Neprimjetan nadzor aktivnosti u operacijskom sustavu

Undetectable Operating System Activity Monitor

Mentor: Prof. dr. sc. Branko Jeren

Zadatak

Za uspješnu zaštitu računalnog sustava od napada, potrebno je pratiti sve aktivnosti korisnika i aplikacija koje oni pokreću. Zadatak je analizirati poznate metode nadzora aktivnosti u operacijskom sustavu, prepoznati njihove nedostatke te definirati zahtjeve na sustav nadzora kojeg korisnici operacijskog sustava ne mogu ni otkriti, ni omesti. Na osnovi definiranih zahtjeva, konstruirati i izvesti neprimjetni sustav nadzora aktivnosti u operacijskom sustavu.

Tekst rada: Neprimjetan nadzor aktivnosti u operacijskom sustavu.

Kronologija

1. tjedan (5.-11.3.2012.)

Izvještaj

Počeo istraživati o introspekciji virtualnih strojeva (engl. Virtual Machine Introspection, VMI) kao potencijalnom pristupu rješenja problema neprimjetnog nadzora korisnika. Ova metoda omogućava iskorištavanje virtualizacijske tehnologije za kompletan nadzor rada korisnika na sustavu. Virtualizacijski alati imaju, kao centralnu komponentu, sloj nazvan Virtual Machine Monitor (ili HyperVisor), koji služi kako bi se hardware apstrahirao i na konzistentan način prikazao operacijskim sustavima unutar virtualnih strojeva.

Daljni plan

- Odrediti vrste virtualizacijskih tehnologija
- Odrediti ključna svojstva za implementaciju sustava sigurnog i nezamjetnog nadzora korisnika

2. tjedan (12.-18.3.2012.)

Izvještaj

Postoje dvije jasno definirane vrste virtualizacijskih alata: Tip I te Tip II. Tip I predstavlja tradicionalne virtualizacijske alate (poput VMWare ESXa) koji se nalaze direktno iznad hardwarea računala, te zapravo glume mali operacijski sustav, koji nudi identično sučelje kao i hardware (prema gornjem

sloju gdje se nalaze virtualizirani OSovi), a programski rješava probleme upravljanja memorijom i izvršavanja procesa (s obzirom da je moguće virtualizirati više OSova). Tip II je host-based virtualizacijska tehnologija (poput User-Mode Linuxa, VMWare Workstationa) koja se nalazi unutar nekog operacijskog sustava, a pruža mogućnost virtualizacije operacijskih sustava. Osim toga, postoje i hibridni virtualizacijski alati (mješavina gorenavedenih tipova). Ključna svojstva za izgradnju sustava sigurnog i nezamjetnog nadzora korisnika su izolacija, introspekcija i interpozicija. Izolacija je sama po sebi dostupna korištenjem virtualizacijskih tehnologija. Introspekcija se odnosi na iskorištavanje VMM sloja kako bi se omogućio uvid u virtualni stroj. Interpozicija je svojstvo koje omogućuje kontrolu umetanjem naredbi u stroj koji nadziremo. Osim toga, čini mi se da bi poželjno svojstvo bilo da se virtualizacijski alat (točnije VMM) ne modificira (time možemo unijeti nepotrebne greške), nego je potrebno odabrati virtualizacijsku tehnologiju koja omogućava maksimalan uvid u stanje nadziranog operacijskog sustava.

Izvještaj sa sastanka (14.3.2012)

Sve informacije iz gornjeg paragrafa su prenesene nadležnom mentoru. Odlučeno je da se otkriju metode iskorištavanja VMMa za ostvarivanje nezamjetnog nadzora, te definiranje svojstava kakve bi takav sustav trebao zadovoljavati, kako bi se moglo početi raditi na preglednom radu.

Daljnji plan

- Definiranje svojstava i ograničenja za uspostavu sigurnog i nezamjetnog nadzora
- Pregled već dostupnih tehnologija
- Definiranje poboljšanja u odnosu na postojeće tehnologije

3. tjedan (19.-25.3.2012.)