Шундай қилиб, электромагнит майдонда жойлашган юпқа анизотроп пластиналар тебраниш масаласининг математик модели ишлаб чиқилди.

Бунда электромагнитэластик юпқа анизатроп пластинанинг геометрик ночизиқ деформацион-кучланиш ҳолатига электромагнит майдон таъсирлари ўрганилди;

Гамильтон-Остроградский вариацион тамойили асосида Кирхгоф-Ляв гипотезаси, Коши муносабатлари, Гук қонуни ҳамда Максвелл электромагнит тензор кўринишларидан фойдаланиб, потенциал энергия, кинетик энергия ва ташқи кучлар бажарган ишнинг вариацион кўринишлари аниқланди. Натижада кўчишга нибатан бошланғич ва чегаравий шартларга эга, хусусий ҳосилали дифференциал тенгламалар системаси кўринишидаги математик модели олинди;

Бу тенгламалар, тадқиқ қилинаётган пластина чегараларини маҳкамлаш ҳолатларига қараб, тегишли чегаравий шартларда ечилади.

Адабиётлар

1. Амбарцумян С.А., Багдасарян Г.Е., Белубекян М.В. Магнитоупругость тонких оболочек и пластин. - М.: “Наука”. 1977.
2. Амбарцумян С.А. Теория анизотропных пластин. - М.: «Наука», 1987. –С. 360.
3. Амбарцумян С.А., Белубекян М.В. Некоторые задачи электромагнитоупругости пластин. –Ереван: 1991. –С. 144.
4. Кабулов В.К. Алгоритмизация в теории упругости и деформационной теории пластичности. - Ташкент: «Фан», 1966.
5. Васидзе К. Вариационной методы в теории упругости и пластичности. Пер с англ. – М.: «Мир», 1987. –С. 542.

РЕЗЮМЕ

Мақола юпқа мураккаб шаклдаги анизотроп пластиналарнинг электромагнит эластиклик деформацион-кучланиш ҳолатини математик моделлаштиришга бағишланади.

РЕЗЮМЕ

Статья посвящена математическому моделированию электромагнитно-упругого, деформационно-напряженного состояния анизотропных пластин сложной формы.

SUMMARY

The article is devoted to the mathematical modeling of the electromagnetic-elastic deformation-stress state of anisotropic plates of thin complex shape.

УДК 004.056.5

БИР МӘРТЕЛИК ПАРОЛЬ ТИЙКАРЫНДА БИР БАҒДАРЛЫ АУТЕНТИФИКАЦИЯ ПРОТОКОЛЛАРЫНЫҢ АНАЛИЗИ

Ж.Т.Арзиева – *техника илимлери бойынша философия докторы, доцент*
С.М.Калмуратова – *стажер оқытыўшы*
Н.Р.Палўаниязова - *студент*
Бердақ атындағы Қарақалпақ мәмлекетлик университети

Таянч сўзлар: бир марталик парол, БМП, HOTP алгоритми, TOTP алгоритми, SMS, smart-karta, token, RSA Security.
Ключевые слова: одноразовый пароль, ОПР алгоритм HOTP , алгоритм TOTP, SMS, смарт-карта, токен, RSA Security.
Key words: one-time password, OTP, HOTP algorithm, TOTP algorithm, SMS, smart card, token, RSA Security.

OTP (One-time password) тармақ ямаса хызметтен пайдаланыўда бир мәртелик пароллерге тийкарланған механизм болып, ол қолға киргизилген логин/парольден қайта пайдалана алмаўды кепиллей алады. Бундай жағдайда, пайдаланыўшының логини өзгерместен, ҳәр бир урыныўда оның пароли өзгерип турады.

Бир мәртелик пароллер, әдетте, бир тәреплеме функциялар есапланған *хэш функциялар* тийкарында пайда етиледи ямаса хэш функциялар тийкарында аутентификация протоколы ислеп шығылады. OTP тийкарындағы бир бағдарлы аутентификация протоколлары олардан бири есапланады. Бул аутентификация протоколларында қарыйдар ҳәм серверде бир қыйлы “санақ мәниси” болып, қарыйдар бул санақ мәниси ҳәм жасырын гилти жәрдеминде бир мәртелик паролды генерация қылады ҳәм оннан кейин санақтың мәниси асырылады. Генерация қылынған бир мәртелик паролды пайдаланыўшы серверге киритеди. Өз нәўбетинде, сервер де клиент пенен бирдей болған санақ мәниси ҳәм жасырын гилти жәрдеминде бир мәртелик паролды генерация қылады ҳәм қарыйдар тәрепинен киритилган пароль менен салыстырылады. Салыстырыў нәтийжеси қанаатландырарлы болғанда пайдаланыўшы аутентификациядан өткен есапланады. Кери жағдайда болса, аутентификациядан өте алмайды [1:45].

