ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ФАРҒОНА ФИЛИАЛИ

ТЕЛЕКОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ВА КАСБИЙ ТАЪЛИМ ФАКУЛЬТЕТИ

“АХБОРОТ– ТАЪЛИМ ТЕХНОЛОГИЯЛАРИ” КАФЕДРАСИ

«Идентификация ва аутентификация” фани бўйича

“МАЪРУЗАЛАР МАТНИ

ФАРҒОНА 2017

«Идентификация ва аутентификация». Маърузалар матни**. 58-бет**

Тузувчи:

Худойназаров У.У Мухаммад ал-Хорахмий номидаги Тошкент ахборот технологиялари университети фар-она филиали ахборот таълим технологиялари кафедраси асистенти.

Тақризчи:

М.Турдиматов Фарғона давлат университети доценти.

Ушбу маъруза матни ҳозирги кунда тармоқ хавфсизлиги муаммоси корхона ва ташкилотларда мавжуд ахборот коммуникацион тизимларида тутган ўрни, уларни ҳал этиш усуллари, ахборот хавфсизлиги тизимларини ахборот-коммункацион тизимларда ишлаш принципи, уларни қўлланиш афзалликлари, ривожланиш тамойиллари ва республикамизда тармоқ хавфсизлиги бўйича олиб борилаётган изланишлар ва ишлаб чиқилган воситалари ҳамда уларнинг келажакдаги ўрни масалаларини қамрайди.

«Идентификация ва аутентификация» фанидан тайёранган маъруза матни талабаларнинг ахборотни самарали қайта ишлашдаги асосий усуллари тўғрисидаги билимларни, шунингдек маълумотларни хавфсиз узатишни таъминловчи аутентификациянинг асосий усуллари тўғрисидаги билимларини оширишда катта роль ўйнайди.

1-маруза:

Асосий тушунчалар. Идентификациялаш усуллари. Структурали идентификация. Параметрли идентификация.

1. Асосий тушунчалар
2. Аутентификация жараёнларини категорияларга булиниши

Компьютер тизимида руйхатга олинган хар бир субъект (фойдаланувчи ёки фойдаланувчи номидан харакатланувчи жараён) билан уни бир маънода индентификацияловчи ахборот боглик.

Бу ушбу субъектга ном берувчи сон ёки символлар сатри бўлиши мумкин. Бу ахборот субъект ***идентификатори*** деб юритилади. Агар фойдаланувчи тармоқда руйхатга олинган идентификаторга эга бўлса у легал (қонуний), акс холда легал булмаган (ноқонуний) фойдаланувчи хисобланади. Компьютер ресурсларидан фойдаланишдан аввал фойдаланувчи компьютер тизимининг идентификация ва аутентификация жараёнидан ўтиши лозим.

Идентификация (Identification) - фойдаланувчини унинг идентификатори (номи) буйича аниқлаш жараёни. Бу фойдаланувчи тармоқдан фойдаланишга уринганида биринчи галда бажариладиган функциядир. Фойдаланувчи тизимга унинг сўрови буйича ўзининг иденгификаторини билдиради, тизим эса ўзининг маълумотлар базасида унинг борлигини текширади.

Аутентификация (Authentication) - маълум килинган фойдаланувчи, жараён ёки қурилманинг хакикий эканлигини текшириш муолажаси. Бу текшириш фойдаланувчи (жараён ёки қурилма) хақиқатан айнан ўзи эканлигига ишонч хосил қилишга имкон беради. Аутентификация ўтказишда текширувчи тараф текширилувчи тарафнинг хакикий эканлигига ишонч хосил қилиши билан бир қаторда текширилувчи тараф хам ахборот алмашинув жараёнида фаол қатнашади. Одатда, фойдаланувчи тизимга ўзи хусусидаги ноёб, бошқаларга маълум бўлмаган ахборотни (масалан, парол ски сертификат) киритиши орқали идентификацияни тасдиклайди.

