УДК 654.16

Сопубеков Нематилла Абдилахатович
техника илимдеринин кандидаты, доцент
Ош технологиялык университети
Сопубеков Нематилла Абдилахатович
техника илимдеринин кандидаты, доцент
Ош технологиялык университети
Sopubekov Nematilla Abdilakhatovich
candidate of technical sciences, associate professor
Osh Technological University
Самусев Илья Александрович, магистрант
Ошский технологический университет
Самусев Илья Александрович, магистрант
Ош технологиялык университети
Ilya Alexandrovich Samusev, graduate student
Osh Technological University

ИСПОЛЬЗОВАНИЕ НОВЫХ ТЕХНОЛОГИЙ В ОРГАНИЗАЦИИ БЕЗОПАСНОГО ПОТОКА ИНФОРМАЦИИ

Аннотация. Основная цель данного исследования — рассмотреть возможности основных технологий по обеспечению безопасности в современных открытых сетях. Предметом исследования являются протоколы VPN и SSL/TLS, использование этих технологий в сфере связи, их основные особенности, различия и преимущества, их расположение на сетевом уровне и их место в информационной безопасности. Методом сравнения возможностей этих технологий было проанализировано, что хотя эти технологии являются конкурирующими технологиями, они дополняют друг друга и расширяют существующие функциональные возможности. В результате, несмотря на то, что протоколы имеют разные свойства, была определена возможность решения различных задач и процессов на основе их совместного использования.

Ключевые слова: информация, информационная безопасность, технология, протокол, криптография, сеть, узел, процесс.

КООПСУЗ МААЛЫМАТ АГЫМЫН УЮШТУРУУДА ЖАҢЫ ТЕХНОЛОГИЯЛАРДЫ КОЛДОНУУ

Аннотация. Бул изилдөөнүн негизги максаты азыркы учурдагы ачык тармактарда коопсуздукту камсыз кылуу үчүн негизги технологиялардын мүмкүнчүлүктөрү карап чыгуу. Изилдөө предмети болуп VPN жана SSL/TLS протоколдору эсептелинет, бул технологиялардын байланыш тармагында колдонулушу, аларды колдонуудагы негизги өзгөчөлүктөрү, айырмачылыктары жана артыкчылыктары, тармак деңгээлинде жайгашуусу, маалымат коопсуздугундагы орду маанилүү орунга ээ. Бул технологиялардын мүмкүнчүлүктөрүн салыштыруу усулу аркылуу алар бири бирине атаандаш технология болсо да бири-бирин толуктап, колдонуудагы функционалдык мүмкүнчүлүктөрүн кеңейтүүгө шарт түзүлөөрү анализденди. Жыйынтыгында протоколдор ар кандай касиеттерге ээ болсо да аларды биргелешип колдонуунун негизинде ар кандай маселелерди жана процесстерди чечүү мүмкүнчүлүгү аныкталды.

Негизги сөздөр: маалымат, маалымат коопсуздугу, технология, протокол, криптография, тармак, түйүн, процесс.

USING NEW TECHNOLOGIES TO ORGANIZE A SECURE FLOW OF INFORMATION

Abstract. The main purpose of this study is to examine the capabilities of key technologies to provide security in modern open networks. The subject of the study is the VPN and SSL/TLS protocols, the use of these technologies in the field of communications, their main features, differences and advantages, their location at the network level and their place in information security. By comparing the capabilities of these technologies, it was analyzed that although these technologies are competing technologies, they complement each other and extend existing functionality. As a result, despite the fact that the protocols have different properties, the possibility of solving various problems and processes based on their joint use was determined.

Key words: information, information security, technology, protocol, cryptography, network, node, process.

Азыркы учурда заманбап коом бул маалыматтык коом болуп эсептелет. Себеби, маалыматтык технологиялар экономикага, социалдык чөйрөгө жана мамлекеттин, социалдык топтордун жана жеке адамдардын ишмердүүлүгүнүн башка тармактарына терең кирип, суроо-талапка ээ болуп калды. Мамлекеттик органдардын, ири, орто жана чакан бизнести башкаруу, банк, билим берүү жана саламаттыкты сактоо, ошондой эле өндүрүштүк, социалдык жана жеке турмуштун башка тармактары тарабынан ар кандай чечимдердин кабыл алынышы ири долбоорлорду кайра иштетүүнү талап кылат.

Ачык тармактарда коопсуз маалымат агымын уюштуруунун эң кеңири таралган жолдору виртуалдык жеке тармактарды (VPN) жайылтуу жана SSL/TLS протоколун колдонуу болуп саналат. Берилген маалыматтарды коргоону камсыз кылуу үчүн эки технологиянын тең өзгөчөлүктөрүн карап көрөлү.

