Нов български университет
Ne varietatem timeamus

КУРСОВА РАБОТА

ПО ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

НА ТЕМА:

ЗАЩИТА НА ИНФОРМАЦИЯ ЧРЕЗ ЗАСИЧАНЕ НА ПРОНИКВАНИЯ

Изготвил:

Кристиан Салуми

f64669

4-курс

2-ри семестър

Проверил:

СОФИЯ

2015/2016, Пролетен семестър

УВОД

През 21в. развитието на телекомуникационните мрежи е направило гигантски скок от верижните и пакетни мрежи към изцяло IP базираните мрежи. Това развитие е създало единна среда, в която комуникацията от приложения и услуги е прехвърлена до върха на IP протокола. В същото време скоростите за обмен на информация са се увеличили значително от 2G радио мрежи за достъп до 3G. Също така, устройствата, които абонатите на телекомуникационни мрежи използват, са се развили до такава степен, че границата между мобилни телефони и компютри вече е доста неясна. С модерните мобилни устройства, познати още като смарт телефони, потребителят може да прави почти всичко, което може да бъде направено с един обикновен персонален компютър. Това означава, че цялото съдържание на интернет днес се побира в джоба на всеки притежател на смарт телефон.

Въпреки, че развитието на комуникационните мрежи води до по-добра устойчивост на технологиите, то води със себе си и редица нови и нежелани възможности. Заплахи, които са били приложими само във фиксирани мрежи, днес са осъществими и в достъпа на радио мрежите. Имайки предвид, че заплахите стават все повече и по-сложни, това означава, че и системите за сигурност трябва да станат по-интелигентни. Основните мерки за сигурност като „защитни стени“ и „антивирусни скенери“ са в техните граници за справяне с нарастващия брой интелигентни атаки през интернет. Решение за повишаване на общите мерки за сигурност на мрежите е повишаването на нивата на сигурност със системи за откриване и проникване.

За да разберем каква роля играе детекторът за проникване в телекомуникационните мрежи, трябва да погледнем един прост пример. Помислете за детектора за проникване като за охранител, който пази входната врата на фабрика. Помещенията на фабриката представляват мрежата на мобилния оператор, а оградата на фабриката е защитната стена на оператора. В този пример, служителите на фабриката ще са трафикът в мрежата на оператора.

Известно е, че фабриките са добре защитени и няма да допуснат вътре в помещенията хора, които не притежават нужните пропуски. Оградата или в този случай защитната стена, има отговорността да държи всички нежелани посетители извън помещенията на фабриката. Точно както защитната стена,

оградата има дупки(вратички), което позволява на служителите да влизат и излизат от фабриката. Тези дупки в оградата правят фабриката уязвима за нежелани посетители, което налага и необходимостта от охранител, който да пази главния вход.

В зависимост от ролята, която изпълнява охранителят, докато наблюдава хората, които влизат и излизат от фабриката, той уведомява началника на сигурността, когато открие подозрителен обект, който се мъчи да премине през главния вход. Основната функция на системата за проникване е, че тя е първият пример за защита. Тази система генерира аларма, когато открие нещо подозрително, след което персонала по сигурността в мрежата на оператора допълнително разследва причината за алармата.

За да може защитата да върши успешно своята работа, са необходими набор от правила и инструкции. В контекста на тази защита по отношение на телекомуникационните мрежи, правилата и инструкциите са алгоритми, които самата защита използва, за да анализира мрежовия трафик. Въпросът е : „Как трябва да бъдат дефинирани тези правила и инструкции и по-специално какви са критериите, по които се решава какви функции трябва да се следят?“ Именно отговорът на този въпрос е основната цел, която си поставя авторът на настоящата курсова работа.

1. Заплахи за телекомуникационните мрежи

Развитието в телекомуникационните мрежи се насочва към мобилност в радио мрежите за достъп. Например, във Финландия, много от операторите изтеглят медните проводници в селските райони и подменят цифровите абонатни линии за връзка с 3G. Според новинарските статии, докладвани в HS.fi[1] и Tietokone.fi[2], компанията обявява своите планове за изтегляне на медните проводници и тяхната замяна.

В известен смисъл развитието, или както някои биха се изразили неразвитието на мрежите, е преминало от локални мрежи за достъп до радио мрежи за достъп, което е по-лесно и евтино за извънградските райони, където гъстотата на мрежовата инфраструктура е незадоволителна. Независимо, че във

[1] http://www.hs.fi/talous/artikkeli/Sonera+korvaa+lopetettavat+lankaverkot+3gll%C3%A4+ja+Digitan+450-verkolla/1135234793887
[2] http://www.tietokone.fi/uutiset/2008/sonera_sulkee_19_000_adsl_liittymaa

Финландия е налице дискусия[3] относно развитието на широката оптична мрежа в страната, за момента единственият вариант за множество хора е все още да използват RAN връзки.

От гледна точка на абоната може да изглежда, че инфраструктурата на телекомуникационните мрежи се състои само от група радио кули, пръснати из селските и градски райони. В действителност обаче, основната инфраструктура на мрежата е доста по-сложна от базови станции и радио интерфейси.

Телекомуникационните мрежи имат много общо с корпоративните мрежи. В корпоративните мрежи има стотици компютри и потребители, свързани помежду си чрез рутери, суичове и взаимосвързани мрежи.. В телекомуникационните мрежи има същите елементи, както и в корпоративните мрежи, но в допълнение има и няколко мрежи за радио достъп (RAN) от GSM към LTE и огромен брой стационарни и мобилни потребители. Инфраструктурата на телекомуникационните мрежи може да бъде разделена на три под-мрежи: мрежа за достъп; основна мрежа и сервизна мрежа. Това е илюстрирано на фигура 1.1

- **Мрежи за достъп**

Частта от мрежата, която осигурява връзка и достъп на потребителите до услугите на техния доставчик, се нарича мрежа за достъп (фиг.1.1) Мрежата за достъп може да се раздели на фиксирани мрежи за онлайн достъп(Ethernet, xDSL, WLAN) и радио мрежи за достъп (2G, 3G, LTE, CDMA, WLAN). Друго понятие, използвано в телекомуникационните мрежи, е потребителската мрежа. Тази мрежа е комбинация от мрежовия достъп едновременно на потребителските съоръжения на абоната, като мобилни телефони, лаптопи и пр.[4]

- **Развиваща се пакетна централна мрежа**

Междинната мрежа, която свързва мрежите за достъп със сервизните мрежи, се нарича развиваща се пакетна централна мрежа.(фиг.1.1) В допълнение към опериращата междинна мрежа, централната мрежа е отговорна за операциите по цикличното и пакетно превключване, абонатното таксуване, AAA услугите и абонатните услуги за управление на мобилността. [3]

[3] L 22.12.2009/1186, (Law for supporting broadband development in rural areas).

[4] 3GPP TS 23.401 V10.2.1, 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspect; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 10). 3GPP, 2011. Technical Specification.