Годишник Телекомуникации 2024, том 11 с. 131-141

Yearbook Telecommunications 2024, vol. 11, p. 131-141

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.13

АНАЛИЗ НА СИГУРНОСТТА В КОМУНИКАЦИОННИ МРЕЖИ ЗА ИНТЕРНЕТ НА НЕЩАТА

Красен Ангелов

SECURITY ANALYSIS IN COMMUNICATION NETWORKS FOR THE INTERNET OF THINGS

Krasen Angelov

Резюме: Това проучване има за цел да анализира предизвикателствата, свързани с управлението на огромното количество данни, генерирани от устройствата на Интернет на нещата (IoT), да оцени риса и да категоризира заплахите за сигурността в мрежите за IoT и да предложи съответни контрамерки за повишаване на сигурността. С увеличаването на броя на свързаните устройства се увеличават и свързаните с тях рискове за сигурността, което подчертава необходимостта от квалифицирани заинтересовани страни за смекчаване на тези рискове и предотвратяване на потенциални атаки. Предложената категоризация предоставя ценна информация за разнообразните роли и отговорности на заинтересованите страни в екосистемите на IoT, позволявайки по-добро разбиране на техните взаимовръзки. Тази категоризация улеснява по-ефективното вземане на решения, като отчита специфичния контекст и отговорности на всяка група заинтересовани страни. Този подход подобрява процеса на вземане на решения в областта на управлението на сигурността на IoT. Това би позволило разработката на ефективни стратегии за справяне с променящите се предизвикателства пред сигурността на мрежите за IoT.
Ключови думи: Интернет на нещата, заплахи за киберсигурността, оценка на риска, стратегия за киберсигурност

Abstract: The objective of this study is threefold: firstly, to analyze the challenges associated with managing the vast amount of data generated by Internet of Things (IoT) devices; secondly, to assess the nature and categorize security threats in IoT networks; and thirdly, to propose corresponding countermeasures to enhance security. As the number of connected devices increases, so do the associated security risks. This highlights the need for qualified stakeholders to mitigate these risks and prevent potential attacks. The proposed categorization provides valuable insights into the multifaceted roles and responsibilities of stakeholders in IoT ecosystems, facilitating a more nuanced understanding of their interrelationships. This categorization facilitates more effective decision-making by taking into account the specific context and responsibilities of each stakeholder group. This approach has been demonstrated to enhance the decision-making process in the domain of IoT security management. This would facilitate the development of effective strategies to address the evolving security challenges of IoT networks.
Keywords: Internet of Things, cybersecurity threats, risk assessment, cybersecurity strategy

1. ВЪВЕДЕНИЕ

Интернет на нещата (IoT) претърпя бърз растеж и е все по-широко разпространен в различни области, включително здравеопазване, транспорт, производство и интелигентни домове. Това разширяване подчертава спешната необходимост от справяне с предизвикателствата пред сигурността, свързани с управлението на голямото количество данни, генерирани от IoT устройства [1]. С увеличаването на броя на свързаните устройства се увеличават и рисковете за сигурността. IoT устройствата често имат уязвимости, които могат да бъдат използвани от злонамерени лица, което води до нарушения на поверителността, изтичане на данни, подправяне на устройства или дори

физически повреди. Разследването и справянето с тези рискове за сигурността е от решаващо значение за защитата на целостта, поверителността и наличността на IoT системите [2]. Разбирането на ролите, отговорностите и взаимозависимостите на тези заинтересовани страни е от съществено значение за ефективното вземане на решения, разпределението на ресурсите и стратегиите за смекчаване на риска. Фокусът на тази статия върху категоризацията на заплахите и на заинтересованите страни допринася за подобряване на разбирането на динамиката на заинтересованите страни в управлението на сигурността на IoT.

Управлението на сигурността на IoT и категоризирането на заинтересованите страни се сблъсква с няколко пречки [3, 4], включително предизвикателства, свързани с мащабируемостта, проблеми с хетерогенността и оперативната съвместимост, проблеми с поверителността и защитата на данните, пропуски в сътрудничеството и комуникацията, адаптивност към динамични IoT среди и оптимизиране на мерките за сигурност за IoT устройства с ограничени ресурси. За да се преодолеят тези предизвикателства, е от съществено значение да се ангажират мултидисциплинарни изследователски усилия и да се постигне напредък в протоколите за сигурност и технологиите за подобряване на поверителността, стандартизацията, рамките за сътрудничество и техниките за управление на ресурсите [3,5]. Чрез ефективно справяне с тези пречки, областта на сигурността на IoT и управлението на заинтересованите страни може да постигне значителен напредък в постигането на сигурни и устойчиви внедрявания на IoT.

2. АНАЛИЗ НА ЗАПЛАХИТЕ В IOT МРЕЖИТЕ

Интернет на нещата (IoT) е бързо развиваща се технология с потенциал да трансформира множество аспекти от нашето ежедневие. IoT устройствата са оборудвани със сензори и комуникационни възможности, което им позволява да събират и предават данни през интернет. Тези устройства са полезни в редица приложения, включително интелигентни жилища, индустриална автоматизация и транспортни мрежи.

