ЕВРО БАЛКАН

ЗБОРНИК НА ТРУДОВИ

Прва меѓународна научна конференција
„Влијанието на научно – технолошкиот развиток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија“

Скопје 20-21 декември 2013

ЗБОРНИК НА ТРУДОВИ: Прва меѓународна научна конференција
„Влијанието на научно – технолошкиот развиток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија“

Организатор: Институт за дигитална форензика
Универзитет „Евро-Балкан“ - Скопје

Уредник: Проф.д-р Сашо Гелев

Издавач: Универзитет „ЕВРО-БАЛКАН“ Скопје
Република Македонија
www.euba.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

001.3:330/378(497.7)(063)

МЕЃУНАРОДНА научна конференција (1 ; 2013 ; Скопје)
Влијанието на научно-технолошкиот развиток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија : зборник на трудови / Прва меѓународна научна конференција, Скопје 20-21 декември, 2013 ; [уредник Сашо Гелев]. - Скопје : Универзитет "Евро-Балкан", 2014. - 706 стр. : граф. прикази ; 24 см

Дел од текстот на англиски јазик. - Библиографија кон трудовите

ISBN 978-608-4714-05-7

а) Научен развиток - Општествени науки - Македонија - Излагања на конференции
COBISS.MK-ID 95578634

Програмски одбор

- Проф. д-р Павлина Витанова, ЕВРО-БАЛКАН, копретседател;
- Проф.д-р Сашо Гелев– Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија копретседател
- Проф. Влатко Чингоски, Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија
- Проф. д-р Лада Садиковиќ, Факултет за криминалистика, криминологија и безбедност, Универзитет во Сараево;
- Проф. д-р Здравко Скакавац, Факултет за правне и пословне студије, Универзитет УССЕ, Нови Сад;
- Проф. Д-р Божо Крстајиќ, Електротехнички факултет - Подгорица, Црна Гора
- Доц. д-р Марјан Николовски, Факултет за безбедност, Универзитет Св. Климент Охридски, Битола, Република Македонија
- Доц. д-р Ненад Танески, Војна академија, Скопје, Република Македонија
- Проф. д-р Гордан Калајџиев, Правен факултет, Универзитет Св. Кирил и Методиј – Скопје, Република Македонија
- Доц. д-р Митко Богданоски, Војна академија Скопје, Република Македонија
- Доц. д-р Роман Голубовски, Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија
- Проф. Д-р Драган Михајлов, УКИМ; Република Македонија
- Д-р Никола Протрка, Полициска академија, Загреб, Република Хрватска
- Проф. Д-р Тони Стојановски, Австралија
- Д-р Зоран Нарашанов, Винер осигурување, Скопје, Република Македонија
- Проф. Д-р Стефан Сименов, Академија за внатрешни работи на Република Бугарија

Организацискиодбор

- Проф. д-р Сашо Гелев, претседател;
- Проф. д-р Павлина Стојанова, член;
- Проф. д-р Александар Даштевски, член;
- Доц. д-р Вангел Ноневски, член
- Доц. д-р Јорданка Галева
- М-р Славко Гавриловски, секретар;
- Валентина Гоцевска, член;
- Игор Панев, член;
- Ивана Крајчиновиќ, член
- Драгана Каровска, член

Aleksandar Sokolovski
NEOCOM
Saso Gelev
ETF Radoviš - UGD
Vlatko Cingoski
ETF Radoviš - UGD

Signature driven e-mail spam detection using network intrusion detection methodology

Abstract:*The scope of this research paper is one of the most important aspects nowadays, the security and management of one of the most important services the e-mail and all of the alike online services today. This paper attempts to investigate the possible benefits of using standard signature-driven spam detection logic in combination with algorithm for network intrusion detection system (NIDS).*
The primary objective is to verify that proposed solution (standard signature-driven spam detection logic and NIDSalgorithm) will be an effective strategy for dealing with e-mail spam detection.
The main aim is to determine best possible integration of standard signature-driven spam detection logic in combination with algorithm for network intrusion detection system, for creating more effective solution for dealing with e-mail spam compared to the previous solutions available.
This will be achieved by testing the effectiveness of the solution compared to other solutions until today, by using network simulators NS-3.
Keyword: *e-mail, spam, network intrusion detection system, network security, agent based security.*

1. Вовед

Како што интернетот полека се развива да биде и постанува главен извор за наоѓање и споделување на информации, како и главен подржувач на електронската трговија, Се повеќе и повеќе се зголемува проблемот кој просто и едноставно се нарекува емаил СПАМ.