Көптөгөн компаниялар шаардын, өлкөнүн, ал тургай, бүткүл дүйнөнүн ар кайсы аймактарында өздөрүнүн катышуусун кеңейтүүгө багытталган. Эгерде мурда борбордук аппаратты, алыскы филиалдарды жана түйүндөрдү бирдиктүү маалымат мейкиндигине бириктирүү үчүн компанияларга атайын бөлүнгөн байланыш линияларын тартып, көп каражат сарпталышы керек болсо, глобалдык тармактардын өнүгүшү менен абал өзгөрдү. Коомдук линияларды жана байланыш каражаттарын колдонууда берилүүчү маалыматка табигый коркунучтар, демек компаниянын өзүнө да коркунучтар келип чыгат. Бул коркунучтарды чечүү - өткөрүлүп берилген маалыматтарды коргоону камсыз кылуу.

Ачык тармактарда коопсуз маалымат агымын уюштуруунун көптөгөн жолдору бар. Биз көңүлүбүздү эң кеңири таралгандарына бурабыз: виртуалдык VPN жеке тармактарды жайылтуу жана SSL/TLS протоколун колдонуу. Бул технологиялар кээде бири-бирине түздөн-түз карама-каршы келет жана окшош маселелерди чечүү үчүн иштелип чыккан технологиялар катары каралат, бул биздин көз карашыбыз боюнча таптакыр туура эмес.

VPN жана SSL/TLS технологиялары

VPN – маалыматты коргоонун криптографиялык ыкмаларын колдонуу менен ишеним деңгээли төмөн ачык тармактын үстүндө ишенимдүү тармактарды жана түйүндөрдү бириктирген коопсуз виртуалдык тармакты уюштурууга мүмкүндүк берүүчү технологиялардын жыйындысы.

VPN протоколдорунун ар бири өзүнүн иштөө өзгөчөлүктөрүнө жана берилүүчү маалыматтардын коопсуздук даражасына ээ (мисалы, L2TP өз алдынча маалыматтарды коргоону камсыз кылбайт), бул алардын келип чыгыш тарыхы жана аларды түзүү максаттары менен аныкталат.

IPsec жана IPlir протоколдорун эң коопсуз, универсалдуу жана келечектүү деп эсептөөгө болот, ошондуктан VPN технологиясынын касиеттерин андан ары изилдөөдө биз аларга көбүрөөк көңүл бурабыз.

SSL/TLS – компьютер тармактары аркылуу криптографиялык жактан коопсуз байланыштарды уюштуруу үчүн иштелип чыккан протокол. SSL/TLS протоколдор үй-бүлөсүн өнүктүрүү үчүн баштапкы чекит Netscape тарабынан иштелип чыккан SSL 1.0 протоколу болуп саналат, бирок анда бир катар олуттуу коопсуздук көйгөйлөрүнүн болушунан улам эч качан жарык көргөн эмес. Үй-бүлөнүн биринчи версиясы 1995-жылы пайда болгон SSL 2.0 протоколу болуп саналат. Дээрлик ошол замат, кайрадан протоколдун экинчи версиясында болгон кемчиликтерден улам, ал кайра иштелип чыккан, анын натыйжасында 1996-жылы SSL 3.0 пайда болгон. Кийинки кадам протоколдун үчүнчү версиясын модернизациялоо жана анын атын Secure Sockets Layer-тен Транспорт Layer Security дегенге өзгөртүү болду. Ошентип, 1999-жылы TLS 1.0 протоколу жарыкка чыкты, ал кийинчерээк дагы эки жолу өзгөрүүгө дуушар болгон: 2006-жылы TLS 1.1 протоколу, 2008-жылы TLS 1.2 пайда болгон. Кийинчерек протоколдун башка жаңы версиялары иштелип чыкты.

Технологияларды салыштыруу

VPN жана SSL/TLS технологиялары, албетте, жалпы өзгөчөлүктөргө ээ, мисалы, алардын ар бири маалыматты коргоо үчүн криптографиялык ыкмаларды колдонот. Ошентсе да, алардын ортосунда бир катар принципиалдуу айырмачылыктар бар, алардын айрымдарын биз кененирээк карап чыгабыз.

