APPLICATION OF MULTIAGENT SYSTEMS FOR THE PURPOSES OF CYBERSECURITY

Pavel G. Gerasimov

Gate-92 DG – Intellekt TGK, Sevlievo-Sofia, Bulgaria, p.g.gerasimov@gmail.com

***Abstract**: The following article has the aim to present some theoretical and practical application aspects of the multiagent systems designed for the purpoces of cybersecurity and as a result to present a new type of multiagent systems that could be developed. Contemporary multiagent systems focus themselves mostly on the protection of the communication infrastructure and leave a gap in the endpoint protection, which is utilized in most cases for attacking and observing control over sensitive information arrays and resources or systems that are designed for providing information services. Our focus is on the endpoint protection and the management tools that are used in order to set to minimum the ability for attack through the smallest piece of the information system.*

***Keywords**: Multiagent systems, Cybersecurity, Endpoint protection, Network protection, Intrusion detection systems.*

ПРИЛОЖЕНИЕ НА МНОГОАГЕНТНИ СИСТЕМИ ЗА ЦЕЛИТЕ НА КИБЕРСИГУРНОСТТА

Павел Г. Герасимов

Въведение

Киберсигурността през последните няколко години се превърна в понятие, което придоби значителна по своите мащаби популярност и навлезе скоростно в дневния ред на съвременното информационно общество. Ако преди малко повече от десетилетие, общественият консенсус се базираше на физическата сигурност и защита на отделният индивид и мерките и способите прилагани за постигането на първите две, то днес е налице все по-активния дебат касаещ защитата на отделния индивид в дигиталното пространство.

С развитието на информационните технологии през последното десетилетие човечеството и отделният индивид установиха една нова форма на заплаха, а именно кибер заплахите. Кибер заплахите са сравнително ново явление, което може да се твърди, че в началото бе достояние на определени професионални кръгове и международни, бизнес и държавни структури, което с течение на времето започна да се превръща в тема както за размисъл, така и за задъбочена дискусия за по-широк кръг от индивиди обединявани от една обща характеристика – използването на възможностите на интернет и информационните технологии.

С развитието на кибер заплахите, паралелно но не и с изпреварващо темпо се развиват и решенията касаещи пряко обезпечаването на мерките по киберсигурността и прилагането на съ-

ответните политики в същата област. Палитрата от технологии и решения, които днес биват впрегнати по посока на обезпечаване на киберсигурността е толкова голяма, че много трудно може да бъде обхваната в рамките на едно кратко разглеждане. Въпреки това, измежду наличните технологични решения и ресурси днес своя път започват активно да си проправят и системите използващи изкуствен интелект и по-специално системите базирани на интелигентни автономни агенти.

Интелигентните автономни агенти намират широко приложение при реализацията на многоагентни системи за мрежова информационна сигурност от гледна точка използването им като основни функционални единици пряко ангажирани с постигането на определени цели и изпълнението на определени задачи, които биват дефинирани още на ниво проектиране на системата и уточняване на специфичните изисквания към нея. За да бъде максимално добре разбрана философията на многоагентните системи е необходимо да бъде разбрана ролята на интелигентния агент и начините на взаимодействието му с останалите агенти съставящи системата.

Целта на настоящите разглеждания е да направи кратък преглед на налични многоагентни разработки и решения касаещи киберсигурността, да анализира техните предимства и недостатъци и на база извършения анализ да бъде предложена нов тип многоагентна система, която да предразполага създаването на инструментариум, който да обезпечава в максимална степен прилагането на мерките по линия на киберсигурността.

Преглед на съществуващи решения

В началото на настоящите разглеждания нека първо да дефинираме понятието агент. Агент е такъв тип компютърна система, която при поставянето си в определена среда е способна да извършва набор от автономни действия, с които да решава определен набор от задачи, поставени в процеса на нейното проектиране. Автономният интелигентен агент като отделна система е способен да извършва наблюдение спрямо средата, в която е поставен посредством сензори и същевременно да извършва промени в нея посредством средства познати в теорията като ефектори или манипулатори по посока реализиране на дефинираните в процеса на проектиране цели и задачи. [1]

Автономният интелигентен агент има три основни режима на работа, които обуславят неговата автономност – перцепция, разсъждение и действие. Интелигентния агент бива характеризиран и с още едно свойство, а именно гъвкавост, което се изразява във възможността интелигентния агент да се ориентира и да изпълнява задачи в среда, която не е предварително дефинирана и съответно е налице необходимост агента да се адаптира и обучава в процеса на работа. Съществуването на автономен интелигентен агент бива обусловено и от гледна точка на „агентно-ориентираното програмиране, което има в себе си за цел прилагането на концепциите залегнали в дефиницията за изкуствен интелект и свързаните с нея технологични решения. [14]

Многоагентната система бива разглеждана теоретично като система съдържаща в себе си два или повече автономни интелигентни агенти, активно взаимодействащи помежду с дейности представляващи социализиране, координиране и договаряне, които биват прилагани за изпълнението на определени действия по посока на постигане на зададените предварително цели и задачи. [1, 6, 7, 9] Въпреки, че е налице организационно взаимодействие между отделните агенти съставящи една многоагентна система, е от критично значение да бъде разбрано, че многоагентната система няма как да изпълнява зададена обща цел. Точно обратното, при многоагентната система е налице задаване на строго индивидуална и конкретна цел спрямо всеки един съставящ агент. Хипотетично е допустимо наличието на обобщена обща цел, която се дефинира от проектиращият/ите системата, но това е реализируемо само и единствено посредством включването на голям брой интелигентни агенти с дефинирани индивидуални локални цели, които да водят към реализацията на обобщената цел посредством осъществяване на нейни подчасти. [1]

