VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
INFORMATIKOS KATEDRA

Magistro tezių tema ir laukiami rezultatai

Netradiciniai UNIX sistemų saugumo modeliai

Atliko: 1 kurso 1-osios gr. magistrantas
Marius Gedminas

Darbo vadovas:
Albertas Agejevas

Vilnius
2002

Darbe trumpai apžvelgiami tradicinio UNIX saugumo modelio trūkumai ir nagrinėjami keli skirtingi šio modelio plėtiniai, siekiantys tuos trūkumus pašalinti ar palengvinti. Nagrinėjami šie saugumo mechanizmai:

- priėjimo kontrolės sąrašai (Access Control Lists, ACL)
- galimybės (Capabilities)
- privaloma priėjimo kontrolė (Mandatory Access Control, MAC)

Darbo tikslai yra nustatyti šių mechanizmų tinkamumą bei pritaikomumą skirtingose situacijose (namų kompiuteris, tarnybinė tinklo stotis, daugelio vartotojų sistema) ir pasiūlyti saugumo taisyklių rinkinius kiekvienai iš jų, derinančius saugumą, funkcionalumą bei patogumą.

Darbą galima suskirstyti į šias pagrindines dalis:

- uždavinio formulavimas
- priėjimo kontrolės sąrašų taikymas
- galimybių taikymas
- privalomos priėjimo kontrolės taikymas
- bendro modelio kūrimas

Kiekvieną dalį apžvelgsime smulkiau.

Uždavinio formulavimas

Skirtingose situacijose reikalingi skirtingi saugumo lygiai. Priimtinos rizikos lygis įprastiniam namų kompiuteriui ir žinomos kompanijos viešai tinklo tarnbinei stočiai skiriasi. Taip pat skiriasi sistemos naudojimo scenarijai, vartotojų rolės bei priimtinas saugumo priemonių (ne)patogumo laipsnis.

Šios darbo dalies tikslas – apibrėžti skirtingas sistemos naudojimo situacijas, įvertinti pavojaus modelius bei riziką kiekvienoje iš jų ir pagal tai nustatyti norimą saugumo sistemos funkcionalumą.

Priėjimo kontrolės sąrašų taikymas

Priėjimo kontrolės sąrašai (access control lists) išplečia UNIX failų sistemos vartotojų bei grupių modelį. Jie leidžia griežčiau aprašyti priėjimo lygmenis, padidindami saugumo modelio lankstumą, bet kartu ir sudėtingumą.

Šios darbo dalies tikslas būtų išanalizuoti, kokias problemas išsprendžia priėjimo kontrolės sąrašų taikymas, kokios naujos problemos iškyla dėl jų vartojimo, ir kada šio mechanizmo vartojimo nauda nusveria kainą.

Galimybių taikymas

Galimybės (capabilities) leidžia sumažinti riziką sumažindamos visagalio UNIX `root` vartotojo reikšmę sistemai. Tradiciškai `root` vartotojas gali atlikti daugelį veiksmų, neleidžiamų kitiems vartotojams. Iš kitos pusės, jei tam tikrai sistemos daliai prireikia atlikti bent vieną iš tų veiksmų, jai turi būti suteiktos visos `root` vartotojo privilegijos, pažeidžiant minimalių privilegijų principą. Galimybės leidžia šias privilegijas suteikti nepriklausomai viena nuo kitos.

Šios darbo dalies tikslas būtų išanalizuoti, kokias problemas išsprendžia galimybių taikymas, kaip galima būtų jį realizuoti, ir kada tai apsimoka.

Privalomos priėjimo kontrolės taikymas

Tradiciškai UNIX realizuojama savarankiška priėjimo kontrolė (discretionary access control), t.y., vartotojai patys gali/turi nurodyti priėjimo lygį savo duomenims. Privaloma priėjimo kontrolė (mandatory access control), dažnai vartojama valdiškose sistemose, dirbančiose su slapta informacija, neleidžia vartotojams savavališkai ar per neapsižiūrėjimą perduoti savo privilegijų kitiems.

Šios darbo dalies tikslas būtų išanalizuoti, kokias problemas sprendžia privaloma priėjimo kontrolė.

Bendro modelio kūrimas

Šios darbo dalies tikslas yra sukurti išplėstinį UNIX saugumo modelį remiantis tradiciniu UNIX saugumo modeliu, priėjimo kontrolės sąrašais, galimybėmis bei privaloma priėjimo kontrole. Modelis turi būti kiek galima paprastesnis, bet jis turi būti pakankamai saugus ir turi spręsti uždavinio formuluotėje apibrėžtas problemas.

Darbo planas

- literatūros apžvalga
- uždavinio formulavimas
- priėjimo kontrolės sąrašų taikymo analizė
- galimybių taikymo analizė
- privalomos priėjimo kontrolės taikymo analizė
- bendro modelio kūrimas
- sukurto modelio pritaikomumo analizė apibrėžtose situacijose
- išvadų formulavimas

Darbo rezultatai

- uždavinio formuluotė
- bendras saugumo modelis
- modelio taikymai skirtingoms situacijoms