Нарастващата популярност и широкото използване на IoT устройства обаче доведоха и до нови предизвикателства пред сигурността. IoT устройствата често нямат подходящи мерки за сигурност, което ги прави уязвими за атаки. Тези атаки могат да варират от прости мрежови атаки до по-сложни, насочени към самите физически устройства [6]. Сигурността на IoT екосистемата е сложна и интердисциплинарна област, която съчетава киберсигурността с различни инженерни области, като машиностроенето и електротехниката. Тя надхвърля защитата на данни, сървъри, мрежова инфраструктура и информация. Тя включва и надзор и управление на физически системи, свързани чрез интернет, независимо дали по централизиран или разпределен начин.

2.1. Класификация и анализ на атаките в IoT мрежите

Различните категории атаки могат значително да повлияят на сигурността на IoT устройствата и информацията, която те събират и предават. От съществено значение е както организациите, така и отделните лица да имат познания за тези видове атаки и да прилагат подходящи мерки за защита срещу тях. Класификация на IoT атаките е показана на Фиг. 1.

- **Атаки срещу устройства в IoT**

Заплахите за сигурността, насочени към специфични устройства или типове устройства, експлоатират уязвимости в хардуера или софтуера на устройството, като потенциално причиняват вреда на самото устройство или на мрежата, към която е свързано. Тези атаки, специфични за устройството, включват експлоатиране на известни уязвимости в операционната система, фърмуера или хардуера на устройството, компрометиране на устройството чрез фишинг атаки или дори физическо манипулиране на устройството [7]. Тъй като броят на IoT устройствата продължава да расте, за

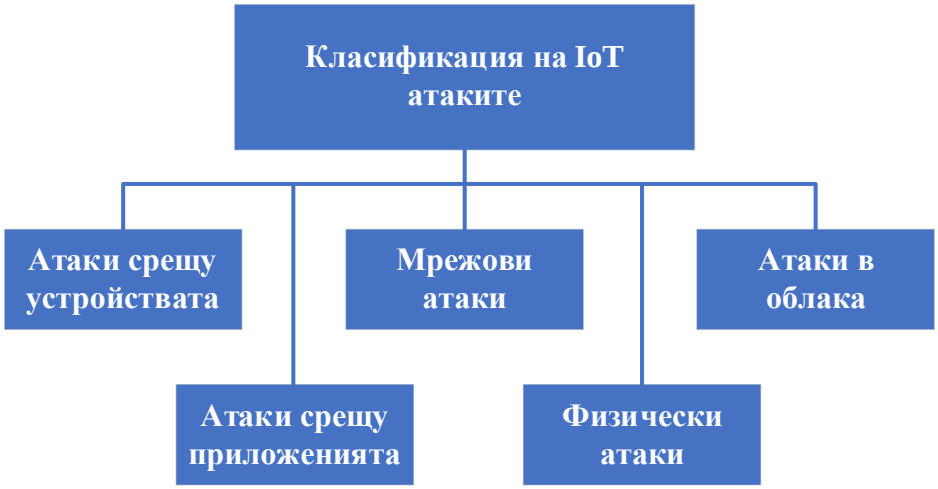
Годишник Телекомуникации 2024, том 11 с. 131-141

Yearbook Telecommunications 2024, vol. 11, p. 131-141

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.13

производителите е от решаващо значение да дадат приоритет на сигурността на устройствата, а потребителите също трябва да предприемат проактивни мерки за защита на своите устройства. Това може да включва актуализиране на софтуера, използване на силни пароли и повишено внимание при свързване с ненадеждни мрежи.



Фиг. 1. Класификация на IoT атаките на база техните характеристики

- **Атаки срещу приложения в IoT**

Заплахите за сигурността, насочени към приложенията и софтуера, работещи на IoT устройства, експлоатират уязвимости в приложенията, включително проблеми в кода или начина, по който приложението взаимодейства с други системи [7]. Примери за атаки срещу приложения в IoT включват междусайтово скриптиране [8], SQL инжектиране и атаки с препълване на буфера [9]. Тези атаки могат да компрометират сигурността на устройството и потенциално да предоставят на нападателите достъп до чувствителни данни или контрол върху устройството. За да се предотвратят атаки срещу приложения в IoT, е изключително важно разработчиците да се придържат към практики за сигурно кодиране, а потребителите трябва да гарантират, че устройствата им са актуализирани с най-новите корекции за сигурност и версии на софтуера. Освен това, използването на технологии за криптиране и удостоверяване може да помогне за защита от атаки срещу приложения в IoT.