Защитата на многоагентните системи за целите на киберсигурността е обект на разглеждания за редица колективи в научния мир. В публикация по темата озаглавена "Security in Multi-Agent Systems", авторите Хедин и Морадиан коментират важността на аспектите касаещи защитата на многоагентните системи като засягат проблема свързан с липсата на визия от страна на разработчиците относно защитата на системите. Авторите правят забележката, че този проблем се появява в следствие на масовото прилагане на т.нар. „Гея-методология" и неспособността на последната да предложи механизми за защита на многоагентната система. [7] В същата своя публикация авторите изказват твърдението, че многоагентните системи страдат и от още един недостатък що се касае до защитата на определени видове софтуерни приложения и информационни системи. Този недостатък се състои в слабости свързани с удостоверяването на информацията, която агентите събират от интернет, възможностите за неоторизиран достъп до даден агент, част от многоагентната система, както и несигурната комуникация между агентите съставляващи многоагентната система, което създава предпоставки за пробив в системата и от там несанкциониран достъп до защитаваната система. [7]

В научна публикация озаглавена „Multi-agent systems for protecting critical infrastructure", авторът Бейг прави анализ и коментар относно важността на многоагентните системи що се касае до приложението им за защита на най-различни категории системи, като такива за електронна търговия, електронно здравеопазване, системи за контрол на достъпа, телематика, транспорт и околна среда. [4] В разглежданията си авторът прави важното уточнение, че една добре проектирана и функционираща многоагентна система се базира на прилагането на техники от областта на невронните мрежи, размитата логика и генетичните алгоритми. Прилагането на тези техники осигурява сигурно и адекватно възприемане от страна на всеки съставящ многоагентната система агент и възможност за гарантирана реакция в критична за системата ситуация. Важна особеност, която следва да бъде отчетена е в случай на отказ на даден агент съставящ системата да изпълнява поставените му задачи, същият да бъде своевременно изолиран от системата и заменен функционално от съседните агенти, които поемат неговите функции. [4]

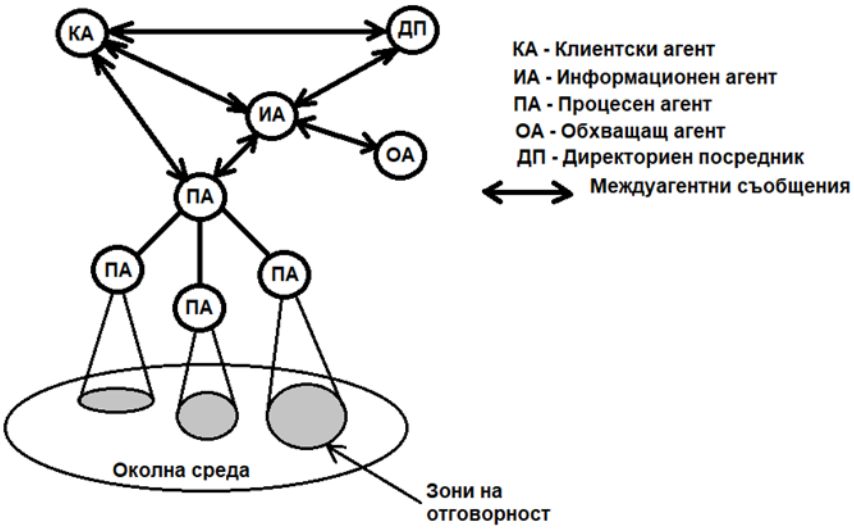
В друго изследване в същото направление озаглавено Cybersecurity as an Application Domain for Multiagent Systems, авторът изказва становището, че приложението на многоагентни системи има капацитета да спомогне за повишаването на киберсигурността на бизнеса, обществения сектор и държавната администрация. Многоагентните системи могат да бъдат счетени като едно от съвременните средства с възможност да запълни пропуските на техническо ниво при другите типове решения и същевременно да способства за обезпечаване на киберсигурността от гледна точка на социалния и човешкия фактор. [13] За да бъде максимално пълноценна една многоагентна система проектирана за целите на киберсигурността е налице нуждата от прилагането на две основни стъпки. Първата стъпка се съдържа в създаването на математическият модел на взаимодействието и формализирането на определени правила, касаещи процедурите по вземане на решение. Втората стъпка е свързана с интерпретирането на реалната работна среда, тестването, изследването и прецизната настройка на системата.

Удовлетворяването на горе-представените изисквания и изпълнението на представените стъпки създава предпоставки за реализиране на т.нар. „разслояване на системата". Разслояването позволява задаване на определени правила за действие на съставящите една многоагентна система агенти. Разслояването позволява реализирането на процедури по защита на системи обработващи и съхраняващи големи масиви от данни и платформи подпомагащи функционирането на подобен род системи. [12]

Обща структура на многоагентните системи

За да бъде разбрано по-добре функционирането на многоагентните системи нека да си послужим с една примерна илюстрация на многоагентна система и да разгледаме ролите, които имат

съставляващите я агенти. На фигура 1 е представена примерна схема на многоагентна система и съставящите я агенти.



Фигура 1: Схема на многоагентна система с ролите на съставящите я агенти

От това, което виждаме на фигура 1 можем да установим, че са налице четири отделни роли агенти и една системно специфична роля обозначена като „директориен посредник“.[10] Агентите, които изпълняват ролята на процесни агенти са отговорни за изпълнението на определен процес и свързаните с него дейности, като същевременно обезпечават и активното наблюдение на всички променливи и изменения засягащи дадена пространствено или функционално дефинирана среда и процесите случващи се в нея. Ролята на процесния агент е съпроводена и от още една особеност изразяваща се в йерархичност на процесния агент. Йерархичността се изразява в процесното ниво, на което се намира съответния агент, т.е. агент, който е с по-ниско йерархично ниво ще обработва по-голямо количество процесна информация свързана с контрола и следенето на определени параметри на средата, в която се намира. Нещо повече, агентът с по-ниско йерархично ниво препредава резултата от обработената информация на агента/ите от по-високо йерархично ниво, които обработват значително по-малко количество информация и изпълняват по-скоро обобщаващи функции в системата. [10]

Ролята на *информационния агент* се свързва с обработката на информацията в многоагентната система. Често пъти тази роля бива възприемана като основно свързващо звено между информационните ресурси и потребителите. Информационния агент е пряко отговорен за осъществяването на процесите свързани с обработка на информация, която е необходима за дейността на останалите агенти съставляващи многоагентната система. Информацията, която бива придобивана и обработвана от информационния агент бива раздробявана на малки порции и предавана в процеса на междуагентна комуникация към заинтересованите агенти.