Идентификация ва аутентификация субъекгларнинг (фойда-ланувчиларнинг) хакикий эканлигини аниқлаш ва текширишниш ўзаро богланган жараёнидир Муайян фойдаланувчи ёки жараённинг тизим рссурсларидан фойдаланишига тизимнинг рўхати айнан шуларга боғлиқ. Субъектни идентификациялаш ва аутентификациялашдан сўнг уни авторизациялаш бошланади.

Авторизация (Authorization) - субектга тизимда маълум ваколат ва ресурсларни бериш муолажаси, яъни авторизация субъект харакати доирасини ва у фойдаланадиган ресурсларни белгилайди. Агар тизим авторизацияланган шахсни авторизацияланмаган шахсдан ишончли ажрата олмаса бу тизимда ахборотнинг конфиденциаллиги ва яхлиглиги бузилиши мумкин. Аутентификация ва авторизация муолажалари билан фойдаланувчи харакатшш маъмурлаш муолажаси узвий боғланган.

Маъмурлаш (Accounting) - фойдаланувчининг тармоқдаги харакатини, шу жумладан, унинг ресурслардан фойдаланишга уринишини қайд этиш. Ушбу хисобот ахбороти хавфсизлик нуқтаи назаридан тармоқдаги хавфсизлик ходисаларини ошкор қилиш, тахлиллаш ва уларга мос реакция кўрсатиш учун жуда мухимдир.

Маълумотларни узатиш каналларини химоялашда ***субъектларнинг ўзаро аутентификацияси.*** яъни алоқа каналлари орқали боғланадиган субъектлар хакикийлигининг ўзаро тасдиғи бажарилиши шарт. Хакикийликнинг тасдиғи одатда, сеанс бошида, абонентларнинг бир-бирига уланиш жараёнида амалга оширилади. «Улаш» атамаси орқали тармоқнинг иккита субъекти 5тасида мантикий боғланиш тушунилади. Ушбу муолажанинг максади конуний субъект билан амалга оширилганлигига ва барча ахборот мўлжалланган манзилга боришлигига ишончни таъминлашдир.Ўзининг хакикийлигининг тасдиклаш учун субъект тизимга турли асосларни кўрсатиши мумкин. Субъект кўрсатадиган асосларга боғлиқ холда аутентификация жараёнлари куйидаги категорияларга бўлиниши мумкин:

Бирор нарсаии билиш асосида. Мисол сифатида парол, шахсий идентификация коди PIN (PersonalIdentificationNumber) хамда «сўров жавоб» хилидаги протоколларда намойиш этилувчи махфий ва очиқ калитларни кўрсатиш мумкин;

Бирор нарсага эгалиги асосида. Одатда, булар магнит карталар, смарг-карталар, сертификатлар ва touchmemory курилмалари;

Қандайдир дахлсиз характеристикалар асосида. Ушбу категория ўз таркибига фойдаланувчининг биометрик характеристикаларига (овозлар. кўзининг рангдор пардаси ва тур пардаси, бармоқ излари, кафт геометрияси ва х.) асосланган усулларни олади. Бу категорияда криптографик усуллар ва воситалар ишлатилмайди. Беометрик характеристикалар бинодан ёки қандайдир техникадан фойдаланишни назоратлашда ишлатилади.

Парол - фойдаланувчи хамда унинг ахборот алмашинувидаги шериги биладиган нарса. Ўзаро аутентификация учун фойдаланувчи ва унинг шериги ўртасида парол алмашиниши мумкин. Пластик карта ва смарт-карта эгасини аутентификациясида шахсий идентификация номери PIN енналган усул хисобланади. PIN - коднинг махфий қиймати фақат карта эгасига маълум бўлиши шарт.

Динамик - (бир мирталик) парол - бир марта ишлатилганидан сўнг бошқа умуман ишлатилмайдиган парол. Амалда одатда доимий паролга ёки таянчиборога асосланувчи мунтазам ўзгариб турувчи қиймат ишлатилади.