- **Мрежови атаки в IoT**

Заплахите за сигурността, насочени към мрежовата инфраструктура, използвана от IoT устройства, експлоатират уязвимости в самата мрежа, потенциално компрометирайки сигурността и функционалността на свързаните устройства. Примери за мрежови атаки в IoT включват атаки „човек по средата“ [10], атаки за отказ на услуга (DoS) [11] и атаки с неоторизиран достъп. Тези атаки могат да позволят на нападателите да прихващат и манипулират данни, предавани по мрежата, или да нарушават мрежата, което влияе върху наличността и надеждността на свързаните устройства. За да предотвратят мрежови атаки в IoT, организациите трябва да внедрят практики за сигурно проектиране и внедряване на мрежи, като например използване на защитени протоколи, защитни стени и контрол на достъпа. Освен това, редовното наблюдение на мрежовата активност и своевременното справяне с всякакви инциденти, свързани със сигурността, може да помогне за смекчаване на риска от мрежови атаки в IoT.

- **Физически атаки в IoT**

Физическите атаки в контекста на IoT се отнасят до заплахи за сигурността, които включват физическа манипулация на устройство. Тези атаки могат да варират от просто манипулиране до по-сложни и злонамерени дейности, включително кражба или унищожаване на устройството [12]. Физическите атаки могат да бъдат особено вредни в критични инфраструктурни системи, използвани в сектори като здравеопазване, транспорт или производство на енергия. За да се предотвратят физически атаки, е изключително важно производителите да дадат приоритет на сигурността при проектирането на своите устройства, а потребителите да обезопасят устройствата си на физически недостъпни места за неупълномощени лица. Освен това, прилагането на мерки като сигурни корпуси, защитни пломби или биометрично удостоверяване може да помогне за смекчаване на риска от физически атаки.

- **Облачни атаки в IoT**

Заплахите за сигурността, насочени към облачната инфраструктура и услуги на IoT устройства, експлоатират уязвимости в облачната платформа, нейните приложения или комуникацията между облака и IoT устройствата. Примери за облачни атаки в IoT включват пробиви в облачните данни, неправилни конфигурации на сървъри и неоторизиран достъп до облачни ресурси [13]. Тези атаки могат да компрометират чувствителни данни, съхранявани в облака, да нарушат функционирането на свързани IoT устройства или да предоставят на нападателите неоторизиран достъп до облачни ресурси. За да предотвратят облачни атаки в IoT, организациите трябва да възприемат сигурни облачни внедрявания и практики за управление, като например внедряване на криптиране, контрол на достъпа и инструменти за мониторинг. Редовното актуализиране и актуализиране на облачни платформи и приложения също може да помогне за смекчаване на риска от облачни атаки в контекста на IoT.

2.2. Оценка на въздействието на атаките и контрамерки

Въздействието на атаките в областта на сигурността на интернет на нещата (IoT) може да бъде значително, което да доведе до различни последици, като финансови загуби, щети върху репутацията, физически щети и загуба на критична информация. Разбирането на тези въздействия е от решаващо значение за организациите и отделните лица, за да приоритизират мерките за сигурност и да смекчат рисковете, свързани с IoT атаките. Тук се разглежда въздействието на атаките в три специфични области: атаки по странични канали (Side-Channel Attack – SCA), пост-квантова криптография (Post-Quantum Cryptography – PQC) и усилия за стандартизация:

- **Атаки по странични канали (SCA)**

SCA представляват значителна заплаха за сигурността на IoT (Интернет на нещата), тъй като използват непреднамерени „течове“ по странични канали, за да извлекат чувствителна информация. Тези атаки могат да имат сериозни последици, включително неоторизирано разкриване на криптографски ключове и поверителни данни, като по този начин компрометират цялостната сигурност на IoT системите [14]. За да се смекчи въздействието на SCA, са разработени няколко контрамерки [15, 16], като техники за откриване и коригиране на грешки, механизми за излишък, практики за сигурно внедряване и техники за маскиране, които въвеждат случаен шум в траекториите на захранването или се съпротивляват на анализа на захранването.

Комбинацията от атаки с диференциален анализ на мощността (Differential Power Analysis – DPA) и диференциален анализ на грешки (Differential Fault Analysis – DFA) представлява значителна заплаха за криптографските реализации. Атаките, които използват непреднамерени течове по странични канали, като например консумация на енергия, електромагнитно излъчване или информация за времето, могат да извлекат чувствителна информация от криптографските реализации [14]. За да се смекчат

Годишник Телекомуникации 2024, том 11 с. 131-141

Yearbook Telecommunications 2024, vol. 11, p. 131-141

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.13

рисковете, свързани с тези комбинирани атаки, контрамерки като схеми за прагови реакции (Threshold Implementations – TI) и схеми за откриване на грешки са от решаващо значение. TI схемите осигуряват вградени функции за сигурност и устойчивост на несанкционирано отваряне на конструкции, докато схемите за откриване на грешки включват механизми за излишък и проверка на грешки [15]. Тези мерки повишават устойчивостта на криптографските системи и предпазват от компрометиране на чувствителна информация чрез анализ на грешки и мощност [14, 15]. Чрез прилагането на тези контрамерки, сигурността на криптографските реализации може да бъде ефективно подобрена срещу комбинирани DPA и DFA атаки.