Агентите, които изпълняват ролята на *Клиентски агенти* са пряко ангажирани с подпомагане на процеса по осигуряване на потребителски интерфейс, който да подпомага потребителят при извършването на определени дейности свързани с мониторинг върху многоагентната система и нейното управление. В случай на многоагентни системи с по-голям мащаб клиентските агенти се

използват и за предоставянето на отделен строго специфичен интерфейс за всяка отделна операция, заявена от потребителя.

Ролята на *Обхващащия агент* е свързана с достъпването на наследствени източници (източници на исторически данни) и обезпечаване на процеса по тяхното преобразуване в общ формат, като същевременно се създава възможност и за поддържането на услуги свързани с извличане на данни. *Директориинния посредник*, който бе споменат по-рано е специализиран тип агентна роля, която е стандартизирана от *Foundation for Intelligent Physical Agents (FIPA)* и се използва основно за управление на списъка от налични агенти и техните възможности.

Общи характеристики на средата на функциониране на многоагентна система

Средата на функциониране и действие, в която е поставена една многоагентна система е от особено значение както за нея, така и за агентите съставящи системата. Средата има основна роля при определянето на функционирането и предназначението на един интелигентен автономен агент. [1] Средата на функциониране се охарактеризира от пет основни двойки признаци, които я представят най-детайлно.

Първата двойка е „*Достъпна-Недостъпна*“. Достъпна е тази среда, в която при поставянето си агента е способен да получи своевременно пълна актуална и точна информация относно нейните състояния. Обратното, когато агентът при попадането си в средата не е способен да получи вече посочената информация, то тя се охарактеризира като недостъпна.

Втората двойка е „*Детерминистична – Недетерминистична*“. Като детерминистична се възприема тази среда, която позволява на всяко действие да има единичен гарантиран ефект, т.е. няма да имаме налични неопределености по отношение на състоянията, които ще бъдат резултат от извършваните действия.

Третата двойка признаци е „*Епизодична – Неепизодична*“. Като епизодична ще бъде възприемана тази среда, при която поведението на агента ще зависи от количеството (броя) на дискретните епизоди, без да е налице връзка между поведението на агента в различни сценарии. При неепизодичната среда агентът сам трябва да реши какви действия да предприеме въз основа само на текущият епизод. [1]

Четвъртата двойка признаци „*Статична – Динамична*“ дефинира следните признаци. При статична среда е налице неизменност като единственото, което търпи промяна е поведението на средата, което е пряк резултат от поведението и действията на агента. Динамичната среда се характеризира с това, че освен агента, който действа в нея съществуват и други процеси случващи се в нея и вследствие на това средата се изменя по начин, който е извън управлението на агента.

Последната двойка признаци е „Дискретна – Непрекъсната“. Дискретната среда се характеризира с определен краен брой от действия възприети в нея, докато при непрекъснатата броят на действията клони към безкрайност.

Основни типове интелигентни агенти

В чисто теоретичен аспект многоагентните системи често пъти биват разглеждани и като под-област на разпределените системи с изкуствен интелект. Това причисляване спомага от своя страна за дефинирането на три основни типа интелигентни агенти, а именно:

- *Когнитивен агент* – това е тип агент, който е способен да намери решение на комплексен проблем, посредством комуникация с други агенти и взаимодействие със собствената си база знания. Основните характеристики на когнитивният агент са: висок капацитет за извършване на разсъждения, обработка на данни, перцепция, обучение, управление, комуникация и експертиза в областта на действие.

- *Реактивен агент* – това е тип агент, който е способен да реагира бързо на прост проблем, неизискващ комплексни разсъждения. Нещо повече, при активно взаимодействие между голям брой агенти от този тип е налице повишено ниво на интелигентност на системата.

- *Хибриден агент* – това е тип агент, който може да бъде определен като смесица между реактивен и когнитивен агент. Хибридният агент притежава определени рефлекси (реактивна еволюция), посредством които решава повтарящи се или често срещани проблеми и същевремено има способността да мисли (когнитивен похват) що се касае до по-комплексни системни ситуации.

Обща класификация на многоагентните системи

От архитектурна гледна точка многоагентните системи се делят на еднородни, които биват съставени от еднотипни агенти; разнородни, които са комбинация от различни типове агенти; централизирани, при които системи с приоритет се отчитат сигнали, които са от по-горно йерархично ниво; децентрализирани, при които всеки съставящ агент има свое собствено произволно поведение, независещо от останалите съставящи агенти и комбинирани, които са системи обединяващи характеристики от досега описаните архитектури. За най-често срещан тип архитектура в практиката се считат комбинираните многоагентни системи.

При многоагентните системи е налице възможност и за въвеждане на допълнителни характеристики свързани с разнообразието на използваните в една система агенти, откъдето многоагентните системи се разделят на хомогенни и хетерогенни. Според възможностите, с които системата разполага е налице възможност за дефиниране на обикновени и разширени многоагентни системи, а според вида и реализацията на целите на многоагентната система да се разделят на съгласувани и противоречиви. От гледна точка на архитектурата си многоагентните системи могат да бъдат разделени на йерархични и децентрализирани, откъдето можем да изведем още три основни модела, а именно:

- *Делиберативна система* - това е такъв тип архитектура на многоагентна система, която съдържа изрично представен символичен модел на света, в който решенията се вземат чрез логически мотиви, въз основа на съществуващ модел и символна манипулация.

- *Реактивна система* – това е такъв тип многоагентна система, която не може да бъде адекватно описана от релационен или функционален аспект. Релационният аспект разглежда програмите като функции обхващащи от първоначалното до терминалното състояние.

- *Хибридна система* – това е такъв тип многоагентна система, при която агентът е изграден от две подсистеми: делиберативна, която разработва планове и взема решения базирани на логически мотиви и реактивна подсистема, която е способна да реагира на промени в средата без необходимост от сложни разсъждения.

