S E S 2 0 2 2
Eighteenth International Scientific Conference
SPACE, ECOLOGY, SAFETY
19 – 21 October 2022, Sofia, Bulgaria

ЗАПЛАХИ ПРЕД КИБЕРУСТОЙЧИВОСТТА НА САТЕЛИТНИЯ СЕКТОР

Димитър Димитров, Димитър Николов

ВВМУ 'Н. Й. Вапцаров'
e-mail: dimitar@gmx.us; d.nikolov@nvna.eu

Ключови думи: *сателитен сектор, кибер атаки, квантови атаки, етични хакери*

Резюме: *В статията е разгледано значението на сателитния сектор в съвременния свят, секторите, в които се използват, и ползите от тях. Представени са някои от слабостите в киберсигурността на спътниците и техните принципи на комуникация. Направен е преглед на някои от кибер атаките в този сектор и техните последици. Акцентирано е на заплахите от квантови атаки и техните възможности. Описани са специални събития, насочени към етичните хакери, с цел откриване на нови слабости и подобряване на киберустойчивостта на спътниковия сектор.*

THREATS TO THE CYBER RESILIENCE OF THE SATELLITE SECTOR

Dimitar Dimitrov, Dimitar Nikolov

Nikola Vaptsarov Naval Academy
e-mail:dimitar@gmx.us; d.nikolov@nvna.eu

Keywords: *satellite sector, cyber attacks, quantum attacks, ethical hackers*

Abstract: *The paper discusses the importance of the satellite sector in the modern world, the sectors in which they are used and their benefits. Some of the cybersecurity weaknesses of satellites and their communication principles are presented. Some of the cyber attacks in this sector and their consequences are reviewed. Threats from quantum attacks and their capabilities are highlighted. Special events targeting ethical hackers are described with the aim of identifying new vulnerabilities and improving the cyber resilience of the satellite sector.*

Сателитният сектор и хакерите

Само шест десетилетия след изстрелването на първия изкуствен спътник тази технология вече доминира като основен метод за комуникация, навигация и свързаност. Благодарение на спътниковия сектор човечеството осъществи свързаност, каквато никога досега не е имало. В началото на експедициите до Антарктида никой не е предполагал, че ще може да комуникира в реално време от една точка на света до друга. Днес това е възможно благодарение на спътниковата комуникация. Геостационарните спътници помагат на транспортната индустрия да се движи и да бъде толкова ефективна, колкото е сега. Милитаризацията на спътниците естествено е била една от основните цели при тяхното създаване. Днес те служат на всички разузнавателни служби с многофункционални задачи. При тази зависимост от тях обаче ние оставаме уязвими в тяхно отсъствие. Новите оръжия са пряко зависими от използването на спътници за насочване и локализиране. Ето защо спътниковият и космическият сектор са критични инфраструктури за нацията.

Както всяка критична инфраструктура, спътниковият и космическият сектор също представляват интерес за злонамерени хакери. Използването на подходящи тактически кибератаки може да обезсили защитните му реакции по време на военен конфликт. Пример за това е войната в Украйна. В координация с началото на войната в ранните часове на 24 февруари руска APT група извърши атака срещу интернет доставчика KA-SAT, част от Viasat. Нападението срещу сателита KA-SAT е наземно. Атаката е била осъществена със зловреден софтуер с кодово име AcidRain. Този зловреден софтуер се възползва от

неправилно конфигурирани мрежови устройства на доставчиците на интернет услуги. Това позволява да се презапише флаш паметта на модеми и маршрутизатори, така че те да станат неизползваеми. Засегнати са десетки хиляди устройства, а интернет свързаността в голяма част от страната е силно ограничена. Прекъсването на такъв важен метод за комуникация се отразява тежко както на населението, така и на военните части. В резултат на затрудненията на украинските военни да осъществяват надеждни комуникации, настъплението на руските военни сили набира скорост. Това доказва колко важна част от националната сигурност всъщност са сателитите. Става ясно, че в бъдещите военни операции държавите с развито информационно командване и разузнаване ще насочат настъпателната си тактика и към космическия и сателитния сектор.

Развитието на спонсорирани от държавата хакерски групи, лесният достъп до кибернетични оръжия и непроследимите криптовалути като средство за разплащане са само някои от причините за увеличаването на хакерските атаки на държавно ниво, инфраструктурата и високочувствителните агенции. Свързаността между злонамерените хакери предопределя високата им подготовка в областта на шпионажа, саботажа и офанзивните дейности.