FPGA (Field-Programmable Gate Arrays) системите играят ключова роля при внедряването на криптографски алгоритми за IoT устройства. Независимо от това, физическите характеристики на FPGA, като консумация на енергия, електромагнитно излъчване и информация за времето, могат неволно да изнесат информация за вътрешните операции и секретните ключове на внедрените алгоритми [17]. SCA, включително атаки за анализ на мощност и атаки за грешки, се възползват от тези течове, за да извлекат чувствителна информация от FPGA-базирани реализации. Атаките за анализ на мощност анализират моделите на консумация на енергия, за да изведат секретни ключове, докато атаките за грешки манипулират FPGA, за да индуцират грешки и да анализират произтичащите от това вариации в поведението [17]. За да се подобри сигурността на FPGA-базираните реализации срещу SCA, изследователите работят върху контрамерки, включително такива, насочени към пост-квантови криптографски алгоритми, като например Ring-Learning with Errors (Ring-LWEs) [18]. Тези контрамерки имат за цел да смекчат изтичанията по страничните канали и да защитят чувствителна информация, обработвана от FPGA. Освен това са разработени специфични техники за откриване на грешки за FPGA платформи, за да се открие и смекчи въздействието на грешки в криптографски алгоритми, като например Ring-LWEs [19].

- **Пост-квантова криптография (PQC)**

С възхода на квантовите изчисления нараства опасението, че традиционните криптографски алгоритми, като например криптографията с елиптични криви и Rivest-Shamir-Adleman, може да са уязвими за разбиване от квантови компютри [20]. Пост-квантовата криптография (PQC) има за цел да се справи с това предизвикателство, като предоставя криптографски алгоритми, които са устойчиви на атаки от квантови компютри. Приемането на PQC има последици за приложенията за сигурност в различни области, включително IoT. Въздействието на внедряването на PQC върху сигурността на IoT е двойно [20]. Първо, приемането на PQC алгоритми изисква значителни промени в криптографските протоколи и инфраструктура. Този преход може да въведе предизвикателства, като например повишени изисквания за изчислителни и сторидж ресурси за IoT устройства, което потенциално би могло да повлияе на тяхната производителност и ограничения на ресурсите. Второ, осигуряването на съвместимост между наследените IoT системи и PQC алгоритмите е от решаващо значение за осигуряване на безпроблемен преход без компромис със сигурността. В момента се полагат усилия за стандартизиране на PQC алгоритми и протоколи, целящи постигане на оперативна съвместимост и широко разпространение. Стандартизацията на PQC е от съществено значение за установяването на сигурна основа за бъдещи внедрявания на IoT, тъй като позволява разработването на стабилни криптографски системи, способни да издържат на атаки от квантови компютри.

В контекста на вградените системи, включително IoT устройства, е изключително важно да има специфични реализации на PQC алгоритми, оптимизирани за ARM Cortex M4 и Cortex-A процесори. Тези процесори се използват широко във вградените системи поради ниската си консумация на енергия и рентабилност [21].

Различни статии са фокусирани върху разработването и анализа на PQC реализации на ARM процесори, по-специално на Cortex-M4 и Cortex-A процесорите. Например, в [22] се обсъжда реализацията на алгоритмите Curve448 и Ed448 на процесора Cortex-M4. В [23] фокусът е върху реализацията на алгоритъма SIKE (Supersingular Isogeny Key Encapsulation) на процесора Cortex-M4, като последната версия е SIKE Round 3 [23]. А в [24] се изследва имплементацията на пост-квантовия криптографски алгоритъм Kyber върху 64-битови ARM Cortex-A процесори.

Техниките за откриване и диагностициране на грешки са от първостепенно значение за осигуряване на надеждността, целостта и сигурността на криптографските алгоритми, като шифъра на Pomaranch [25], хеша на Grostl [26], шифъра на Midori и RECTANGLE шифъра [27]. Тези техники играят жизненоважна роля в идентифицирането и смекчаването на грешки, които могат да компрометират функционалността и устойчивостта на криптографските системи. Чрез своевременно откриване и отстраняване на грешки, тези техники помагат за поддържане на ефективността и устойчивостта на криптографските алгоритми, като по този начин защитават чувствителна информация и осигуряват защита срещу потенциални атаки.

- **Усилия за стандартизация**

Стандартизацията играе ключова роля за подобряване на сигурността на IoT, като предоставя последователни рамки, протоколи и насоки за внедряване на сигурни системи. Целта на усилията за стандартизация е да се установят най-добри практики и да се насърчи оперативната съвместимост, като се позволи на различни IoT устройства, платформи и услуги да работят безпроблемно заедно, като същевременно се гарантира сигурността. Чрез дефиниране на общи изисквания за сигурност, протоколи и алгоритми за криптиране, усилията за стандартизация помагат за предотвратяване на уязвимости и осигуряват приемането на надеждни механизми за сигурност в IoT екосистемата [6]. Стандартизацията също така предоставя насоки за сигурна комуникация, удостоверяване, контрол на достъпа и защита на данните, като по този начин смекчава рисковете, свързани с IoT атаки.