Критериите, по които може да бъде оценена една многоагентна система са съгласуваност и координация. Съгласуваността се измерва като качество на взетото решение, ефективно използване на ресурсите, концептуална яснота и други. Координацията се явява степента, до

която агентите са способни да избегнат външната дейност изразяваща се в синхронизация и подреждане на тяхната активност. [1]

Общи характеристики на многоагентната система

Всяка една многоагентна система може да бъде охарактеризирана посредством използването на следните основни характеристики, които да спомогнат за нейното максимално подробно представяне:

- *Възприятие* – това е общата информация достигаща до сензорите на агентите, която впоследствие бива обработвана. Възприятието позволява на агентите да наблюдават данни, които се различават пространствено, времево или дори семантично. Тази способност позволява частично наблюдение на средата от всеки агент, което има различни последствия при вземането на решения от агентите.

- *Контрол* – при многоагентните системи контролът е децентрализиран, което от своя страна означава, че не съществува централен процес, който събира информация от всеки агент и след това решава какви действия трябва да предприеме всеки агент.

- *Знания* - при многоагентните системи нивата на познанията за отделните агенти и за състоянието на заобикалящата ги среда може да се различават значително. Тук като ключово понятие може да бъде разгледано общото знание, според което всеки агент знае факт, но и всеки агент знае, че всеки друг агент знае този факт.

- *Комуникация* – взаимодействието се свързва с определена форма на комуникация, като при многоагентните системи комуникацията може да бъде възприета като двупосочен процес, при който всички съставляващи агенти могат да бъдат потенциални податели и получатели на съобщенията.

- *Факторизация* – това е способността на един агент да дефинира възможностите си на база идентифицирането си с обект, който е свързан със сферата на приложение, за която е проектиран агента.

- *Гъвкавост* - при многоагентните системи гъвкавостта намира приложение от гледна точка на способността за оптимизация на една система с параметри, които не се различават значително, чрез внимателно планиран график и система за управление. Използвайки свойството гъвкавост съставящите агенти могат да се преконфигурират в процеса си на работа, което се явява важно предимство за системи, които трябва да отговарят на широк спектър от различни условия.

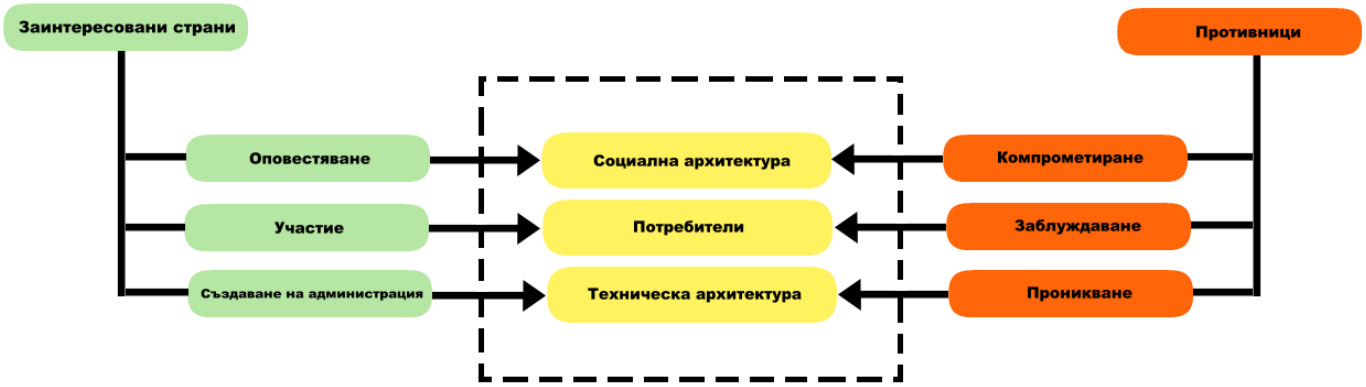
- *Промяна* – при използването на конвенционални техники следва да бъде отчетено, че най-скъпата част от една система, независимо от нейното предназначение не са машините, екипировката, оборудването или енергийните ресурси необходими за работата й, а създаването и последващото обслужване и поддръжка на софтуера обезпечаващ функционирането на същата. При системите с дълъг период на експлоатация е налице увеличение на разходите в продължение на времето на експлоатация.

Многоагентните системи и киберсигурността

Киберсигурността като понятие и като област на научно-изследователска дейност може да бъде свързана под една или друга форма с философията стояща зад създаването на многоагентните системи. Налице са изследователски твърдения според, които проблемите поставени от киберсигурността и решенията, които тези проблеми изискват могат много трудно да

бъдат решени еднозначно посредством решения, осланящи се на използването на един единствен интелигентен агент, който да бъде ангажиран с изпълнението на широкия спектър от изисквани действия. [13]

Многоагентните системи могат да бъдат възприети като технологично решение, до което се достига по естествен начин от гледна точка на факта, че за удовлетворяването на изискванията поставяни към осигуряването на киберзащита е необходим кооперативно базиран подход, който да осигури възможност за отчитането на интересите на две основни групи. Тук използваме израза две основни групи затова, защото при прилагането на многоагентния подход за целите на киберсигурността биват взети под внимание изискванията и очакванията към системата на защитаваната страна и възможните способи, средства и подходи, които ще бъдат използвани от атакуващата страна. Тук се появява необходимостта от намирането на баланс между предпазване и ограничаване на защитаваната страна и същевременно предвидимост и непредвидимост за атакуващата страна. За да бъде разбрана по-добре логиката на киберсигурността и връзката ѝ с многоагентните системи нека да разгледаме структурата на екосистемата на киберсигурността представена на фигура 3 .[13]



Фигура 3: Структура на екосистемата на киберсигурността

Заинтересованите страни съставляват в себе си всички компании, организации, държавни структури и отделни индивиди, които предприемат мерки по посока на защита на някаква определена чувствителна информация или система обработваща или съхраняваща такава информация. Противниците представляват атакуващите системата, върху която са приложени мерки за защита. Това са всички злонамерени страни опитващи да осъществят атака върху системата използвайки неправомерни средства и изследвайки системата за наличие на слабости. Всяка от двете страни прилага определен пакет от действия по посока защитата на системата, които най-общо биват групирани в три основни групи на дейности, отговарящи за трите основни елемента на защитаваната система.