«Сўров-жавоб» тизими - тарафларнинг бири ноёб ва олдиндан билиб бўлмайдиган «сўров» қийматини иккинчи тарафга жўнатиш орқали аутентификацияни бошлаб беради, иккинчи тараф эса сўров ва сир ёрдамида хисобланган жавобни жўнатади. Иккала тарафга битта сир маълум бўлгани сабабли, биринчи тараф иккинчи тараф жавобини тўғрилигини текшириши мумкин.

Сертификатлар ва рацамли шиолар - агар аугентификация учун сертификатлар ишлатилса, бу сертификатларда рақамли имзони ишлатилиши талаб этилади. Сертификатлар фойдаланувчи ташкилотининг масъул шахси,

сертификатлар сервери ёки ташқи ишончли ташкилот томонидан берилади. Internet доирасида очиқ калит сертификагларини тарқатиш учун очиқ калитларни бошқарувчи қатор тижорат инфратўзилмалари PKI (PublicKeyInfrastructure) пайдо бўлди. Фойдаланувчилар турли даража сергификатларини олишлари мумкин.

Аугентификация жарёнларини таъминланувчи хавфсизлик даражаси буйича хам туркумлаш мумкин. Ушбу ёндашишга биноан аутентификация жараёнлари куйидаги турларга бўлинади:

- пароллар ва рақамли ссртификатлардан фойдаланувчи аутентификация;
- криптографик усуллар ва воситалар асосидаги катьий аутентификация;
- ноллик билим билан исботлаш хусусиягига эга бўлган аутентификация жараёнлари (протоколлари);
- фойдаланувчиларни биометрик аутентификацияси.

Хавфсизлик нуқтаи назаридан юкорида келтирилганларнингхар бири ўзига хос масалаларни ечишга имкон беради. Шу сабабли аутентификация жараёнлари ва протоколлари амалда фаол ишлатилади. Шу билан бир қаторда таъкидлаш лозимки, ноллик билим билан исботлаш хусусиятига эга бўлган аутентификацияга қизиқиш амалий характерга нисбатан кўпроқ назарий характерга эга. Балким, яқин келажакда улардан ахборот алмашинувини химоялашда фаол фойдаланишлари мумкин.

2-маруза:

Аутентификациялашнинг аҳамияти ҳамда вазифалари. Ахборотни ҳимоялашда аутентификациянинг ўрни.

1. Аутентификациялаш тизимларини таркиби
2. Ахборотни ҳимоялашда аутентификациянинг ўрни

Аутентификациялаш тизимлари типидан қатъий назар бешта элементдан ташкил топади.

Биринчи элемент - аутентификациядан ўтиши шарт бўлган инсон ёки жараён, фойдаланиш субъекти.

Иккинчи элемент – билдирувчи белги, инсон ёки жараённи бошқаларидан ажратиб олиш учун идентификатор.

Учинчи элемент – фойдаланувчи субъекти идентификаторини тасдиқлаш жараёни яъни аутентификатор.

Тўртинчи элемент - Тизим эгаси (администратор), тизимдан фойдаланиш жавобгарлигини, авторизациядан ўтган фойдаланувчиларни ва бошқа фойдаланувчиларни аутентификациялаш механизмидан ўтказиш.

Бешинчи элемент – аутентификациялаш механизми.

Муваффақиятли аутентификациядан ўтган фойдаланувчига маълум бир хуқуқлар тўплами берилади. Бунинг учун тизимдан фойдаланишни бошқариш механизми хизмат қилади. Ушбу механизм ёрдамида фойдаланувчи субъекти агар аутентификациядан ўтмаган бўлса тизимдан фойдаланиш хуқуқидан махрум этилади.

