Elosztott behatolásérzékelő rendszerek lehetőségei, gyakorlati alkalmazás

Gyimesi Judit

Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai kar

A behatolásérzékelő rendszerek (Intrusion Detection Systems – IDS) olyan szoftveres, vagy hardveres rendszerek, melyek automatizálják a hálózatban vagy rendszerben levő események monitorozását, gyanús, támadásra utaló jeleket keresve. Feladatuk a már elkezdett behatolás, támadás felismerése. Adatfeldolgozási módszerük alapján egyik csoportjuk az anomália-detektáló IDS-ek, melyek abból indulnak ki, hogy támadás esetén a szokásostól eltérő viselkedés, hálózati forgalom tapasztalható. Minden felhasználóhoz készítenek egy felhasználói profilt, amit bizonyos időközönként frissítenek, és ha attól egy küszöbértéknél nagyobb eltérésű viselkedést tapasztalnak, akkor feltételezik a támadást. Nagy előnyük, hogy új, még ismeretlen támadásokkal is hatásosan veszi fel a harcot. Kijátszhatóságuk miatt azonban érdemes más biztonsági eszközökkel együtt használni.

Több IDS elosztott alkalmazásával számos probléma megoldási ötletét is felvázolom, részletesebben elemezve a hálózati férgek terjedésének felismerését és korlátozását. Erre bemutatok egy általam kidolgozott algoritmust, melynek hatékonyságát matematikai analízissel szemléltetem. Eszerint az IDS-ekkel védett alhálózatunkban a fertőzés második hulláma kivédhető, ám már a terjedés első, veszélyes szakasza is sokszor megfékezhető.