Тармак моделинде жайгашуусу

Белгилей кетчү нерсе, бул технологиялар ISO/OSI тармактык маалымдама моделинин ар кандай катмарларына таандык. VPN протоколдору, адатта, маалымат шилтемеси же тармак катмарларына кирет, ал эми SSL/TLS транспорттук жана колдонмо катмарларынын ортосунда отурат (адатта презентация катмары катары классификацияланат). Бул көбүнчө технологиялардын мүмкүнчүлүктөрүн жана аларды колдонуу сценарийлерин аныктайт.

IPSec жана IPlir VPN протоколдору эки түйүн ортосундагы бардык трафикти коргойт, бул колдонуучуга ишенимдүү тармакка алыстан туташкан учурда, ал түздөн-түз ага киргендей, анын толук мүчөсү болууга мүмкүндүк берет.

SSL/TLS протоколу байланыш түйүндөрүндө иштеген тиркемелердин ортосунда коопсуз байланышты орнотуп, белгилүү бир тиркемеге алыстан коопсуз кирүүнү уюштуруу мүмкүнчүлүгүн ачат. Бул айырмачылык, биз төмөндө карап чыга тургандардын көбү сыяктуу эле, тигил же бул технологиянын пайдасына чечмелениши мүмкүн эмес. Ал белгилүү бир технологиянын белгилүү бир тапшырмага ылайыктуулугун баалоого гана мүмкүндүк берет. Мисалы, бардык трафикти коргоо керек болсо, VPN технологиясына артыкчылык берилиши керек, ал эми бир гана тиркемеге кирүү керек болсо, SSL/TLS колдонуу көбүрөөк мааниге ээ болушу мүмкүн. Ошол эле учурда, ар бир учур үчүн коопсуздукту бузуунун кесепеттери (бүт тармакка же бир эле тиркемеге жетүү) же айрым тиркемелердин иштөө өзгөчөлүктөрү сыяктуу тиешелүү касиеттерин унутпашыбыз керек, алардын айрымдары маанилүү функцияларды камсыз кылбашы мүмкүн. SSL/TLS аркылуу корголгон учурда кирүү башкаруусун кылдаттык менен конфигурациялоого болорун да эске алуу керек, анткени тиркемелердин ортосунда түздөн-түз коопсуз байланышты уюштуруу ар бир тиркеме үчүн ар кандай колдонуучунун кирүү укуктарын коюуга мүмкүндүк берет. Мындан тышкары, ар кандай колдонуучулар үчүн кирүү укуктарын дифференциялоо жөнөкөйлөтүлгөн.

Каралып жаткан технологиялар тар-

мактын ар кандай деңгээлдерине таандык экендиги алардын NAT түзүлүштөрү менен иштөө өзгөчөлүктөрүнө да өз изин калтырат. Бул түзмөктөр IP-пакеттердеги IP даректерин өзгөртөт, бул IP пакеттеринин бүтүндүгүн көзөмөлдөгөн VPN протоколдору колдонулса, алар аркылуу коопсуз трафикти өткөрүүдө кыйынчылыктарды жаратышы мүмкүн. Мындай протоколдорго, мисалы, IPsec кирет. Бул маселени чечүү жолу катары NAT-T технологиясын колдонуу каралышы мүмкүн, бул корголгон пакеттердин NAT түзүлүштөрү аркылуу ийгиликтүү өтүшүнө мүмкүндүк берет. Бирок, NAT-T технологиясы бардык VPN ишке ашыруулары тарабынан колдоого алынбайт, бул колдонулган чечимдердин шайкештигине терс таасирин тийгизет. SSL/TLS протоколунда NAT түзмөктөрүндө сүрөттөлгөн көйгөйлөр жок, анткени ал транспорттук катмардын үстүндө жайгашкан жана анын иштешинин тууралыгы IP даректерин жана порт номерлерин өзгөртүүдөн көз каранды эмес. Каралып жаткан технологиялардын дагы бир маанилүү айырмасы VPN чечимдери транспорттук протокол катары TCP жана UDP экөөнү тең колдоно алат, ал эми классикалык SSL/TLS чечимдери TCP гана колдоно алат. Бул пакеттик жоготуулардан улам келип чыккан трафиктин кечигүүлөрү маанилүү болгон сценарийлерде SSL/TLS колдонууну чектейт. Белгилей кетсек, мындай учурлар үчүн DTLS деп аталган альтернативдүү протокол иштелип чыккан, ал UDP транспорттук протоколун колдоо үчүн кайра иштелип чыккан TLS 1.1 версиясы. Бирок, бардык эле жалпы SSL/TLS ишке ашыруу DTLS колдоосун камсыз кыла бербейт.