СПАМ пораките се најчесто пораки кои се праќаат до корисници со цел да се извлечат информации како (име презиме адреса итн), или да бидат пренасочени до лажен сајт преку кој може да се "украдат" нивните лозинки итн. Или спам е лажна информација пратена преку емаил од еден до друг корисник, испраќачот на пораката е најчесто непостоечна личност.

Емаил спамот има големо негативно влијание врз корисничкото искуство на емаил корисниците. Смап пораките се многу голема закана за ширење на многу лажни информации низ Интернетот и со тоа намалување на веродостојноста на Интернет информациите.

Емаил спамот заедно со "лажно" креираните веб страни и неточните информации на нив, се еден од најголемите предизивици со кој се соочуваат ИСП (Интернет Сервер Провајдерите) како и Пребарувачките Алгоритми (search engines) како Google, Yahoo итн. Иако проблемите со емаил спамот се многу добро познати и постојат некои решенија, кои сеуште не се многу ефикасни поради тоа што развојот на антиспам техниките и механизмите е лимитиран поради не постоењето на КОРПУС за веб спам кој би го водел глобалниот развој на антисмап-от.

Исто така проблемите се зголемија со појавата на бесплатните емаил сервери.

Како несакана последница на бесплатните емаил сервери низ светот, се појави спамот. Спамот или емаил спам пораките се сериозне проблем кој ги афектира сите Интернет корисници. Според MessageLab, во моментов повеќе од 60% од емаил сообраќајот е спам. Иако постојат голем број на антиспам механизми и техники, спамот е сеуште голем проблем.

Потребно е да се изнајде решение за декетција и спречување на спам пораките што поблиску до страна на праќачот на спамот со цел да се намали нивниот волумен и препраќање како и да се намалеи непотребниот спам сообраќај од страна на емаил серверите, како и потрошеното време за процесирање и анализа на примените пораки на емаил серверите.

Во моментов отворените прокси сервери се главни извори на спам пораки. Овие сервери се омилен избор на креарорите на спам пораките поради можноста да се сокријат.

Поради тоа, заштитата на информацијата е клучна работа и една од приоритетните задачи на кој било безбедносен систем, без оглед дали се работи за заштита на еден компјутер, мрежа од компјутери, или податоци на една цела компанија.

Во денешно време многу големо внимание се посветува на сигурноста на компјутерските мрежи. Секој ден се објавуваат вести дека некоја компјутерската мрежа е пробиена од некој хакер. За да се заштитат од вакви несакани последици компаниите и сите останати се трудат со различни техники на подобар начин да го заштитат пристапот на одредени луѓе до нивните податоци.По дефиниција, сигурноста на компјутерската мрежасе состои однепробојна инфраструктура, полиси наметнати од мрежниот администратор за да се заштитат податоците од не авторизирани луѓе. Тоа се луѓе кои не се предвидени да бидат корисници на таа мрежа и мрежниот администратор постојано ја надгледува и одржува мрежата со цел за нејзина поголема ефективност.

2. SPAM LAUNDERING MECHANISMS

Во овој дел се истражуваат техниките за детекција на спам. Под прокси емаил серве се мисли компјутер или сервер на кој е инсталирана апликација SOCKS која прави транслација на протоколот или ги препишува IP адресата и бројот на портата и секако како такви ги тунелира пакетите. Емаил препраќачот (relay) ја прима целата порака и потоа целата порака само ја препраќа до наредниот емаил сервер (до крајниот). Емаил прокси има потреба конекцијата на двете страни (двата емаил сервери) од проксито да бидат синхронизирани додека емаил порака се праќа (од едниот до другиот сервер). Емаил препраќачот (relay) ја додава информацијата "Received Form" (во која е запишана IP адресата на праќачот и временски запис – timestamp, кога пораката е примена) пред хедерот на пораката пред пораката да биде испратена.