Погледнато в глобален план, насочеността към сателитния и космическия сектор не е толкова висока, колкото към останалите, но е въпрос на време това да се промени. Експанзията на човека в космоса и неговата зависимост предразполагат към атаки, като например групи за изнудване. RaaS (Ransomware as a service) е генератор на стотици милиони долари годишно от жертвите на рансъмуер атаките. Тези атаки и методи имат за цел да криптират данните на жертвата, като за тях може да бъде поискан откуп, а за чувствителни организации той може да достигне няколко милиона. Тези цели се вписват добре в профила на бъдещите и някои от настоящите (Starlink, SpaceX) космически и сателитни сектори.

Квантовата комуникация – ползи и атаки

Квантовите комуникационни протоколи се считат за надежден начин за комуникация и пренос на данни. Това е така при условие, че всички входове в системата са напълно характеризирани и портовете (каналите за комуникация) са затворени. Въпреки това, компонентите на квантовата комуникация могат да бъдат променени. При третиране чрез лазерно лъчение могат да бъдат променени характеристиките на компонентите. Това води до уязвимости в квантовата комуникационна система. При такъв тип атака върху тези компоненти системата за разпределение на квантовите ключове (Quantum Key Distribution) биват компрометирани.

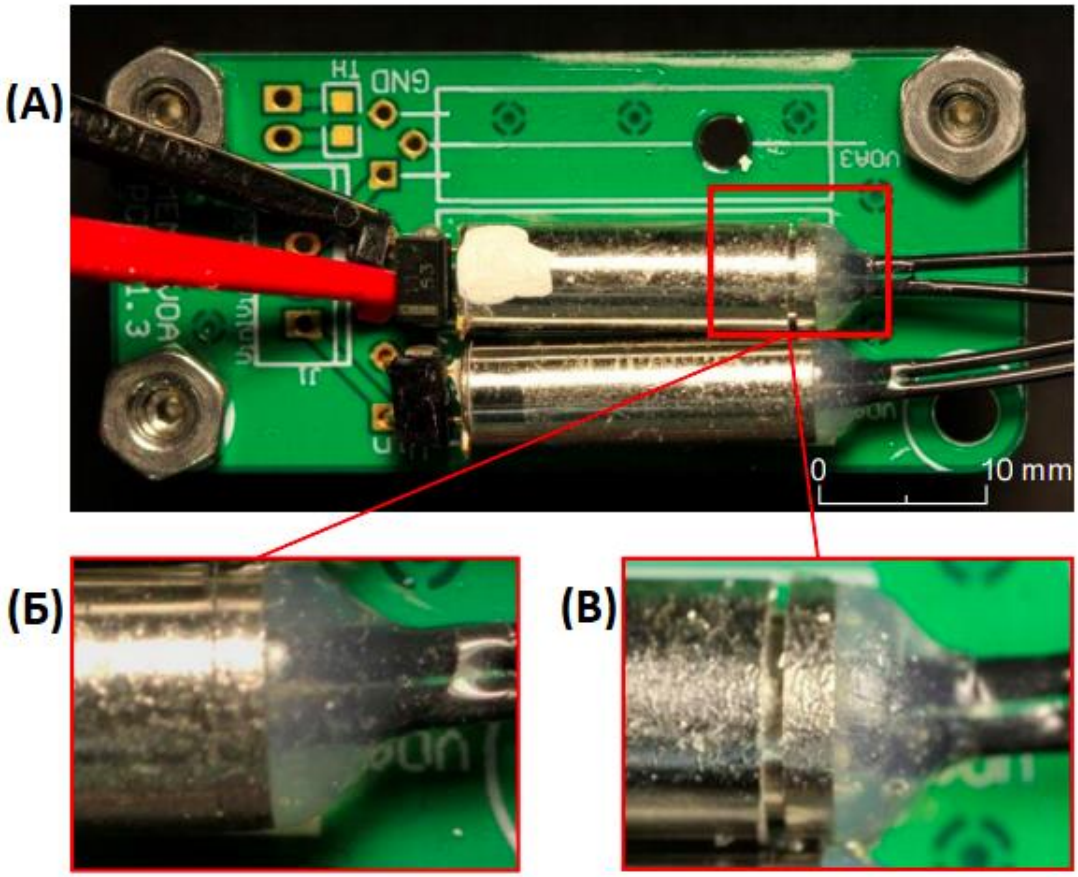
Целта на използването на QKD [1, 2] е да бъде премахната математическата част от уравненията за предаване и криптация на ключовете. Това се постига чрез използване на принципите на квантовата физика. Премахвайки „нормалните“ математически изчисления, премахваме и математическата бариера за разбиване. В следствие на това колкото и мощни компютри да бъдат използване за атака на грубата сила, резултатът няма да е положителен. Адаптирането към шум е друго положително качество на квантовата комуникация. Използвайки свойствата на квантовата механика, когато се пренася поток данни, и той попадне на някакъв шум, предизвикан от хакер или друг нарушител, ключовете се адаптират и променят. В резултат на това нападателите не могат да хакнат предаването, а неоторизирана страна няма да може да подслушва мрежата. Другият много важен плюс на квантовата криптография е, че ключа се изпраща под формата на фотони. Фотоните и светлината не могат да бъдат разбити или копирани.