Както е видно от фигура 3, защитаваната система се състои от три основни компонента: социална архитектура, потребители и техническа архитектура. Социалната архитектура се свързва с дефинирането на правилата за взаимодействие със защитаваната система и правилата за комуникация вътре в нея. Нещо повече, социалната архитектура обхваща правилата за достъп на отделните потребители възползващи се от възможностите на съответната система и съответно определя процедурите по делегиране на права на достъп. Техническата архитектура съдържа в себе си

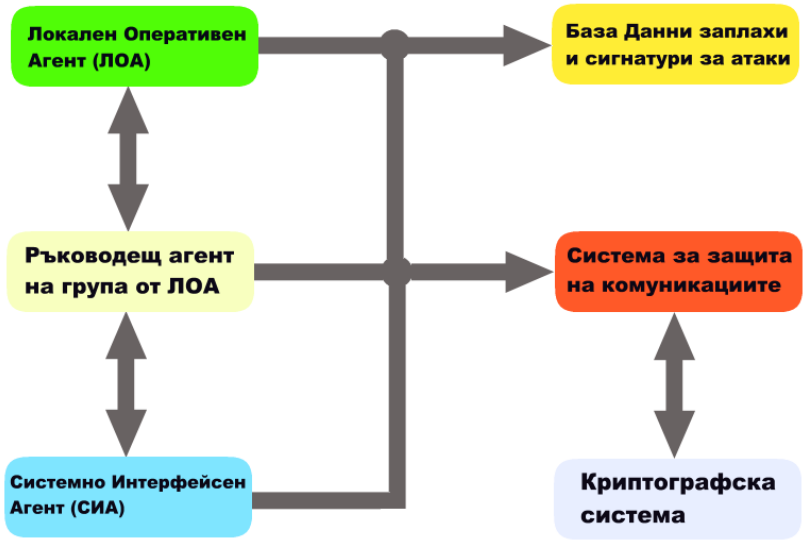
хардуерното и софтуерно обезпечаване на защитаваната система. Обобщено погледнато социалната архитектура дефинира поведението на потребителите и връзките, които те ще осъществяват със системата, а също така и връзките между отделните звена вътре в защитаваната система.

Ако трябва да бъде идентифицирано най-уязвимото звено в днешната екосистема на киберсигурността, то това е звеното „социална архитектура“. Социалната архитектура, е най-силно уязвима по направление на атаките от типа „вътрешен човек“ (на англ. Insider Attacks), които се характеризират с осъществяване или подпомагане на атаката от вътрешен за една организация човек, които може да спомогне за по-лесното осъществяване на пробив в масиви или елементи от една система, които при каквито и да е било обстоятелства няма как да бъдат достъпени от злонамерената страна. Всъщност може да се твърди, че атаките от типа „вътрешен човек“ са най-често срещани в корпоративния свят и в определени държавни или публични структури. Причините за възникването на този тип атаки са много и най-различни поради, което е много трудно да бъдат обхванати накратко в нашите разглеждания. Съществуват твърдения, че тези атаки се базират на първо място на психологическа основа и на второ на база преследване на определен личен интерес, но и до днес изследователите по темата се затрудняват с даването на точна причина за възникването на този тип атаки и заплахи.

Многоагентните системи може да се каже, че намират идеално приложение в подпомагането на защитата на потребителското ниво и нивото на социалната архитектура от екосистемата на киберсигурността. Гъвкавостта и способността за делегиране на изпълнението на широк кръг от задачи на многоагентните системи ги прави предпочитан вариант при решаването на задачи, касаещи защитата на тези два основни слоя. Говорейки за осигуряване на защитата на ниво социална архитектура и потребители, сме длъжни да съобразим, че технически приложимото решение се налага да премине през създаването на определени потребителски или системни норми. За правилното дефиниране на тези норми е необходимо да бъде прецизно определено поведението на бъдещите или настоящите потребители на една система и да се остави възможност за допълнително дефиниране на норми на поведение в процеса на работа на системата.

Предложение на многоагентна система за целите на киберсигурността

Многоагентната система, която ще разгледаме като предложено решение комбинира в себе си характеристики от двуслойните защитни многоагентни системи, многоагентните системи използващи модулно-базирани агенти и многоагентните системи със стохастичен характер, като обединява положителните характеристики, които те предоставят и същевременно позволява коригиране на техните недостатъци, което от своя страна спомага за по-голяма устойчивост на изследваната система. На фигура 4 е представена структурната схема на предлаганата многоагентна система.



Фигура 4: Структура на предлаганата многоагентна система.

Нека да разгледаме по-подробно отделните съставящи елементи на предлаганата система, които са илюстрирани на фигура 4.

Локален оперативен Агент (ЛОА) – локалният оперативен агент е пряко натоварен с осъществяването на защитата на единичното локално устройство или локално базаиран информационен масив. Локалният оперативен агент е такъв тип агент, който притежава модална структура, която му позволява изпълняването на широк комплекс от задачи изразяващи се в наблюдение и контрол на обработваната локално информация, наблюдение и контрол на входящите и изходящи информационни пакети, мониторинг и контрол на дейноста на потребителя, а когато говорим за терминално устройство, което се използва от повече от един потребители по определен протокол, контрол и регистрация на тяхната дейност. Локалният оперативен агент е директно свързан с базата данни съхраняваща информация за налични вирусни сигнатури, характеристики на атаки и подробна информация за съществуващи и възможни кибер заплахи и атаки. Локалният оперативен агент има за задача в процеса на осигуряване на защитата да извършва динамична оценка на защитеността на устройството или масива, за който отговаря като въпросната оценка се състои в периодично „преслушване“ за уязвимости или наличие на заплахи. Локалният оперативен агент е натоварен и с още една много важна задача, а именно защита на наличните локални информационни ресурси. В своя процес на работа агента извършва анализ на наличните локално базирани ресурси и генерира докладно съобщение до системно интерфейсният агент, който да информира администратора за информационният риск касаещ конкретното локално устройство. Когато информационният риск бъде оценен се инициира процедура по криптографска защита на наличните локални информационни масиви, посредством алгоритъм изгенериран от криптографската система.