Емаил проксито не запишува таков тип на информации за време на процесот на праќање или процесот на трансмисија на пораката. Од перспектива на примачот на емаил пораката, Емаил проксито е оригиналниот исопраќач на емаил пораката. Поради оваа функционалност Емаил проксито е една од оминелите избори за маил сервери на праќачите кои испраќааат спам (Спамер). Иницијално спамерот пребарува на интернет да најде отворени прокси емаил сервери, тоа се сервери кој е најчесто погрешно, нецелосно или лошо конфигурирани прокси сервери, кои поради пропустите дозволуваат било кој да се поврзе и да ги користи нивните сервиси. Денес постојат многу Интернет страници, Интернет портали како и бесплатни софтверски апликации кои нудат пребарувачка функционалност за наоѓање на отворени емаил прокси сервери. Но, голем дел од овие сервери брзо се отстрануваат од мрежа како отворени емаил прокси сервери (серверите се реконфигурирани со цел да се спреми спамирањето). Најидеално решените за спамерите е да имаат повеќе од еден "приватен" и стабилен прокси емаил сервер. Домашните компјутери кои се поврзани на Интернет со перманентна стабилна конекција се одлична мета или кандидат емаил прокси-а за спамерите.

Со цел еден компјутер да може да биде реконфигуриран од одреден спамер за да стане емаил прокси сервер за испраќање на смап емаил пораки, се користи малициозен софтвер за презамање контрола. Од кога преку малициозниот софтвер ќе се инсталира успешно на пример програмата SOCKS, овие "зомби" компјутери стануваат емаил проски сервери спремни за препраќање на спам пораки (пораки на кој не може да се открие почетната дестинација). Најголем дел на корисниците на домашни компјутери дури и кога имаат инсталирано на нивните компјутери SOCKS и тие да се испраќачи на спам пораки, тие истите најчесто воопшто не знаат за тоа и најголемиот дел од обичните корисници воопшто не можат да откријат сами. Последните истражуваања покажуваат дека најголемиот број на смап пораки се испратени од домашни незаштитени компјутери.

Со цел да се спречи големиот број на домашни компјутери кои се спамери, најголемиот дел од ИСП (Интернет Сервис Провајдерите) имаат политика да ги блокираат емаил портите 25 (SMTP портата 25), со ова се спречува било кој да биде испраќач те емаил сервер. Најчесто таа функција на емаил сервери ја имаат точно специфицирани и добро заштитени сервери.

Со оваа политика или преземен чекор за заштита ИСП се справуаат со спам пораки од домашните компјутери на нивните Интернет Корисници. Значи емаил серверот на ИСП прави емаил препраќање (relay) само на SMTP пораки од одредени IP адреси не од сите.

Нажалост спамерите имаат најдено заобилокување и за ова ограничување, наместо пораката да ја праќаат директно од Отворените емаил прокси компјутери, тие пораките ги испраќаат прво до емаил серверот на Интернет Провајдерот, таа порака потоа се препраќа понатаму.

Во фебруари 2005 Spamhaus, известија дека поради блокирањето на SMTP пратените пораки од било која адреса, и опишаното заобиколување на спамерите. Емаил серверите (главните емаил сервери на ИСП-ата) на ИСП станаа најголемите емаил спамери. Со ова проблемот со спамот не е решен, само наместо извор на пораките да бидат домашните компјутери на корисниците, извор на спам се станати легитимните емал сервери на ИСП.

Во следниот дел се објаснуваат Антиспам техниките кои се користат.

3. Техники за АнтиСпам

Многу антиспам техники се предлозежи и имплементирани со цел да се справат ИСП со емаил спам пораките од различни аспекти. Според поставеноста на антиспам механизмите техниките можат да се поделат во две категории: ориентирани кон примачот (recipient-oriented) или ориентирани кон праќачот (sender-oriented). Во следниот дел ќе бидат објаснети двете категории и решенија на механизми за справување со емаил спам.

3.1. АнтиСпам Техники ориентирани кон примачот

Оваа категорија на Аптиспам техники или блокираат / одложуваат емаил спам да стигнат до примачите на пораката или ги одбележуваат / маркираат емаил пораките дека се спам. Поради големиот број на решените истите се поделе во две под-категории:

- АнтиСпам Техники ориентирани кон примачот базирани според содржина (concent based)
- АнтиСпам Техники ориентирани кон примачот не базирани според содржина (non-content-based)

3.1.1 АнтиСпам Техники ориентирани кон примачот базирани според содржина

Технкиите користени во оваа под категорија се базираат на детектирање на спам пораки според анализирање на содржината на емаил пораката која ја побива примачот на истата, анализата вклучува анализирање на хедерот на пораката како и самата содржина (body).