Въпреки това, този метод крие рискове. Ако предаването на квантовите ключове не се изпълни по точно определен начин, те стават слаби към атаки чрез светлинно инжектиране [3]. При тези атаки към влакното на QKD се добавя допълнителна ярка светлина, която прониква вътрешността на защитените станции, за да отнесе битове от тайния ключ. Подобни слабости в предаването на квантовите ключове са в основата на редица атака. Такива атаки са атаките на фалшивите състояния, атаки с пренасочване на фазите и атаки с изместване на времето.

Атака тип DoS (Denial of Service) също е възможна. При тази атака се атакува стандартния път на обмен на ключовете с мощно лазерно излъчване, което може да варира между 316mW (25dBm) и 9W за период до 10 секунди. При успешно изпълнена атака се наблюдава промяна в затихване на усилвателя, което води до увреждане на устройството. На Фиг. 1. е демонстрирана такава атака.

На Фиг. 1 [4] се наблюдава физическото отделяне на капачката на усилвателя в резултат на атаката. Снимка (А) е общ изглед на елемента, фокус на атаката. Снимка (Б) е елемента преди атака. Снимка (В) е елемента след атака. Може да се забележи как капачката се е отделила и това предизвиква проблем във функционирането на усилвателния елемент. Атаката е предизвикала приблизително 26% увеличение на средния брой фотони в рамките на

квантовия канал при долната граница и спад с около 50% при горната. На този тип атаки, е базирано с голяма вероятност действието на руската лазерна система „Пересвет“, с чиято помощ наскоро бяха неутрализирани множество сателити Starlink.



Фиг. 1. DoS атака над усилвател на QKD[4]

Атаката се осъществява в следните стъпки:

1. OSINT и разузнаване за намиране на информация за производителя на компоненти на QKD за таргетирания сателит.
2. OSINT и разузнаване за намиране на образци от конкретния елемент и партида. Калибриране на лазерните установки за максимален ефект.
3. Установяване на орбитните елементи и траекторията на сателита. Изчисляване на времевите параметри за контакт.
4. Прихващане и атака над сателита в периода на достъп.
5. Внасяне на корекции за подобряване на ефективността.

Ролята на етичните хакери и правителствени проекти в подобряването на киберустойчивостта на сателитите

За щастие хакерите не са само злонамерени. Хакерите с добри намерения, известни още като "бели шапки", имат за цел да повишат киберустойчивостта на компаниите, институциите или, в този случай, на сателитния сектор. Те действат само с разрешение, което им позволява да тестват системите за слабости и ако открият такива, да разработят план за отстраняването им. Първите стъпки към осигуряване на киберсигурността в околоземна орбита се предприемат от военните структури на държавите. За Съединените щати това са Изследователската лаборатория на военновъздушните сили (AFRL), DARPA и Министерството на отбраната, а за Русия - MISiS. След навлизането на киберсигурността във все повече области и сектори обаче тенденцията за съсредоточаване само върху държавните структури за разработване на киберсигурност за спътниковия сектор се промени. AFRL, DARPA и

Министерството на отбраната, в комбинация с известните форуми Black Hat и DEFCON, създадоха първото състезание от типа " Завладяване на знамето". Това състезание е отворено за всички. Целите на състезанието са да се хакне специален симулатор от типа Flat-Sat или някакъв специално поставен в орбита сателит, собственост на Министерството на отбраната на САЩ, и да се анализират неговите слабости, точки на компрометиране и атаки. На този етап съществуват основно 4 големи западни състезания и проекти от този тип: Hack-A-Sat, CYSAT, Space-BACN и Blackjack.

Hack-A-Sat [5] е създаден основно от Изследователската лаборатория на Военновъздушните сили на САЩ, но в разработването на състезанието участват и други правителствени институции като DARPA, Космическите сили и МО на САЩ. За първи път то е представено през 2020 г. и оттогава е ежегодно събитие. Hack-A-Sat 1 се базира на Flat-Sat, като има непряко предизвикателство в орбита. Hack-A-Sat 2 надгражда събитието, като включва атака/защита на Flat-Sat с цифрови близнаци, които да имитират команди за всички състезатели. Hack-A-Sat 3 ще има за цел предварително тестване на Flat-Sat софтуер, базиран на USSF Moonlighter. Hack-A-Sat 4 през 2023 г. ще бъде състезание от типа " Завладяване на знамето", но с истински сателит. Moonlighter[6] е специално проектиран сателит, който се очаква да бъде изведен в орбита през 2023 г.