Эксплуатациялоо жана каржы маселелери

Белгилүү бир чечимди тандоодо колдонуучулар көңүл бурган негизги параметрлердин арасында бул чечимдердин конфигурациясынын жана иштешинин жөнөкөйлүгү, ошондой эле алардын баасы шексиз. Бул параметрлер кандайдыр бир кошумча программалык камсыздоону орнотуу жана аны конфигурациялоо зарылдыгы менен түздөн-түз байланыштуу. VPNди жайылтуу, адатта, атайын жабдыктарды же программалык камсыздоону, андан кийин бир топ татаал конфигурацияны орнотууну талап кылат. SSL/TLS аркылуу коопсуз байланыштарды ишке ашыруу жана конфигурациялоо биринчи караганда бир топ жөнөкөй иш болуп көрүнөт. Бул негизинен ар кандай заманбап браузер SSL/TLSде кардар ролун ойной ала тургандыгы менен байланыштуу.

Кардардын программалык камсыздоосун орнотуу зарылдыгынын жоктугунан келип чыккан артыкчылыктар айкын жана каржылык жана уюштуруучулук чыгымдарды кыскартуу менен көрсөтүлөт. Бирок бул жерде да кээ бир өзгөчөлүктөр бар. Белгилей кетчү нерсе, браузерди кардар катары колдонуу бизге веб-тиркемелерди колдонууга гана мүмкүндүк берет. Башка тиркемелер менен иштөөнү уюштуруу үчүн сизде кошумча түрдө браузер үчүн атайын Java апплеттери же ActiveX плагиндери болушу керек, алар биринчиден, өзүнүн кемчиликтерине ээ болушу мүмкүн, экинчиден, аларды орнотуу браузердин коопсуздук саясатына карама-каршы келиши мүмкүн. башка, ансыз деле зыяндуу плагиндердин коркунучтарына алып келиши мүмкүн.

Мындан тышкары, VPN болгон учурда кардар программасын орнотуу зарылчылыгы анын алдын ала квалификацияланган конфигурациясы менен бирге максаттуу маалыматтарга уруксатсыз кирүүнү кыйындаткан кошумча коопсуздук чарасы катары каралышы мүмкүн.

SSL/TLS колдонууда кардар тарапты орнотуунун оңойлугуна келсек, бул билдирүү сервердин аутентификациясы гана аткарылган өз ара аракеттенүүдө гана туура болот. Эгерде кардардын ау-

тентификациясы кошумча талап кылынса, анда VPNди жайылтууда пайда болгон жашыруун/жеке ачкычтарды баштапкы жеткирүү жана алардын коопсуз сактагычын уюштуруу сыяктуу көйгөйлөр SSL/TLS үчүн да пайда болот.

Чечимдин баасына таасир эткен дагы бир өзгөчөлүк - бул технологиянын шайкештиги. Ар кандай VPN ишке ашыруулар, алар бир эле протоколго негизделген болсо да, ар дайым бири-бири менен шайкеш келбейт. Бул системаны кеңейтүү жана бир нече системаны бир системага бириктирүү процессин татаалданткан бир типтеги жабдууларды колдонуу зарылдыгына алып келет. SSL/TLS ишке ашыруулар көбүрөөк унификацияланган, бирок көбүнчө айрым криптографиялык алгоритмдерди, функцияларды жана параметрлерди колдоо жагынан айырмаланат.

Маалымат коопсуздугу

VPN технологиясын колдонууда тараптардын аутентификациясы адатта сертификаттардын (IPsec) же алдын ала бөлүштүрүлгөн жашыруун ачкычтардын (IPsec, IPlir) негизинде жүргүзүлөт. Бул сиздин конкреттүү сценарийиңизге жараша эң ылайыктуу аутентификация ыкмасын тандоого мүмкүндүк берет.

SSL/TLSде аутентификация үчүн колдонулган классикалык ыкма сертификаттарды колдонуу болуп саналат. Бирок, сырсөзгө негизделген аутентификация жана алдын ала бөлүшүлгөн ачкыч аутентификациясы сыяктуу альтернативалуу ыкмалар бар, бирок алар SSL/TLS ишке ашыруларынын өтө чектелген саны менен колдоого алынат. Демек, SSL/TLS протоколун колдонгон системалардын басымдуу көпчүлүгү коопсуздук сертификаттарга жана PKIге негизделген системалардын бардык негизги кемчиликтерине ээ.