Емаил Антиспам техниките според емаил адреса користат едностави филтри бели листи или црни листи (blacklists). Во белите лист се содржат сите прифатливи емаил адреси, додека во црните листи се содржат сите неправитливи емаил адреси. Црните листи лесно можат да се заобиколат со тоа што ако некоја емаил адреса се наоѓа на црна листа спамерот ќе креира нова емаил адреса, поради ова е корисно користењето и на бели листи со емаил адреси.

Garris има развиено нов систем на креирање на бели листи со емаил адреси, со користење на автоматска популација на белите листи со искористување на пријатен-пријатен релацијата помеѓу емаил кореспонденциите.

SpamAssasin е Хеуристички филтер, кој се базира на откривање на спам базирано според детекција на непрафатливи клучни зборови во хедер или содржина на порака или испраќање на емаил од домаин кој не постои воопшто (не може да се надје запис на ниту еден ДНС).

Секоја емаил порака SpamAssasin ја верифицира со хеуристичкиот филгер на правила, според тие правила се одредува дали пораката е спам или не.

Постојат и филтри базирани на машинско учење, бидејќи детекцијата на емаил спамот може да биде конвертирана во проблем на класификација на текст. Многу Содржински ориентирани филтри користат машинско учење за детекција на емаил спам.

Друг тип на пристап е Пристарно базиран (Bayesian-based) пристап на детекција на спам. Овие Пристрасни методи можат да ги променат алатките за класификација соодветно.

3.1.2 АнтиСпам Техники ориентирани кон примачот не базирани според содржина

Технкиите користени во оваа под категорија се базираат на детекција на спам според изворна IP адреса, рата на испраќање на пораките, злоупотреба на СМТП (SMTP) стандардите.

DNSBLs се дистрибуирани црни листи, кои зачувуваат IP адреси изворни IP на спамерите.

До нив се пристапува со користење на ДНС кверија. Кога ќе се воспостави SMTP конекција, MTA-то (Mail Transfer Agent) на примачот на пораката ја потврдува IP адресата на праќачот со помош на DNSBLs, ако IP

адресата се наоѓа на црната листа, примачот прекунува конекција без да го добие емаилот, ако IP-то не е на црната листа, емаил пораката се прима.

МАРИД: MARID (MTA Authorization Records In DNS) е класа на техники за справување со фалсивикувани емаил адреси. МАРИД исто така се базира на ДНС и може да се види како дистрибуирана бела листа на авторизирани МТА. Повеќе драфт верзии за МАРИД се предложени, некои од нив се веќе во активна употреба. К-Р (Challenge-Response, C-R): се користи за се задржи веродостојноста (merit) на белите листи без загуба на важни информации. Доаѓачки пораки чија емаил адреса не се наоѓа на белата листа се вратени назад со цел да бидат проверени за спам "рачно" од администраторот на ИСП, наместо автоматски.

Ако администраторот потврди дека таа порака не е спам, емаил адресата се додава на белата листа и при следното праќање на емаил од истата адреда емаил порака ќе помине. Tampfailing е базирано на фактот дека легитимните СМТП сервери имаат имплементирани механизми за повторен обид (retry) кој се бара од СМТП, но смаперите не можат да имплементираат механизми за повторен обид (retry). Ова најчесто имплементира со креирање на сива листа која ги зачувува која ги зачувува пораките и МТА-та кои не поминале од прв обид. Задоцнетите пораки е една од негативностите на Антиспам механизмите и техниките. Ова најчесто се случува кај МТА серверите кога почнуваат да добиваат во еден момент голем број на пораки и со цел да се спречи спам сите пораки се процесираат и поради тоа има доцнење. Постојат и техники базирани на Анализа на Однесување (Behavior Analysis), тие откриваат спам пораки според однесувањето на праќачот и анализа на СМТП конекцијата.

3.2. АнтиСпам Техники ориентирани кон праќачот

Постојат и методи на регулација на користење. За ефикасна детекција на спамот уште на изворот, ИСП (интернет сервис провајдерите) и ЕСП (емаил сервис провајдерите) преземаат повеќе различни механизми како што е блокирање на порта 25, СМТП автентификација, со цел да се регулира користењето на емаил сервисот. Предложени се и повеќе протоколи за испраќање на пораки (Message submission protocol) кои во иднина треба да го земенат СМТП, ти би се користеле кога емаил порака се испраќа од еден МКА (Маил кориснички Агент - Mail User Agent) до неговиот МТА, Пред испраќање на маилот до дестинацискатa адреса.

