat ja heikot puolensa.

3.1 Sääntöpohjainen havaitseminen (misuse detection)

Sääntöpohjaisessa havaitsemisessa oletetaan, että hyökkäykset täyttävät tunkeutumiselle tyypilliset tunnusmerkit. Järjestelmään määritellään ennalta tiettyjä sääntöjä, joilla yritetään tunnistaa, onko kyseessä tunkeutujan käytös. Järjestelmä voi myös yhdistellä sääntöjä ja muunnella niitä hieman, jolloin pystytään havaitsemaan myös variaatioita tunnetuista tunkeutumismenetelmistä.

Sääntöpohjainen järjestelmä on tehokas tunnettujen hyökkäysten havaitsemises-

sa, eikä se aiheuta paljoa vääriä hälytyksiä, koska ilmoitus tunkeutumisesta tehdään vain sääntöihin määriteltyjen toimintojen tapahtuessa. Suurena ongelmana on kuitenkin se, että säännöt täytyy määritellä itse, eikä järjestelmä kykene siten havaitsemaan kokonaan uudenlaisia hyökkäyksiä, koska tunkeutuminen ei täytä mitään järjestelmään määritellyistä tunnusmerkeistä.

3.2 Tilastollinen havaitseminen (anomaly detection)

Tilastollisessa havaitsemisessa lähtökohtaisena oletuksena on, että tunkeutumisyritys poikkeaa järjestelmän normaalista käytöstä. IDS-järjestelmä tulkitsee normaalin käytön meluksi, ja yrittää havaita verkkoliikenteestä datan, joka ei ole pelkästään melua. Tunkeutumisen erottaminen melusta ei ole yksinkertaista. IDS-järjestelmän pohjaksi täytyy rakentaa tilasto tietojärjestelmien normaalista käytöstä, ja tilastoa tulee päivittää jatkuvasti käyttötapojen muuttuessa. Kaikki, mikä ei ole normaalia tilastossa määriteltyä käytöstä tulkitaan tunkeutumiseksi.

Tilastollisen havaitsemisen suurin etu sääntöpohjaiseen järjestelmään verrattuna on sen kyky havaita kaikki hyökkäykset, ei vain niitä, jotka on osattu järjestelmään määritellä. Toisaalta kaikkea järjestelmien normaalia, sallittua käyttöä ei ole mitenkään voitu tilastoida IDS-järjestelmään. Toimintatavastaan johtuen tilastollisella järjestelmällä on kaksi suurta heikkoutta - normaali, poikkeava käyttö tulkitaan tunkeutumiseksi, mikä aiheuttaa suuren määrän vääriä hälytyksiä sekä tunkeutuminen, joka ei poikkea normaalista käytöstä, jää huomaamatta. Erityisesti jälkimmäinen näistä on vaarallista.

3.3 IDS-järjestelmien kehitys

Uusia, tehokkaampia IDS-järjestelmiä on kehitetty yhdistämällä sääntöpohjaisen ja tilastollisen havaitsemisen vahvoja puolia yrittäen samalla eliminoida heik-

kouksia. Nykyisten järjestelmien ongelmana on se, että ne ovat kykeneviä havaitsemaan ammattitaidottomien tunkeutujien yritykset, mutta ammattitaitoiset tunkeutumiset jäävät huomaamatta [AMC00]. Usein juuri nämä aiheuttavat suurimman uhkan yrityksille.

IDS-järjestelmät pystyvät havaitsemaan tunkeutumisia, mutta toisaalta tuottavat myös paljon vääriä hälytyksiä, mikä saattaa lannistaa tietoturvasta vastuussa olevia työntekijöitä. Jos vääriä hälytyksiä on liikaa, ei niihin kiinnitetä enää tarpeeksi huomiota ja todelliset hyökkäykset saattavat hukkua väärien hälytysten sekaan.

4 Yhteenveto

IDS-järjestelmät ovat tarkoitettuja tunkeutumisen havaitsemiseen eivätkä ne itsessään tarjoa minkäänlaista suojaa tunkeutumisia vastaan. Ne antavat ainoastaan ilmoituksen mahdollisesta tunkeutumisesta sellaisen havaitessaan. IDS-järjestelmien käyttöönotto yrityksissä on täysin turhaa, mikäli niiden toimintaa ei ymmärretä eikä niiden käyttöön osata resursoida tarpeeksi voimavaroja. Annetusta tunkeutumishälytyksestä ei ole mitään hyötyä, ellei joku osaa ja ehdi toimia hälytyksen tullessa sopivalla tavalla.

Lähteet

AMC00 Allen, J., McHugh, J., Christie, A., Defending Yourself: The Role of Intrusion Detection Systems. *IEEE Software* September/October (2000)

AFV95 Anderson, D., Frivold, T., Valdes, A., Next-genetarion Intrusion Detection Expert System (NIDES) *Technical report, SRI International, Computer Science Lab* (1995)

A80 Anderson, J. P., Computer Security Threat Monitoring and Surveillance. Technical Report, James P Anderson Co., Fort Washington, Pennsylvania, (1980)

KS94 Kumar, S., Spafford, E., A Pattern matching Model for Misuse Intrusion Detection. *Proceedings of the Seventeenth National Computer Security Conference* Baltimore, MD (1994)

MHL94 Mukherjee, B., Heberlein, L., Levitt, K., Network intrusion detection. *IEEE Network* May/June (1994)

NSS The NSS Group, http://www.nss.co.uk/ *IDS Group Test (Edition 1)* (2002)

P02 Power, R., 2002 CSI/FBI Computer Crime and Security survey. *Computer Security Issues and Trends* (2002)

Setal02 Sekar, R., Gupta, A., Frullo J., Shanbhag, T., Tiwari, A., Yang, H., Zhou, S., Specification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. *Proceedings of the 9th ACM conference on Computer and communication security* 265-274 (2002)

SD02 Sherif, J., Dearmond, T., Intrusion Detection: Systems and Models. *Proceedings of the eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises* June (2002)

S96 Sundaram, A., An Introduction to Intrusion Detection. *Crossroads: The ACM Student Magazine*, 2, 2 (1996)