Дагы бир коопсуздук аспектиси кардарлардын аппараттарын коргоо болуп саналат. VPN компаниялары көбүнчө антивирустар, брандмауэрлер, файлдарды шифрлөө сыяктуу кошумча чечимдерди сунушташат. Тиешелүү коопсуздук саясаттарын туура конфигурациялоо менен бирге бул чечимдерди колдонуу кардар түзмөгүнө уруксатсыз кирүү мүмкүнчүлүгүн минималдаштырууга мүмкүндүк берет.

SSL/TLS колдонууда, ага кирүү укугун берүүдөн мурун, кардар түзмөгүндө бир катар текшерүүлөрдү жүргүзүүгө болот. Бирок, мындай текшерүүлөрдү жүргүзүү, адатта, кошумча серепчи апплеттерин орнотууну талап кылат.

SSL/TLS протоколунун кеңири колдонулушу аны деталдуу изилдөө үчүн негиз болуп кызмат кылган жана бул бул протоколдо бир катар кемчиликтерди табууга алып келген. Алсыздыктар архитектуралык болуп бөлүнөт, башкача айтканда, SSL/TLS протоколунун спецификациясынын өзүндөгү кемчиликтерге жана протоколдун конкреттүү ишке ашырууларына гана мүнөздүү болгондорго негизделген. Бул бөлүнүүнү шарттуу деп атоого болот, анткени көпчүлүк архитектуралык алсыздыктар SSL/TLS спецификациясынын теориялык өзгөчөлүктөрүнө негизделген, бирок бир катар практикалык талаптарды колдонууну талап кылат. SSL/TLSге негизги чабуулдарга BEAST, Padding Oracle чабуулдары (Vodoney чабуулу, Lucky 13, Poodle), RC4 агымынын шифрине чабуулдар, «кайра сүйлөшүү» чабуулу, маалыматтарды кысуу негизинде жасалган чабуулдар жана башка чабуулдар кооптуу криптографиялык параметрлерди киргизүүгө негизделген (Freak, Logjam), колдонулган SSL/TLS протоколунун версиясын төмөндөтүүгө негизделген чабуулдар (Heartbleed).

Сандалган чабуулдардын көбү жарыяланып жаткан учурда гана мүмкүн болгон жана кийинчерээк жок кылынган. Бул протоколду иштеп чыгууда SSL/TLS жаңы кемчиликтеринин ачылышы да оң натыйжа берди деп айта алабыз, анткени ал негизинен анын өнүгүшүн аныктап, же аны колдонуу боюнча кошумча

сунуштарды иштеп чыгууга, же жаңы протоколдорду чыгарууга алып келди. Буга карабастан, тармактагы көп сандагы түйүндөр дагы эле SSL/TLS протоколдорунун эски версияларын колдонуп жатышат же жөн гана жаңы чабуулдарды аныктоо ыктымалдуулугунун жогору болушу менен бирге учурдагы сунуштарды эске албай жатышат.

VPNди жайылтуу үчүн колдонулган кээ бир протоколдор ар кандай чабуулдарга кабылышы мүмкүн, буга PPTP протоколундагы бир катар олуттуу кемчиликтер себеп болот. Бирок, IPsec жана IPlir сыяктуу протоколдор коопсуздуктун адекваттуу деңгээлин камсыз кылат деп эсептелинет, анткени аларда учурда эч кандай олуттуу аныкталган кемчиликтер жолуга элек.

Корутунду

Жыйынтыктап айтканда, азыркы учурдагы VPN жана SSL/TLS протоколдорун бир эле маселени чечүүчү технологиялар катары эсептебөө керектигин билишибиз керек. VPN жана SSL/TLS ар кандай маселелерди жана процесстерди чече алат, бул технологиялар ар кандай касиеттерге ээ, аларды биргелешип колдонсо да болот. Бул технологиялар бири бирине атаандаш технология болсо да, алар бири-бирин толуктап, колдонуудагы функционалдык мүмкүнчүлүктөрүн кеңейтүүгө шарт түзүшөт. Алардын ар биринин маалыматтык коопсуздук тармагында өз орду бар экендигин баса белгилеп кетсек болот. Ошол эле учурда конкреттүү технологияны тандоо ар бир технологиянын иштөө өзгөчөлүктөрү менен өзүнүн муктаждыктарын, максаттарын жана шарттарын салыштыруу жолу менен жүргүзүлүүгө тийиш жана колдонууга мүмкүн.

Колдонулган адабияттар

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.

2. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2019. - 474 с.

3. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2020. - 324 с.

4. Нечаев Д. VPN: прошлое, настоящее, будущее. [Электронный ресурс]. Режим доступа: https://habrahabr.ru/company/celecom/blog/221675/

5. https://kyrgyzstanvpn.com/ru/