NIST (Национален институт за стандарти и технологии) е федерална агенция на САЩ, отговорна за насърчаване и поддържане на стандарти в различни области, включително криптография. В областта на леката криптография NIST участва активно в процеса на стандартизация, за да идентифицира и популяризира криптографски алгоритми, подходящи за устройства с ограничени ресурси, като тези, използвани в IoT устройства и вградени системи. Усилията на NIST в областта на леката стандартизация целят да оценят и изберат криптографски алгоритми, които предлагат силна сигурност, като същевременно изискват минимални изчислителни ресурси [27]. Тези алгоритми са проектирани да отговарят на специфичните ограничения на устройствата с ограничени ресурси, включително ниска консумация на енергия, ограничена памет и възможности за обработка.

За да се справят с развиващите се технологии и предизвикателства в сигурността на интернет на нещата, усилията за стандартизация трябва да обхванат области като SCA и PQC, както и специфичните изисквания на вградени системи, като например внедрявания на ARM Cortex M4 и Cortex-A. Разработването и приемането на всеобхватни стандарти за сигурност, които обхващат тези аспекти, са от решаващо значение за установяването на солидна основа за сигурност за устройствата и системите на интернет на нещата. Чрез разбиране на въздействието на атаките в областите на SCA, PQC и стандартизацията, заинтересованите страни могат ефективно да разработят контрамерки и да гарантират

Годишник Телекомуникации 2024, том 11 с. 131-141

Yearbook Telecommunications 2024, vol. 11, p. 131-141

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.13

сигурността и устойчивостта на екосистемите на интернет на нещата. Това разбиране позволява проактивно подобряване на сигурността на системите на интернет на нещата, защита на чувствителна информация и смекчаване на рисковете, свързани с нововъзникващи заплахи.

Таблица 1 обобщава различните видове атаки в областта на киберсигурността и предоставя информация за тяхното въздействие и съответните контрамерки. Таблицата подчертава различните категории атаки, включително атаки срещу устройства, атаки срещу приложения, мрежови атаки, физически атаки, облачни атаки, SCA, атаки чрез DFA и DPA, и PQC атаки. За всяка категория атаки таблицата включва специфични типове атаки, потенциалното въздействие върху сигурността и препоръчителни контрамерки за смекчаване на рисковете.

Таблица 1. Обобщение на видовете атаки, въздействието и контрамерките в киберсигурността на IoT

Тип	Атака	Въздействие	Контрамерки
Атаки срещу устройства	Използване на уязвимости в хардуера или софтуера на устройството, фишинг атаки, физическо манипулиране	Повреда на устройство или мрежа, неоторизиран достъп, компрометиране на данни	Редовни актуализации на софтуера, силни пароли, предпазливи мрежови връзки
Атаки срещу приложения	Уязвимости в кода, междусайтово скриптиране, SQL инжектиране, атаки срещу препълване на буфера	Компрометирана сигурност на устройството, достъп/контрол на данните от страна на нападателите	Практики за сигурно кодиране, софтуерни корекции, криптиране, удостоверяване
Мрежови атаки	Атаки „човек по средата“, DoS атаки, атаки с неоторизиран достъп	Прихващане/манипулиране на данни, прекъсвания на мрежата, компрометирана функционалност на устройството	Проектиране на защитени мрежи, протоколи, защитни стени, контрол на достъпа, мониторинг
Физически атаки	Подправяне, кражба, унищожаване на устройства	Компрометиране на устройство, загуба на данни, прекъсване на критична инфраструктурна система	Сигурен дизайн на устройството, мерки за физическа сигурност, заграждения, удостоверяване
Облачни атаки	Пробиви в облачните данни, неправилни конфигурации на сървъри, неоторизиран достъп	Компрометиране на данни, прекъсвания на устройствата, неоторизиран достъп до облачни ресурси	Сигурно внедряване в облак, криптиране, контрол на достъпа, мониторинг, инсталиране на корекции

Атаки по странични канали (SCA)	Активни и пасивни SCA, атаки за повреди, атаки за анализ на мощността	Компрометиране на чувствителна информация, криптографски имплементации	Откриване/корекция на грешки, излишък, сигурно внедряване, техники за маскиране
DFA и DPA атаки	DFA и DPA атаки	Компрометиране на чувствителна информация чрез анализ на грешки или мощност	Контрамерки, специфични за DFA и DPA, като например защитени от несанкциониран достъп конструкции, откриване на грешки, сигурно внедряване
PQS атаки	Атаки, насочени към PQC алгоритми и имплементации	Компрометиране на криптирани данни, подкопаващо сигурността срещу квантови компютри	Разработване на PQC алгоритми, стандартизация, сигурно внедряване, съображения за съвместимост

Таблица 2 показва определянето на заинтересованите страни и дефинирането на техните роли.