Аутентификациядан ўтиш жараёнига жисмоний шахснинг тизимга пароль ёрдамида киришини мисол келтирсак бўлади. Жисмоний шахс – бу шундай инсонки, яъни у компъютердан фойдаланиш хуқуқига эга инсон. Одатда тизимдан фойдаланадиган жисмоний шахсга идентификацион код берилади яъни фойдаланувчининг исми. Тизим администратори фойдаланувчининг исмига қараб унинг авторизациядан ўтган ёки

ўтмаганлигини аниқлаши мумкин. Ундан ташқари ҳар бир фойдаланувчига ном бериши мумкин яъни “*фойдаланувчи*” каби. Ушбу идентификатордан бир қанча фойдаланувчи гуруҳлар фойдаланиши мумкин. Уларнинг бир биридан фарқлашда махфий парольдан фойдаланилади. Тизим ушбу пароллар ёрдамида тизим фойдаланувчиларини ажратиб, фойдаланувчини приоритетига қараб хуқуқлар тўплами тақдим этади. Ушбу жараёнга мисол сифатида компъютерга регистрация орқали кириш, яъни фойдаланувчининг тизимга кириш учун логин ва парольларини киритишини келтиришимиз мумкин. Бу жараёнда конкрет аутентификациялаш амалга ошмоқда, яъни фойдаланувчи тизимга логин ва паролларини клавиатурадан киритганида тизим автоматик равишда ўқиб олади ҳамда тизим базасида мавжуд ушбу фойдаланувчига тегишли (регистрация жараёнида тизим администратори томонидан берилган ёки фойдаланувчининг ўзи киритган) парол ва логинлар билан солиштирилади. Агар пароль ва логинлар бир бирига мос тушса, демак фойдаланувчи аутентификациядан ўтган ҳисобланади.

Компъютер тизимларида аутентификация ҳамда фойдаланишни бошқариш одатда иккита турли функция сифатида қаралади. Аутентификациялаш жараёни фойдаланувчи идентификаторини тасдиқласа, фойдаланишни бошқариш эса фойдаланувчининг тизим ресурсларидан фойдаланиш хуқуқини белгилайди.

3-маруза:

Аутентификация ҳамда идентификациялашнинг факторлари

1. Аутентификация фактори
2. Аутентификация факторларини турлари

Субъект ўзининг шахсини тасдиқлаш ҳамда тизимдан фойдаланиш учун тизимга қандайдир махфий ахборотни тақдим этади. У тизимга ҳар қандай кўринишдаги ахборотни тақдим этиши мумкин.

Аутентификация фактори – аниқ бир информация тури бўлиб, субъектнинг аутентификациядан ўтиш учун тақдим этадиган махфий ахборотидир.

Одатда учта факторга асосланган аутентификациялаш усуллари мавжуд, яъни:

1.1-жадвал

Аутентификациялаш фактори	**Аутентификациялаш факторларига мисоллар**
Қандайдир билимни, ахборотни билишга асосланган аутентификация	• Пароль; • PIN-код (Personal Identification Number).
Қандайдир воситага эгалик қилишга асосланган аутентификация	• Физик калит; • Магнит карта; • OTP-токен, бир мартали пароль генерация қилувчи қурилма.
Биометрик характеристикаларга асосланган аутентификация	• Бармоқ изи; • Кўз пардаси; • Овоз, товушга асосланган.

Айрим компания ёки фирмаларда кириш-чиқишга кучли назорат ташкил қилинган, яъни компанияга кириш хуқуқи фақатгина чекланган миқдордаги шахсларга берилган бўлади. Масалан, сервер хонасига фақат

администратор ёки молия бўлими хоналарига фақат ушбу бўлим ходимлари кириш хуқуқига эга бўлишлари лозим.

Ҳозирги кунда соха-ташкилотларда кучли назоратни ташкил қилиш учун интеграллашган мантиқий воситалар ёрдамида аутентификацияловчи СКУД системалари қўлланилмоқда. Компъютер тизимидаги ресурслардан фойдаланиш учун смарт-карталардан фойдаланса бўлади. Ушбу воситадан турли хил биноларга киришда жисмоний шахсларни аутентификациялашда кенг фойдаланилмоқда.