Ръководещ агент на група от ЛОА – за начало да започнем с дефиницията на групата от локални оперативни агенти (ЛОА). Една група от локални оперативни агенти може да бъде съставена в диапазона от минимум 5 до 10 локални оперативни агента. Поставяме това ограничение поради това, че обезпечаването с ръководещ агент на група съставена от по-малко от 5 агента е

технически необосновано, а обезпечаването на група от повече от 10 агента е трудно реализируемо от техническа гледна точка и изискващо наличието на сериозен изчислителен ресурс, сложна софтуерна система за обезпчаване на диспечирането на тази бройка локални агенти и увеличаването на вероятността за възникване на уязвимост в системата поради някой от предходно споменатите фактори. Ръководещият агент има за цел дефиниране на задачи към локалните административни агенти, контрол на тяхното състояние изразяващ се в мониторинг на дейността им и периодично тестване на същите посредством генериране на фалшив информационен пакет, който да тества реакцията на локалния агент. В случай, че локален агент пропусне фалшив информационен пакет или отговори с пакет, които е нетипичен за системата на ръководещия агент, ръководещият агент вдига флаг, за наличие на компрометиран агент в системата и предприема процедура по неговото незабавно изключване от нея. Една много интересна особеност на ръководещият агент се състой в това, че същият след изключването на локалния агент поради компрометиране продължава да следи неговото състояние и мерките, които се предприемат по неговото възстановяване. След като възстановяването е преминало локалния агент изпраща инициализиращ пакет към ръководещия агент, който стартира проверка за състоянието на агента, която проверка е отново свързана с фалшив пакет данни. Ако локалния агент отхвърли пакета данни и върне флаг към ръководителя за неоторизиран пакет, това означава, че агентът е вече напълно работоспособен и може да бъде върнат обратно в системата.

Системно интерфейсен агент – системно интерфейсният агент отговаря за осъществяването на връзката на администратора на защитаваната система с многоагентната система за киберсигурност. Системно интерфейсният агент спомага за осигуряване на мониторинг в реално време на всички случващи се процеси в системата на всяко едно ниво. Този агент може да се възприеме, че има Master-функция, тъй като определя целите, които се поставят към ръководителите на групи от локални оперативни агенти и локалните оперативни агенти. Тази способност се обуславя от възможността агента да събира динамична информация от ръководещите и локалните агенти, която бива обработвана, записвана в базата данни и при необходимост извличана от там. Тази информация служи за дефиниране в реално време на правила, политики и процедури за защита, които да се прилагат не комплекно за цялата система, а конкретно за всяка една група от локални агенти или при необходимост от локален агент.

База данни – базата данни съдържа информация за широк спектър от заплахи, вируси, атаки, характеристики на атаки и други. Допълнително базата данни съдържа информация за всеки един локален оперативен агент (ID на агента, статус и история), информация за ръководещите агенти и информация за прилаганите защитни политики (класификация посредством степенуване от 1 до 10, посредством, която се определя и типа на използван криптографски алгоритъм).

Система за защита на комуникацията – системата за защита на комуникацията има за цел обезпечаване на защитена комуникация между отделните агенти съставляващи многоагентната система, която да намали в максимална степен възможността за осъществяване на успешен опит за атака върху многоагентната система, посредством прихващане на информационен пакет данни трансфериран между комуникиращи си агенти. Системата за защита на комуникацията извършва криптиране на комуникацията между отделните агенти посредством криптографски алгоритъм, който позволява на отделните агенти да инициират защитени комуникационни сесии един с друг и съответно да ги осъществяват успешно. Друга допълнителна функция на системата е да следи

за това от кой локален агент, какъв информационен индекс бива подаван по линия на категоризация на информацията, която трябва да бъде защитена на локално ниво.

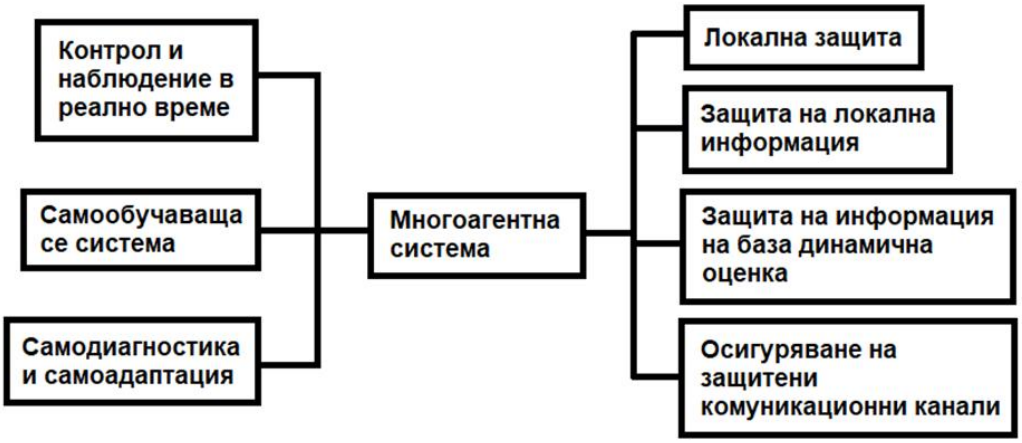
Криптографска система – криптографската система е ангажирана с прилагането на конкретни криптографски алгоритми в зависимост от изискванията, които са подадени към системата за защита на комуникацията. След като системата за защита на комуникацията получи изискването за вида и устойчивостта на необходимия криптографски алгоритъм, тя предава изискванията към криптографската система, която от своя страна спуска такъв към системата за защита.

След като разгледахме накратко съставните елементи на системата нека да разгледаме по-подробно как тя функционира и какви са нейните предимства и недостатъци.