CYSAT [7] е европейският вариант на Hack-a-Sat, организиран от Европейската космическа агенция(ЕКА) и EUSPA и проведен за първи път през 2021 г. Това е конференция с три основни задачи. Първите два дни са свързани с теоретична част за киберсигурността на космическия сектор и нейното значение. Третата част има за цел да предизвика етични хакери да хакнат OPS-SAT. OPS-SAT е CubeSat, изстрелян през 2019 г., и е собственост на ЕКА.

Space-Based Adaptive Communications Node (Space-BACN) [8] е предназначен основно за създаване на евтин, преконфигурируем оптичен комуникационен терминал, който се адаптира към повечето стандарти за оптични междуспътникови връзки, превеждайки между различни спътникови съзвездия. Освен това проектът LEO на DARPA има за цел да изследва спътниковите комуникации и да създаде най-сигурния начин за комуникация на военните агенции.

Проектът BlackJack [9] на DARPA има за цел да разработи и демонстрира критичните елементи за глобална високоскоростна мрежа в ниска околоземна орбита (LEO), която да осигури на Министерството на отбраната високоскоростна връзка, постоянно и устойчиво покритие. Подобно на Space-BACN, BlackJack ще има за цел да проучи киберсигурността в космическия сектор и нейната устойчивост.

Заключение

Благодарение на сателитната комуникация човечеството постигна невиждана досега свързаност. Авиацията, транспортът, навигацията, отбраната и много други примери показват приложимостта на спътниковите комуникации и как те променят света завинаги. Тяхното разработване обаче е ограничено от начина, по който те се транспортират до LEO, MEO или GEO орбита. Тези ограничения принуждават производителите да наблягат повече на производителността, отколкото на сигурността. Ограничението на хардуерните части и трудността да се поддържа актуален софтуерът им, когато са в околоземна орбита, ги предразполага към кибератаки. Мащабна кибератака срещу спътници с критично значение за навигацията би парализирала цялата световна икономика и би имала необратими последици. При новите конфигурации на спътниците се обръща по-голямо внимание на криптирането на данните и сигурността, но ще са необходими десетилетия, за да се заменят несигурните спътникови съзвездия с по-сигурни.

Войната в Украйна също така показа колко важна роля изпълняват спътниците за защита на националната сигурност. Това ги прави критична инфраструктура. А критичната инфраструктура е една от първите цели на войната. Атаката срещу KA-SAT на Viasat доказа точно това. По време на военни действия сателитният сектор и неговите комуникационни услуги ще бъдат една от първите цели, които ще бъдат свалени. Новото поколение кибератаки, като например квантовите атаки, се превръщат в основно предизвикателство за киберзащитата на сателитния сектор.

Благодарение на етичните хакери и събитията, организирани от Министерството на отбраната на САЩ, ЕС и традиционната BlackHat конференция , се полагат основите на нови и иновативни начини за защита на сателитния сектор. Развитието на образованието и научните изследвания в този сектор е основна стъпка към по-сигурно бъдеще. Събирането на специалисти и съсредоточаването им върху актуалния проблем ще доведе до повишаване на киберустойчивостта на сектора и до разработването на препоръки и методики за защита на обикновените спътници.

Като част от националната сигурност и критичната инфраструктура, държавите и техните агенции трябва да се заемат с актуалните проблеми, свързани с киберустойчивостта, пред които са изправени космическият и сателитният сектор, за да се избегнат катастрофални последици.

Литература:

1. Ren, S., Y. Wang, X. Su. Hybrid quantum key distribution network. Sci. China Inf. Sci. 65, 200502 (2022). https://doi.org/10.1007/s11432-022-3509-6
2. NSA, Quantum Key Distribution (QKD) and Quantum Cryptography (QC), https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-
3. Garcia-Escartin, J., S. Sajeed , V. Makarov. Attacking quantum key distribution by light injection via ventilation openings. doi: 10.1371/journal.pone.0236630.
4. Huang, A., R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, V. Makarov. Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution., https://doi.org/10.1103/PhysRevApplied.13.034017
5. Air Force Research Laboratory Public Affairs, Hack-A-Sat, https://afresearchlab.com/technology/hack-a-sat/
6. Wolfe, F., US Space Force to Launch Project Moonlighter Cybersecurity Satellite, https://www.satellitetoday.com/cybersecurity/2021/12/16/us-space-force-to-launch-project-moonlighter-cybersecurity-satellite/
7. Quiquet, F., CYSAT ’22, a space cybersecurity conference in Paris, https://www.spacesecurity.info/en/cysat-22-a-space-cybersecurity-conference-in-paris-april-6-7th-2022/
8. Kuperman, G., Space-Based Adaptive Communications Node (Space-BACN), https://www.darpa.mil/program/space-based-adaptive-communications-node
9. Forbes, S., Blackjack. https://www.darpa.mil/program/blackjack