Таблица 2. Класификация на заинтересованите страни и дефиниране на техните роли

№	**Заинтересована страна**	**Роля**
Г1	Инженер по сигурността на IoT	Актуализиране на системата за сигурност, откриване на заплахи и уязвимости, напр. тестване на системата за сигурност с цел да се проследи и подобри нейната производителност.
Г2	Специалист по сигурността на IoT	Откриване на потенциални атаки към IoT възлите в реално време, внедряване на системи за анализ на сигурността, защита при опасения за сигурността.
Г3	Анализатор на киберсигурността в IoT	Експерт по киберсигурност с фокус върху сигурността на мрежата и IoT инфраструктурата.
Г4	Директор/мениджър по сигурността на IoT	Изисква дълбоки познания относно инфраструктурата и софтуера. Поддържа и обучава екипът в центъра за операции по сигурността и наблюдава оперативните услуги, напр. проверка на наличието, интегритета и конфиденциалността между системите. Управление на риска в мрежата и системите като напр. прониквания в IoT мрежата
Г5	Анализатор на злонамерен софтуер в IoT	Изследване и разбиране на различни типове злонамерен софтуер и неговите механизми за разпространение, напр. анализ на поведението при DDoS атаки. Сканиране на отворени портове, използвани от IoT услугите, включително FTP, SSH и Telnet.
Г6	Консултант по сигурността на IoT	Създаване и разгръщане на най-ефективното решение за сигурност, напр. оценка на риска за IoT мрежата като отказ от Качество на обслужване (QoS) или атаки, целящи да изчерпят енергията на автономните сензори.

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.13

Г7	Анализатор на инциденти в областта на IoT	Анализиране на данните под формата на аларми и сортиране по степен на риск и значимост, напр. едновременно анализиране на DoS, DDoS, Keystroke logging атаки в IoT и присвояването им на ранк.
Г8	Реагиращ на инциденти в IoT	Отстраняване на уязвимости чрез тестване и прилагане на контрамерки по сигурността, напр. проверка на статуса на контрамерките по сигурността в IoT, например, на защитната стена след валидна заплаха и отчитане след това на статуса на проверката.
Г9	IoT одитор	Осигурява съответствието на мрежата с изискванията по закон чрез провеждане на систематична оценка на сигурността, напр. за недостатъчна защита на личните данни поради слабо криптиране или наличие на некриптирани пароли.

3. ЗАКЛЮЧЕНИЕ

В тази статия е представен обобщен анализ за подобряване на вземането на решения в областта на сигурността на IoT. Точното идентифициране и групиране на заинтересованите страни в сигурността на IoT позволява по-ефективно проучване на съответните характеристики и улеснява разделянето на данните въз основа на техните роли, като по този начин подобрява вземането на решения.

Чрез анализа на заплахите, заинтересованите страни и експертните знания са идентифицирани съответните характеристики, допринасящи за ефективното управление на сигурността на IoT устройствата. Това изследване не само групира заинтересованите страни, но и предоставя структурирана рамка за тяхното категоризиране, което позволява по-добро разбиране на различните отговорности и нива на участие на различните групи заинтересовани страни. Това осигурява вземането на по-информирани решения, ефективно разпределяне на ресурсите и прилагане на целенасочени мерки за сигурност за защита на IoT устройствата. Тези усилия ще допринесат за създаването на по-сигурна и надеждна среда за IoT, която насърчава иновациите и е от полза за обществото като цяло.

ИЗПОЛЗВАНИ ИЗТОЧНИЦИ (REFERENCES)

[1] YAO, X., F. FARHA, R. LI, I. PSYCHOULA, L. CHEN, H. NING. Security and privacy issues of physical objects in the IoT: Challenges and opportunities. In *Digital Communications and Networks*. Volume 7, Issue 3, 2021, pp. 373-384. ISSN 2352-8648. Available from: http://doi.org/10.1016/j.dcan.2020.09.001

[2] КЪДРЕВ, Васил, Росен ПАСАРЕЛСКИ. Особености на моделирането и симулацията на риска при комуникационни и осигурителни системи. *Годишник Телекомуникации* [онлайн]. 2020, (7), с. 17-28 [прегледан 07.02.2025]. eISSN 2534-854X. Достъпен на: https://doi.org/10.33919/YTelecomm.20.7.3 [KADREV, Vasil, Rosen PASARELSKI. Osobenosti na modeliraneto i simulatsiyata na riska pri komunikatsionni i osiguritelni sistemi. Godishnik Telekomunikatsii [onlayn]. 2020, (7), s. 17-28 [pregledan 07.02.2025]. eISSN 2534-854X. Dostapen na: https://doi.org/10.33919/YTelecomm.20.7.3]

[3] MOHANTA, B.K., D. JENA, U. SATAPATHY, S. PATNAIK. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. In *Internet Things.* Volume 11, 2020, 10022. ISSN 2542-6605. Available from: https://doi.org/10.1016/j.iot.2020.100227

[4] КЪДРЕВ, В., Росен ПАСАРЕЛСКИ Приложение на подходи на изкуствен интелект и машинно обучение в киберсигурността. *Годишник Телекомуникации* [онлайн]. 2021, (8), с. 53-64 [прегледан 08.02.2025]. eISSN 2534-854X. Достъпен на: https://doi.org/10.33919/YTelecomm.21.8.6 [KADREV, V., Rosen PASARELSKI Prilozhenie na podhodi na izkustven intelekt i mashinno obuchenie v kibersigurnostta. Godishnik