Постои и пристап базиран на трошок (Cost-based), оваа идеја е позајмена од поштенските марки од системот за обична, регуларната пошта. Идејата е доколку се наплаќа за емаил пораките во зависност од бројот на сервери те далечината, смап пораките би престанале.

SHRED предлага користење на електронски маркици за емаил пораките, и доколку бројот на поминати сервери не одговара на далечината, бидејќи смап пораките имаат подолга патека.

3.3 HoneySpam

HoneySpam е спицијализиран honeypot фрамеворк базиран на honeyd за детекција на емаил адресни харвестери (собирачи), бази со смап адреси, како и да спречи или блокира смап сообраќај кој оди преку поставување на "лажни" отворените прокси сервери. Овие лажни отворени прокси сервери се креираат намерно со цел да се отркријат смаперските изворни IP адреси како и емаил пораките од кој потекнуваат спам пораките. Главна предност на HoneySpam за разлика од сите други техники и методи е што собира податоци кои понатаму можат да бида употребени за легални процедури против креаторите на спам пораките.

HoneySpam со креирањето на база на спамери е наблиску до форензичко антиспам решение.

4. Системи За Детекција на напади (Intrusion Detection System)

Систем за детекција на напади (Intrusion Detection System ИДС) го следи мрежниот сообраќај за сомнителни активности и алармира кога ќе детектира напад. Алармирањето најчесто е со известување кое се испраќа до систем администраторот или со праќање порака до некој од уредите во мрежата да го блокираатсомнителниот сообраќај. Ова може да се направи користејќи го SNMP протоколот. Постојат повеќе типови на ИДС, како и различни поделби. Првата поделба е според локацијата на ИДС. Според оваа поделба имаме два типа:

- мрежно базирани ИДС (network based intrusion detection system) каде има еден ИДС за сите хостови во компјутерската мрежа
- хост базирани ИДС (host based intrusion detection system)каде на секој хост имаме посебен ИДС

Друга поделба е според начинот на детекција на нападите:

- Базирани на правила (signature based): овие ИДС детектираат напади според предходно познат правилоза напад. Може да се детектираат само познати напади, но не и нови напади.
- Базирани на аномалија (Anomaly based): овие ИДС како нови напади детектираат сообраќај кој отстапува многу од нормалниот тип на сообраќај.

Кога се покренува аларм може да се случат една од следниве четири опции:

- False Positive: се случил напад кој не е откриен од ИДС
- False Negative: (не е покренат аларм за напад од ИДС, тоа не е напад)
- True Positive (покренат е аларм за напад од ИДС, тоа е напад)
- True Negative (покренат е аларм за напад од ИДС, тоа не е напад)

Веројатноста на погорните е мерка за ефикасноста на алгоритмот користен во ИДС.

Последната поделба е според начинот на реакција на алармот:

- пасивни
- активни

Пасивните само го следат сообраќајот и алармираат во случај на детектиран напад, додека реактивните ИДС превземаат акција најчесто со користење на SNMP протолокол, да го блокираат хостот / напаѓачот од една дадена мрежа да не може да праќа пакети.

Посленда и најнова работа во област на ИДС е мрежен реактивен ИДС со методи за поправка (Network Intrusion Detection and Recovery System). Овие ИДС покрај следење, детектирање на напади, преземање на акции да се отстрани напаѓачот од мрежата, можат да испратат порака до некој од другите сервери да преземат далечинкси акции да се отстрани малициозниот софтвер (софтверот што генерира напади од тој хост) од хостот / компјуерот и на компјутерот повторно да му биде дозволен пристап на мрежа. Една од основните идеи за ИДС-ите како и насоките кон кои тие се движат и развиваат е да го детектираат, остранат или спречат нападот и најдат напаѓачот, со што помала интервенција на систем администраторот. Повеќето од ИДС денеска не се имплементирани со користење на единствен дизајн или функционален пристап. Генерално тие користат повеќе пристапи за да соберат информации и детектираат сомнително однесување во системот. Кога тие се користат заедно, може да бидат наредени во хиерархија (апликација-хост-мрежа). Излезот од ИДС може да се користи од други ИДС во исто или повисоко ниво на хиерархија.

