Sisältö

1 Johdanto

Ohjelmistojen haavoittuvuukset ovat verrattaen ikäviä. Tietoturva-aukoista aiheutuneesta ylimääräisestä työstä tietojärjestelmien ylläpitäjille sekä menetetystä työajasta voi seurata suuria rahallisia tappioita, puhumattakaan mahdollisista henkilötietojen tai yrityssalaisuuksien vuotamisesta. Esimerkiksi Microsoftin IIS-palvelimen haavoittuvuuden avulla levinneestä Code Red-madosta aiheutui yhteensä noin 2,6 miljardin tappiot [MSc02]. Selvästi on toivottavaa, että ohjelmiston tietoturvasta voidaan varmistua ennen ohjelmiston käyttöönottoa.

Tietoturvaongelmia voi yrittää löytää manuaalisesti tutkimalla ohjelman lähdekoodia, mikä tietenkin on mahdollista vain ohjelmiston varsinaisille kehittäjille tai avoimen lähdekoodin ohjelmille. Lähdekoodin puuttuessa täytyy ensin ohjelmatiedosto takaisinkääntää disassembler-ohjelmalla symboliselle konekielelle ja tutkia ohjelmaa konekielitasolla. Kummassakin tapauksessa manuaalinen tutkiminen on työlästä ja aikaavievää, joten automatisoitu ratkaisu on paikallaan.

2 Yleisiä tietoturvaongelmia

3 Testausmenetelmät

3.1 Luokittelu

3.2 Testauksen kriteereitä

Ohjelmistotekniikan menetelmistä tuttu laadunvarmistustekniikka on automaattiset testit [Som06]. Testausta voidaankin soveltaa tietoturvaongelmien välttämiseen tietyin edellytyksin: sen sijaan, että testataan toivotun toiminnallisuuden olemassaoloa, testataankin *epätoivotun käytöksen* puutet-