Telekomunikatsii [onlayn]. 2021, (8), s. 53-64 [pregledan 08.02.2025]. eISSN 2534-854X. Dostapen na: https://doi.org/10.33919/YTelecomm.21.8.6]
[5] KARIE, N.M., N.M. SAHRI, W. YANG, C. VALLI, V.R. KEBANDE. A review of security standards and frameworks for IoT-based smart environments. In *IEEE Access*, vol. 9, pp. 121975-121995, 2021. ISSN: 2169-3536. Available from: https://doi.org/10.1109/ACCESS.2021.3109886
[6] PAL, S., M. HITCHENS, T. RABEHAJA, S. MUKHOPADHYAY. Security requirements for the internet of things: A systematic approach. In *Sensors*. no 20. 2020. 5897. ISSN: 1424-8220. Available from: https://doi.org/10.3390/s20205897
[7] GAUR, V., R. KUMAR. Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices. In *Arabian Journal for Science and Engineering*. Volume 47, 2022. pp. 1353–1374. ISSN 2193-567X. Available from: https://doi.org/10.1007/s13369-021-05947-3
[8] CHAUDHARY, P. B.B. GUPTA, A. SINGH. Securing heterogeneous embedded devices against XSS attack in intelligent IoT system. In *Computers & Security*. Volume 118, 2022, 102710. ISSN 0167-4048. Available from: https://doi.org/10.1016/j.cose.2022.102710
[9] MULLEN, G., L. MEANY. Assessment of buffer overflow based attacks on an IoT operating system. In *Proceedings of the 2019 Global IoT Summit (GIoTS)*, Aarhus, Denmark, 2019; pp. 1–6. ISBN:978-1-7281-2171-0. Available from: https://doi.org/10.1109/GIOTS.2019.8766434
[10] TOUTSOP, O., P. HARVEY. K. KORNEGAY. Monitoring and detection time optimization of man in the middle attacks using machine learning. In *Proceedings of the 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, Washington DC, DC, USA, 2020. pp. 1–7. ISBN:978-1-7281-8243-8. Available from: https://doi.org/10.1109/AIPR50011.2020.9425304
[11] AL-HADHRAMI, Y., F.K. HUSSAIN. DDoS attacks in IoT networks: A comprehensive systematic literature review. In *World Wide Web*. Volume 24, pp. 971–1001. 2021. ISSN 1386-145X. Available from: https://doi.org/10.1007/s11280-020-00855-2
[12] YANG, X., L. SHU, Y. LIU, G.P. HANCKE, M.A. FERRAG, K. HUANG. Physical security and safety of iot equipment: A survey of recent advances and opportunities. In *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, 2022. pp. 4319-4330. ISSN: 1551-3203. Available from: https://doi.org/10.1109/TII.2022.3141408
[13] AHMAD, W., A. RASOOL, A.R. JAVED, T. BAKER, Z. JALIL. Cyber security in iot-based cloud computing: A comprehensive survey. In *Electronics*. 11(1), 16. 2022. ISSN: 2079-9292. Available from: https://doi.org/10.3390/electronics11010016
[14] DEVI, M., A. MAJUMDER. Side-channel attack in Internet of Things: A survey. In *Applications of Internet of Things: Proceedings of ICCCIOT 2020*. Springer: Berlin/Heidelberg, Germany, 2021; pp. 213–222. ISBN 978-981-15-6197-9. Available from: https://doi.org/10.1007/978-981-15-6198-6_20
[15] LO'AI, A.T., T.F. SOMANI. More secure Internet of Things using robust encryption algorithms against side channel attacks. In *Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Agadir, Morocco, 2016; pp. 1–6. ISBN:978-1-5090-4320-0. Available from: https://doi.org/10.1109/AICCSA.2016.7945813
[16] RAVI, P., R. POUSSIER, S. BHASIN, A. CHATTOPADHYAY. On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT: A Performance Evaluation Study over Kyber and Dilithium on the ARM Cortex-M4. In *Proceedings of the Security, Privacy, and Applied Cryptography Engineering: 10th International Conference, SPACE 2020*, Kolkata, India, 2020; pp. 123–146. Available from: https://eprint.iacr.org/2020/1038
[17] MAGYARI, A., Y. CHEN. Review of State-of-the-Art FPGA Applications in IoT Networks. In *Sensors* 2022. *22*(19), 7496. ISSN: 1424-8220. Available from: https://doi.org/10.3390/s22197496
[18] IMAÑA, J.L., P. HE, T. BAO, Y. TU, J. XIE. Efficient hardware arithmetic for inverted binary ring-lwe based post-quantum cryptography. In *EEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 8, 2022. pp. 3297-3307. ISSN: 1549-8328. Available from: https://doi.org/10.1109/TCSI.2022.3169471
[19] SARKER, A., M.M. KERMANI, R. AZARDERAKHSH. Fault detection architectures for inverted binary ring-LWE construction benchmarked on FPGA. In *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 4. 2021. pp. 1403-1407. ISSN: 1549-7747. Available from: https://doi.org/10.1109/TCSII.2020.3025857
[20] ZEYDAN, E., Y. TURK, B. AKSOY, S.B. OZTURK. Recent advances in post-quantum cryptography for networks: A survey. In *Proceedings of the 2022 Seventh International Conference On Mobile Furthermore, Secure Services (MobiSecServ)*, Gainesville, FL, USA, 2022; pp. 1–8. ISBN: 978-1-7281-8837-9. Available from: https://doi.org/10.1109/MobiSecServ50855.2022.9727214
[21] PARK, T., H. SEO, J. KIM, J., H. PARK, H. KIM. Efficient parallel implementation of matrix multiplication for Lattice-Based cryptography on modern ARM processor. In *Security and Communications Network*, 2018, 7012056. ISSN: 1939-0114. Available from: https://doi.org/10.1155/2018/7012056
[22] BISHEH NIASAR, M., R. AZARDERAKHSH, M.M. KERMANI. Efficient hardware implementations for elliptic curve cryptography over Curve448. In *Proceedings of the Progress in Cryptology—INDOCRYPT 2020: 21st International Conference on Cryptology in India*, Bangalore, India, 2020; vol 12578. Springer, Champ. 2020. p. 228–247. ISBN: 978-3-030-65276-0. Available from: https://doi.org/10.1007/978-3-030-65277-7_10