4.1. Мрежно Базирани ИДС

Мрежно базираните ИД системи можат да бидат дефинирани како мрежен хардвер. Тие го мониторираат мрежниот сообраќај и го анализираат врз основа на одреденизаписи. За да се направи ова мрежниот интерфејс е наместен во слободен мод и ги собира сите пакети преку мрежата. Собирањето на податоци е поделено на три главни типа во зависност од записите. Тие се стринг записи, порт записи и хедер записи.Порт записите едноставно го мониторираат сообраќајот помеѓу одредени порти. Ги

набљудуваат добро познатите порти за напад како FTP(TCP 21), telnet (TCP 23) и IMAP (TCP 143). Доколку било која од овие порти не се користи од кој било сервис во системот, пакетите кои доаѓаат на овие порти можат да бидатсомнителни.Предноста на мрежно базираните ИДС е дека тие се генерално ОС независни и работат на мрежно ниво, не се лоцирани на секој хост и немаат никаков ефект на постоечкиот систем. Тие се многу флексибилни. Но исто така тие имаат и недостатоци посебно под големи мрежни преоптоварувања. Генерално тие се слаби во филтрирањето на пакети во преоптоварени мрежи кои имаат многу сообраќај поради големиот број на хостови. Понатаму исто така има проблеми да се додаде нов запис или правило за нов тип напад или непознат протокол.

4.2. Snort

Snort е signature based ИДС лесен и едноставен за користење, изворниот код е само 100 kb, лесно се конфигурира и нема потреба од дополнителни алатки (како софтвер за ‘фаќање’ на мрежниот сообраќај),

Snort ИДС-от е составен од 4 основни дела:

- Декодирање на Пакетите (Packet Decoder), Преведување на содржината на пакетот од HEX системво ANCII систем
- Конверзија на податоците (Pre-procesing)преведување на содржините во разбирлива форма SNORT за процесира понатаму
- Детектирање на падати (Detection Engine), Споредување на пакетите со веќепозаните научени упади / напади
- Испраќање на известување (Post-Processing), Испраќање на известување за детектираните упади / напади

4.3. NetRanger

NetRanger е мрежно базиран ИДС кој е иницијално развиен од WheelGroup, но денеска е интегриран во Security Detection System од Cisco. Го мониторира мрежниот сообраќај со специјализиран хардвер интегриран во Cisco мрежните продукти (рутери, свичеви и сл.). Се состои од Сензори, Директори и PostOffice компоненти. Сензорот се состои од минимум два мрежни интерфејси. Еден за да комуницира со директорот (главниот ИДС агент), изведува операции за одржување и други за да го надгледува (мониторираат) сообраќајот и фаќаатIP мрежни пакети. Кога сензорот ќе одлучи да извести дека има инцидент, праќа податоци до директорот.

Директорите (Directors) овозможуваат централизирана контрола на сензорите кои се поврзани директно со нив. Директорот го надлгедува и контролира сензорот, собира податоци и исто така додава нови потписи за напад кон сензорите. За да се превенира DoS (denial-of-service) напад, самите директори не прават операција, анализи на податоците. Тие пишуваат

множество податоци во датотеки од записи (лог фајл) и овие датотеки можат да бидат прочитани од други бази (NSDB, network security database) и може да бидат одделно анализирани од ИДС. Директорот може исто така да се справи со корисничко дефинираните одговори наспроти извештаите за напад. Може да информира само за безбедносни прашања со покажување дека е во состојба на работа или, исто така, да иницираат работа на други алатки.PostOffice е одговорен за организирањена на сензорите и директорите. Овозможува точка-точка конекција помеѓу сензорите и соодветните директори за да се превенира испраќање извештаи за одреден мрежен дел.

5. Заклучок

Во денешното информатичко општество, информацијата вреди многу. Поради тоа заштитата на информацијата е клучна работа и една од приоритетните задачи на кој било безбедносен систем. Доколку одредена информација се открие од страна на не авторизиран корисник може да биде критична не само за еден човек туку и за целата компанија.

Области во кои се изведуваше истражувањето беа: апликативната безбедност (Firewall, IDS системи) и мрежната безбедност (network security) и детекција на спам (spam email).