Функциониране на многоагентната система

Настоящата многоагентна система, която разглеждаме е способна да функционира комбинирайки методики на работа от трите типа системи, които споменахме в началото на т.4. Сама по себе си системата включва елемент на стохастична многоагентна система, двуслойна многоагентна система и многоагентна система, която се базира на оценъчен принцип. Комбнацията от всичко това със система за защита на комуникацията и съхраняваната информация предразполага към представянето на един нов тип многоагентна система, която до голяма степен решава проблемите налични при предходно споменатите системи. На фигура 5 е представена схема на функционалността на многоагентната система.

Както вече споменахме, системата позволява локална защита на всеки един елемент от защитаваната система. Тази защита се изразява както в защита от атаки и неутрализиране на потенциални заплахи, така и посредством прилагането на криптографски способи за защита на локалната информация. И трите типа многоагентни системи (двуслойна, на база модулно-базирани агенти и със стохастичен характер) не предлагат защита на локалната информация, пропуск, който в случай на рансъмуеър атака може да излезе много скъпо на атакуваната организация или страна.



Фигура:5 Функционалност на предлаганата многоагентна система

Допълнителни отличаващи функционалността на настоящото предложение характеристики са защитата на информацията на база динамична оценка и осигуряването на защитени комуникационни канали. Защитата на информацията на база динамична оценка се осъществява посредством задаването на функция на локалния оперативен агент да прави обхождане на локално разположената информация и на база критерии спуснати от по-висшестоящите агенти да дава предложение за категория на наличната информация, на база която ще се прилага защитен алгоритъм.

Другият вариант на функциониране се състои в това локалният оперативен агент да предоставя информация през ръководещият агент към системно интерфейсният агент, като съответно защитните правила и алгоритми да се дефинират ръчно от администратора на системата. Това решение съдържа в себе си едно предимство, състоящо се в това администратора на системата да извършва групиране на локалните оперативни агенти на база категория на защитаваната информация. Малко по-подробно, тези агенти, които отговарят за защитата на устройства съхраняващи и обработващи информация, която е с категория 5 (средно ниво) ще бъдат групирани и подчинени на един ръководещ агент, тези агенти, които са натоварени със защитата на устройства с локално налична информация с категория 8 (висока степен на защита) пък ще бъдат подчинени на друг ръководещ агент и така докато бъде пълноценно обхванатата цялата защитавана система. Използването на този подход на първо място гарантира по-добра защита на информацията в защитаваната система, по-лесно администриране на защитните процедури и не на последно място индивидуалност, изразяваща се в използването на индивидуален защитен подход спрямо различните категории информация.

Осигуряването на защитени комуникационни канали за връзка между агентите е още една много специфична функционалност на предлаганата многоагентна система. Защитената комуникация се осъществява посредством процес на идентификация между участващите агенти и осигуряване на защита на обменяната информация с помощта на системата за защита на комуникацията и криптографската система. Когато се стартира процес на комуникация първоначално агентите, които ще комуникират обменят един с друг идентификационни кодове. Тези идентификационни кодове служат за проследяване на минала във времето комуникация между отделните агенти и идентификация на увреден агент, в случай на пробив, който е останал прикрит във времето. Идентификационният код има структурата представена на фигура 6.

Фигура 6: Структура на идентификационния код при комуникация

ID-то на агента в нашият теоретичен случай представлява код състоящ се от 1 до 6 цифри, които могат да бъдат всяка цифра от 1 до 9, включително 0 (в зависимост от приложението), който код е уникален и се отнася само за този конкретен агент и никой друг. Кода за защита отново е цифра от 1 до 9, която дефинира агента от коя категория на защита е; с упоменаването на този код системата за защита на комуникацията определя алгоритъма, с който ще бъде защитавана комуникационната сесия. Друга характерна особеност за разглеждания код е времевият маркер (ддммггччммсс – дата, месец, година, час, минута, секунда). Времевият маркер указва в кой ден, в колко часа между кой и кой агент е протекла комуникация. Наличието на този идентификатор отбелязва началото на сесията за комуникация. Кода на сесията има по-скоро функция на ID на

сесията, по което тя да бъде регистрирана в базата данни. ID-то на целевият агент служи за оказване с кой точно агент се желае осъществяване на комуникация. Ако липсва ID на целевия агент не е възможно да се стартира комуникация. След като бъде осъществена връзката с целевия агент се извършва бърза обмяна на синхронизиращи пакети, която цели да удостовери, че връзката е осъществена успешно и агентите могат да започнат да комуникират един с други.

Когато агентите са обменили един с друг необходимата информация, се пристъпва към генерирането на код за край на връзката, който има същата структура като представената на фигура 6 с тази разлика, че след ID-то на целевия агент се поставя индекс, който да маркира края на комуникационната сесия. Когато този индекс бъде отчетен от целевия агент, комуникацията се прекъсва дотогава докато не бъде инициирана нова такава.

Самодиагностиката и самоадаптацията при коментираната система са характеристики, които допълнително намаляват необходимостта от администриране, обслужване и конфигуриране на системата. Самодиагностиката се съдържа във функционалността на отделните ръководещи агенти, която вече разгледахме по-рано, а самоадаптацията спомага за по-добрата мащабируемост на системата и намаляване на необходимостта от съпътстващи промени в процесите на „*разширяване*“ или „*свиване*“ на защитаваната система.

Нека да отделим и необходимото внимание на възможността системата да се самообучава. Самообучението на системата в процеса й на функциониране създава възможността за генериране на широкообхватна база данни от заплахи, сигнатури, вирусни характеристики и данни за възможни заплахи и атаки. При своето първоначално „стартиране“ системата има въведена предварително подготвена база данни с информация за заплахи и атаки, която се обогатява в процеса на функциониране на системата. Нещо повече, съществува възможност към системата да бъде прикачен агентно-базиран модул, който да изпълнява ролята на “honeypot” и в реално време, независимо от процесите случващи се в многоагентната система да събира и обработва данни за налични в интернет пространството заплахи. Идеята на тази опция е създаването на възможност за генериране на информация за заплахи в реално време, която информация да бъде своевременно използвана в процесите по защита.