Бир бағдарлы бир мәртелик пароллерге тийкарланған аутентификация протоколларында OTP ны пайдаланыўшы тәрепинен серверге төмендегише жеткериўи мүмкин:

a) Қарыйдарда да серверде бар болған OTP генераторы ҳәм бир қыйлы санақ мәниси (ҳәм жасырын гилт) бар болып, әдетте қурылма (яки программалық қурал) көринисинде болған *жеке токен* арқалы пайда етиледи. Қурылмада (мәселен, қурылманың экранында пайда болған) ямаса программалық қуралларда (мәселен, арнаўлы мобил қосымшаларында (приложениелеринде)) пайда болған OTP қарыйдар тәрепинен “қолда” киритиледи. Буларға RSA Security шөлкемниң SecurID қурылмасын ямаса TOTP (ямаса HOTP)ға тийкарланған мобил косымшаларды (Google Authenticator, Microsoft Authenticator) мысал етип келтириў мүмкин.

HOTP протоколы. HOTP (An HMAC-Based One-Time Password Algorithm) алгоритми еки тәрепте бөлистирилген гилт K ҳәм бир қыйлы санақ жағдайы C болғанда синхрон ислейди.

TOTP протоколы. TOTP (Time-Based One-Time Password Algorithm) алгоритми HOTP дан парықлы түрде санақ мәниси сыпатында ўақыттан пайдаланады. Ўақыт зоналары менен бар машқалалардан қашыў ушын 1970-жыл 1-январьдан басланыўшы секундта көрсетилген UNIX ўақыт белгисинен пайдаланылған. Бул ўақыт мәниси секундта көрсетилгени ушын ҳәр 30 секундта TOTP ушын кириўши T параметр пайда болады ($T = \left[\frac{UNIX\ ўақты}{30}\right]$).

Әмелде ўақытты синхронлаўға ҳәм санақты синхронлаўға тийкарланған OTP протоколлары жүдә кең пайдаланылады. Бул еки протоколға тийкарланған аутентификация протоколларындағы артықмашылығы ҳәм де кемшиликлери 1-кестеде сәўлеленген.

Ҳәр еки протоколдың да өзине тән артықмашылығы ҳәм кемшиликлери бар болса, қәўипсизлик көзқарасынан қысқа ўақыт даўамында әмел етиўи ҳәм пайдаланыўдағы қолайлылығы себепли ўақытты синхронлаўға тийкарланған аутентификация усыллары-нан пайдаланыў мақсетке муўапық есапланады.

b) OTP сервер тәрепинен пайда етиледи ҳәм узатыў тармақлары арқалы клиентке жеткизиледи. Буларға мысал ретинде мобил қурылмаларына SMS (Short Message Service) арқалы жибериў, электрон почта арқалы жибериў ямаса “қағазға” жазып алыў усылларын келтириў мумкин.

1 – кесте. Ўақытты синхронлаўға ҳәм санақты синхронлаўға тийкарланған OTP протоколларының анализи

Синхронла-ныўшы шама	Қәўипсизлик	Пайдаланыўда
Ўақытқа	*Артық:* OTP мәниси қысқа ўақыт ушын бар.	*Артық:* OTPды қурылма экранынан аңсатлық пенен оқыў мүмкин.
	Кем: OTP мәниси гүзетиўши тәрепинен аңсатлық пенен алыныўы мүмкин.	*Кем:* OTP мәниси ол киритилгенге шекем өзгериўи мүмкин.
Санақ	*Артық:* OTPды генерация қылыў ушын бузғыншы қурылманы басқарыўы талап етиледи.	*Артық:* OTP мәниси пайдаланыў-шының сораўына қарай генерация қылынады; белгили ўақыттан кейин оның мәниси өзгерип қалмайды.
	Кем: OTPды таза OTP пайдаланыўға шекем пайдаланыў мүмкин болады.	*Кем:* OTPды генерация қылыў ушын пайдаланыўшы “генерация қылыў” түймесин басыўы талап етиледи.

SMS (инглиз тилинде *Short Message Service* — «қысқа хабар хызмети») арқалы узатыў – банк – финанс тараўында төлемлерди әмелге асырыўда кең қолланылыўшы ҳәм барлық түрдеги мобил қурылмалар ушын зәрүр болған усыл есапланса да, қатаң қәўипсизлик машқаласына ийе. Яғный, SMS хабарларды ашық ҳалатта жиберилиўи ямаса SS7 маршрутлаў протоколындағы қәўипсизлик машқалалары себепли, оларда жиберилген OTP ды аңсатлық пенен қолға киргизиў мүмкин.

c) Сервер тәрепинен генерация қылынған OTPлар қарыйдарға веб браузерге арнаўлы көринисте усынылады.OTPды жеткизиўдиң бул усылына вебге тийкарланған усылды киргизиў мүмкин. Бул усыл пайдаланыўшының тосыннан усынылған сүўретлери арасынан алдыннан таңланғанларын таныў қәбилетине тийкарланған. Пайдаланыўшы дәслеп дизимнен өтиўде усынылған нәрселердиң (пышық, машина, гүллер ҳәм жасырын топарын таңлайды. Аутентификациядан өтиў даўамында система оған тосыннан таңланған нәрселерди (әлбетте, алдын таңлаған нәрселери де олар арасында болады) усынады. Ҳәр бир усынылғанлардың арқа фонында тәкирарланбас цифр бар болады. Пайдаланыўшы тәрепинен усынылғанлар арасынан алдыннан таңланғанлары белгиленеди ҳәм бул жағдайда арқа фонындағы цифрлар тосыннанлық OTPды пайда етеди [5:3].