Со тестирањето на функционланости на предложениот ИДС, кои се менацирани од предложениот алгоритам, ја потврдивме основната идеја на трудот, што е интеграција на мрежна и апликативна безбедност со цел делумно да се автоматизира и намали потребата од мануална интервенција на систем администраторот. Се надеваме дека ова истражување би можело да придонесе во развивање на идни целосно автотономни ситеми, кои ќе се управуваат со нападите во една компјутерска мрежа (напади кои може да бидат спам емаил кој би можел да украде важни информации) без потреба од интервенција на систем администраторите.

5.1. Идна Работа

Покрај истражувањето кое е извршено во овој труд и заклучоците кои се донесени, сепак остануваат следниве отворени прашања кои би можеле да се истражуваат понатаму во иднина. Тоа се следниве три главни прашања: Anomaly detection, со детекција на нови напади предложениот алогритам сигурно ќе биде подобрен, и процентот на детектирани напади и емаил спамови подобар. Забрзување би се постигнало со кеш (cache) меморија која ќе се користи помеѓу дистрибуираниот агент и централниот ИДС и трето користење на графички процесор со цел да се заврза процесирањето на податоците и да се намали доцнењето.

6. Литература

1. IOANNISAVRAMOPOULOS, MARTINSUCHARA, Protecting the DNS fromRouting Attacks, IEEE COMPUTER,SEPTEMBER/OCTOBER 2009

2. Ulrik Franke, Waldo Rocha Flores, and Pontus Johnson, Enterprise Architecture Dependency Analysisusing Fault Trees and Bayesian Networks,SCS 2009

3. Samrat Mondal and Shamik Sural, XML-Based Policy Specification Framework forSpatiotemporal Access Control, SIN'09, October 6–10, 2009, North Cyprus, Turkey.

4. Christian Braun and Robert Winter, Integration of IT Service Management intoEnterprise Architecture, SAC'07, March 11-15, 2007, Seoul, Korea.

5. Henk Jonkers, Marc Lankhorst, René van Buuren, Stijn Hoppenbrouwers, Marcello Bonsangue,Leendert van der Torre, Concepts for Modelling Enterprise Architectures, 2008

6. Operating Systems Internals and Design Principles (5th Edition), William Stallings, 2009T. Hunter, P. Terry, and A. Judge. Distributed tarpitting:

7. Impeding spam across multiple servers. In Porc. USENIXLISA 2003, San Diego, CA, October 2003.

8. J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan. Fastportscan detection using sequential hypothesis testing. InProc. IEEE Symposium on Security and Privacy 2004,Oakland, CA, May 2004.

9. K. Li and Z. Zhong. Fast statistical spam filter by approximateclassifications. In Proc. ACM SIGMETRICS 2006, St. Malo,France, June 2006.

10. N. Provos. A virtual honeypot framework. In Proc. USENIXSecurity 2004, San Diego, CA, August 2004.

11. S. Radosavac, J. S. Baras, and I. Koutsopoulos. A frameworkfor mac protocol misbehavior detection in wireless networks. InProc. 4th ACM workshop on Wireless security, Cologne,A. Ramachandran, D. Dagon, and N. Feamster. CanDNS-based blacklists keep up with bots? In CEAS 2006,Mountain View, CA, July 2006.

12. A. Ramachandran and N. Feamster. Understanding thenetwork-level behavior of spammers. In Proc. ACMSIGCOMM 2006, Pisa, Italy, September 2006.

13. M. Roesch. Snort - lightweight intrusion detection for networks.In Proc. USENIX LISA 1999, Seattle, WA, November 1999.

14. R. D. Twining, M. M. Williamson, M. Mowbray, andM. Rahmouni. Email prioritization: Reducing delays onlegitimate mail caused by junk mail. In Proc. USENIXAnnual Technical Conference 2004, Boston, MA, June 2004.

15. A. Wald. Sequential Analysis. Dover Publications, 2004.

16. M. Walfish, J. Zamfirescu, H. Balakrishnan, D. Karger, andS. Shenker. Distributed quota enforcement for spam control. InProc. USENIX NSDI 2006, San Jose, CA, May 2006.

17. M. M. Williamson. Design, implementation and test of anemail virus throttle. In Proc. 19th Annual Computer Security

18. Y. Zhang and V. Paxson. Detecting stepping stones. In Proc.USENIX Security 2000, Denver, CO, August 2000.