Годишник Телекомуникации 2024, том 11 с. 131-141

Yearbook Telecommunications 2024, vol. 11, p. 131-141

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.13

[23] ANASTASOVA, M., R. AZARDERAKHSH, M.M. KERMANI. Fast strategies for the implementation of SIKE round 3 on ARM Cortex-M4. In *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 10. 2021. pp. 4129-4141. ISSN: 1549-8328. Available from: https://doi.org/10.1109/TCSI.2021.3096916

[24] SANAL, P., E. KARAGOZ, H. SEO, R. AZARDERAKHSH, M. Mozaffari-Kermani. Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM Cortex-A processors. In *Proceedings of the Security and Privacy in Communication Networks: 17th EAI International Conference, SecureComm 2021*, 2021. pp. 424–440. ISBN: 978-3-030-90021-2. Available from: https://doi.org/10.1007/978-3-030-90022-9_23

[25] MOZAFFARI-KERMANI, M., R. AZARDERAKHSH, A. AGHAIE. Reliable and error detection architectures of Pomaranch for false-alarm-sensitive cryptographic applications. In *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 12. 2015. pp. 2804-2812. ISSN: 1063-8210. Available from: https://doi.org/10.1109/TVLSI.2014.2382715

[26] ABED, S., R. JAFFAL, B.J. MOHD, M. AL-SHAYEJI. An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices. In *Cluster Computing*. Volume 24, 2021. pp. 3065–3084. ISSN: 1573-754. Available from: https://doi.org/10.1007/s10586-021-03324-1

[27] THAKOR, V.A., M.A. RAZZAQUE, M.R. KHANDAKER. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. In *IEEE Access*, vol. 9, 2021. pp. 28177-28193. ISSN: 2169-3536. Available from: https://doi.org/10.1109/ACCESS.2021.3052867

[28] Пасарелски, Р., Теодора Пасарелска. Анализ, мониторинг и контрол на мрежовия трафик в интернет. Сборник с доклади на Национален военен университет "Васил Левски", гр. Велико Търново, 03-04 юли 2014г., том 9, стр 53-67, ISSN: 1314-1937, 2014

[29] Пасарелски, Р., Теодора Пасарелска. Виртуализация и сигурност в петото поколение 5G мобилни клетъчни мрежи, Сборник доклади от научна конференция „Знание, наука, технолоии, иновации" 2023, 6-7 юли 2023г., гр. Велико Търново, стр. 374-387, ISSN 2815-3480, 2023.

[30] СИМЕОНОВА, Цветелина. Развитие на перспективните технологии в „Интернет на свързаните неща" IoT (Internet of Things). София: Асеневци, 2021. ISBN 978-619-7586-25-1. [SIMEONOVA, Tsvetelina. Razvitie na perspektivnite tehnologii v „Internet na svarzanite neshta" IoT (Internet of Things). Sofia: Asenevtsi, 2021. ISBN 978-619-7586-25-1.]

Информация за автора:
доц. д-р инж. Красен Киров Ангелов, Технически университет – Габрово, Катедра „Комуникационна техника и технологии", ул. Х. Димитър № 4, Габрово, Тел.: 066 827 202, e-mail: kkangelov@tugab.bg

Contacts:
Assoc. Prof. Krasen Kirov Angelov, PhD, Technical University – Gabrovo, Department of Communications Equipment and Technologies, 4 H. Dimitar Str. Gabrovo. Tel.: 066 827 202, e-mail: kkangelov@tugab.bg

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 12.09.2024
Дата на приемане за публикуване (Date of adoption for publication): 30.09.2024