Буннан тысқары, Confident Technologies тәрепинен ислеп шығылған вебке тийкарланған OTP система-сында аутентификациядан өтиў ўақтында мобил телефонға сүўретлерди таңлаў имканиятын бериўши силтемени жибереди. Бул силтемеге мүрәжат болғанда веб браузерге сүўретлер арасынан кереклисин таңлаў ҳәм OTPды генерация қылыў әмелге асырылады.

Қолланыўда кең пайдаланыўы көзқарасынан SMSке жибериўге тийкарланған жеткизиў усылы қалғанлары ажыралып турса да, онда қәўипсизлик машқалалары критикалық жағдайларда пайдаланыўды шеклейди. Қурылма көринисиндеги токенлер жоқары қәўипсизликти тәмийинлесе де, оның жоқары баҳалылығы ҳәм барқулла бирге алып жүриў зәрүрлиги себепли қолайсызлықларға себеп болады. Ҳәзирги күнге келип мобил қурылмалардың кең тарқалыўы ҳәм инсанлардың ажыралмас жолдасына айланыўы программалық көринистеги токенлерден пайдаланыў имканиятын асырады. Бирақ, мобил операциялық системалардың қәўипсиз емеслиги ямаса “желке арқалы қараў” сыяқлы ҳүжимлер нәтийжесинде қосымша қәўипсизлик шараларын көриў талап етиледи [1:8].

Почта арқалы жибериў ямаса қағазда жазған ҳалда алып жүриў сәйкес түрде қосымша билимди (почта паролин) ямаса барқулла қасында қәўипсиз сақлаў зәрүрлигин талап етеди. Вебке тийкарланған усыллар болса ҳәзирги күнде кирип киятырған жаңа түсиниклер болып, инсан ядында аңсат сақлаў усылынан пайдаланыўға ҳәрекет етеди.

Әдебиятлар

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. -М.: ИД ФОРУМ, ИНФРА-М. 2011.
2. Knuth D. E. Art of computer programming, Seminumerical algorithms, AddisonWesley Professional, 2. 2014.
3. Alzomai M.H. Identity management: strengthening one-time password authentication through usability: dis. Ц Queensland University of Technology, 2011.
4. Takasuke TSUJI, A One-Time Password Authentication Method, MasterЎs thesis, January 31, 2003.
5. Каримов М.М., Арзиева Ж.Т., Худойкулов З.Т. Муҳаммад Ал-Хоразмий Авлодлари. Илмий-амалий ва ахборот-таҳлилий журнал 4(10) 2019, 3-б.

РЕЗЮМЕ

Ушбу мақолада бир мартали пароллар асосида бир йўналишли аутентификация протоколларининг таҳлили келтирилган. Бир йўналишли бир мартали паролларга асосланган аутентификация усулларида OTPларни етказиш усулларининг қиёсий таҳлили келтирилган.

РЕЗЮМЕ

В статье представлен анализ протоколов односторонней аутентификации на основе одноразовых паролей. Представлен сравнительный анализ способов передачи OTP в методах аутентификации на основе одноразовых паролей.

SUMMARY

The article deals with the state presented the analysis of protocols of single authentication on the basis of single passwords. A comparative analysis is presented OTP transmission methods in autnentification methods based on one-time passwords.

“АМАЛИЙ МЕХАНИКА” ФАНИНИ ЎҚИТИШДА ИННОВАЦИОН ТАЪЛИМ ТЕХНОЛОГИЯЛАРИДАН ФОЙДАЛАНИШ ИСТИҚБОЛЛАРИ

З.Р.Асраев – *таянч докторант*

Бухоро муҳандислик-технология институти

Таянч сўзлар: инновация, инновацион таълим технологиялари, замонавий таълим технологиялари, интерфаол усуллар, кичик гуруҳларда ишлаш, ахборот-коммуникация технологиялари.

Ключевые слова: инновация, инновационные образовательные технологии, современные образовательные технологии, интерактивные методы, работа в малых группах, информационно – коммуникационные технологии.

Key words: innovation, innovative educational technologies, modern educational technologies, interactive methods, work in small groups, information and communication technologies.

Ўзбекистон Республикаси таълим йўналишларининг малакавий талабларидан келиб чиққан ҳолда техник йўналишлар бакалаврларини тайёрлаш бўйича ўқув дастурларини амалга ошириш шартларига қўйилган талаблардан бири бу талабаларнинг касбий компетент-лигини шакллантириш учун соҳада инновацион таълим