Накрая ще отделим внимание на възможността за контрол и наблюдение върху системата в реално време. Тази възможност има по-скоро административен характер, тъй като позволява на лицето, което администрира многоагентната система да наблюдава в реално време статуса на защитаваните обекти и масиви. Допълнително администратора на системата е способен да осъществява и мониторинг върху комуникацията и взаимодействието на съставящите системата агенти. Още една важна способност тук е възможността за осъществяване на диагностика и настройка на многоагентната система на ръка, което може да бъде прилагано в случай на необходимост от страна на администратора.

Предимства и недостатъци на предложената система

Нека за начало да започнем с предимствата на представяната система. Предимствата, които системата има се състоят на първо място във възможността за използване на диференциран подход за защита на информацията, информационните масиви и инфраструктурата. По-рано в настоящата глава споменахме развитието и опасността произлизаща от рансъмуера (по известен като криптовирус) и неговите негативни последици. Точно тук ще отбележим много

същественото предимство на предлаганата система, а именно в случай, че атакуващата страна предприеме някаква форма на криптоатака с предварително извличане и анализ на данните, атакуващата страна няма да разполага практически с нищо (т.е. ще разполага с „информационен отпадък“) поради това, че информацията, която цели да придобие ще бъде криптирана и атакуващата страна няма да може да се възползва от нея. Другото много съществено предимство е намаляването на възможността за осъществяване на т.нар. атаки от вътрешен човек. Възможноста е намалена благодарение на подробните идентификационни процедури, които биват осъществявани в процеса на функциониране на системата, автономността на системата за защита на комуникациите и възможността за контрол и наблюдение в реално време. Най-явното предимство на предлаганата система е защитеността на междуагентната комуникация. Тази защита намалява значително възможността за осъществяване на атака върху многоагентната система и също така повишава защитеността на работата на отделните агенти, което спомага за предоставянето на по-добра защита на защитаваната система. Като минус на настоящата система можем да посочим наличието на известно забавяне породено от наличието на йерархичност в системата и наличието на множество процедури между отделните елементи на системата. Още един признак, който може да бъде счетен като недостатък, е сложността на изграждане на такъв тип система, тъй като тук се налага прецизното проектиране и разработване на база данни, проектиране и разработване на система за защита на комуникациите и криптографска система, която да бъде обезпечена със съответен набор криптографски алгоритми и съответно самата многоагентна система. Някои от недостатъците, като времезакъснението и съпътстващите системи могат да бъдат лесно преодолени посредством много внимателно и детайлно планиране и също така внимателен подбор на използваните инструменти и средства за софтуерна разработка.

Заключение

Многоагентните системи със сигурност имат своето заслужено място в сферата на киберсигурността от гледна точка на техническите възможности, които предоставят. Самото направление е перспективно от научно-техническа гледна точка, тъй като предразполага към значително по своите мащаби творчество и научно-изследователска работа. Оставаме с ясното съзнание, че връзката на многоагентните системи и киберсигурността много трудно може да бъде обобщена в кратък по своя обем изложение, но паралелно с това се оставя вратата за последващи разглеждания в това направление. Като полезен ход за съвременните обществени и държавни администрации би могло да се счете предприемането на стъпки по дефинирането на критерии и изисквания, които да спомогнат по-лесното изграждане и внедряване на интелигентни многоагентни системи за киберсигурност, тъй като днес повече от когато и да е било е налице нуждата от комплексни решения, решаващи широк кръг проблеми на съвременното информационно общество.

References

1. Бошнаков, К., Лекция по Многоагентни системи, Институт по Информационни технологии при БАН, София, 2010

2. Трифонов, Р., Наков, О., Вачков, П., Манолов, С., Йошинов, Р., Попов, Г., Цочев, Г., Павлова, Г., Интелигентни методи и киберсигурност, XXV Конференция Telecom 2017, София, стр. 113-120;

3. Bendovschi, A., Cyber-Attacks-Trends, Patterns and Security Countermeasures, Procedia Economics and Finance, vol.28, 2015, p.24-31;

4. Baig, Z.A., Multi-agent systems for protecting critical infrastructures: A survey, Journal of Network and Computer Applications, vol. 35, 2012, p.1151-1161;

5. Boudaoud, K., Guessoum, Z., A Multi-agents System for Network Security Management, Proceedings of International Conference SMARTNET 2000, Austria, 2000, p. 407-418;

6. Gorodetski, V., Kotenko, I., The multi-agent systems for computer network security assurance: frameworks and case studies, Proceedings ICAIS 2002, Russia, 2002, p. 297-302

7. Hedin, Y., Moradian, E., Security in Multi-Agnet Systems, Procedia Computer Science, vol. 60, 2015, p. 1604-1612;

8. Such, J., Criado, N., Vercouter, L., Rehak, M., Intelligent Cybersecurity Agents, Intelligent Systems, IEEE, 2016, vol. 31, issue 5, p.3-7;

9. Xie, J., Chen-Ching, L., Multi-agent systems and their applications, Journal of International Council on Electrical Engineering, vol.7, issue 1, 2017, p. 188-197;

10. Pirttoja, T., Halme, A., Pakonen, A., Seilonen, I., Koskinen, K., Multi-Agent System Enhanced Supervision of Process Automation, IEEE Xplore, Conference DIS 2006, 2006, p. 151-156

11. Pataky, M., Gruska, D., Multi-agent heterogeneous intrusion detection system, CEUR Workshop Proceedings, 2014, p. 184-195;

12. Talib, A., Atan, R., Abdullah, R., Murad, M.A., Security Framework of Cloud Data Storage Based on Multi Agent System Architecture: Semantic Literature Review, Computer and Information Science, vol. 3, issue 4, 2010, p. 175-186;

13. Singh, M., Cybersecurity as an Application Domain for Multiagent Systems, Proceedings of the 14th International Conference AA-MAS 2015, 2015, Istanbul, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.721.2332&rep=rep1&type=pdf

14. Bandini, S., Manzoni, S., Vizzari, G., Agent Based Modeling and Simulation: An Informatics Perspective, Journal of Artificial Sociaties and Social Simulation, 2009, vol. 12, issue 4, http://jasss.soc.surrey.ac.uk/12/4/4.html;