Аутентификациялаш жараёни бир ҳамда кўп факторли бўлиши мумкин. Агар тизимга кириш жараёнида фақат битта фактордан фойдаланилса бу бир факторли аутентификация ёки бир нечта фактордан фойдаланилса кўп факторли аутентификация ҳисобланади. Масалан кўп факторли аутентификацияга қуйидагиларни мисол келтирса бўлади:

- ✓ фойдаланувчи тизимга киришда смарт карта билан биргаликда парольдан фойдаланиши;
- ✓ бармоқ изи ҳамда физик калит ёрдамида;
- ✓ кўз пардаси ҳамда PIN-код ёрдамида.

Масалан икки факторли аутентификация жараёнига банкоматларни мисол келтирсак бўлади. Чунки банкоматлар билан ишлаш жараёнида магнит палосали карта ҳамда PIN коддан бир вақтнинг ўзида фойдаланиш талаб этилади.

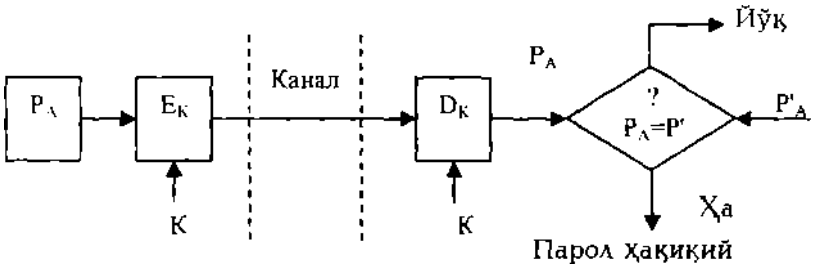
4-маруза:

Паролли аутентификациялаш усуллари.

1. Паролларга асосланган оддий аутентификациялаш тизими
2. Кўп ва бир мартали паролларга асосланган аутентификациялаш тизими

Аутентификациянинг кенг таркалган схемаларидан бири ***оддий аутентификациялаш*** бўлиб, у анъанавий кўп мартали [1ароларни ишлатишига асосланган. Тармоқдаги фойдаланувчини оддий аутентификациялаш муолажасини куйидагича тасаввур этиш мумкин. Тармоқдан фойдаланишга уринган фойдаланувчи компьютер клавиатурасида ўзининг идентификатори ва паролини теради. Бу маълумотлар аутентификация серверига ишланиш учун гушади. Аутентификация серверида сақланаётган фойдаланувчи идентификатори буйича маълумотлар базасидан мос ёзув топилади, ундан паролни топиб фойдаланувчи киритган парол билан таққосланади. Агар улар мос келса, аутентификация муваффакиятли ўтган хисобланади ва фойдаланувчи легал (конуний) макомини ва авторизация тизими орқали унинг мақоми учун аниқланган хуқуқларни ва тармоқ ресурсларидан фойдаланишга рухсатни олади.

Фойдаланувчи А **Аутентификация сервери**



1-расм. Паролдан фойдаланган холда оддий аутентификациялаш.

Равшанки, фойдаланувчининг паролини шифрламасдан узатиш орқали аутентификациялаш варианти хавфсизликнинг хатто минимал даражасини кафолатламайди. Паролни химоялаш учун уни химояланмаган канал орқали

узатишдан олдин шифрлаш зарур. Бунинг учун схемага шифрлаш $E_к$ ва расшифровка қилиш D_K воситалари киритилган. Бу воситалар булинувчи махфий калит К орқали бошқарилади. Фойдаланувчининг хакикийлигини текши риш фойдаланувчи юборган парол $\boldsymbol{P_A}$ билан аутентификациясерверида сакланувчи дастлабки қиймат $\boldsymbol{P_A}$ ни таққослашга асосланган. Агар $\boldsymbol{P_A}$ ва $\boldsymbol{P_A}$ қийматлар мос келса, парол $\boldsymbol{P_A}$ хакикий. фойдаланувчи $\boldsymbol{A}$ эса конуний хисобланади.

Оддий аутентификацияни ташкил этиш схемалари нафақат паролларни узатиш, балки уларни сакдаш ва текшириш гурлари билан ажралиб гуради. Энг кенг таркалган усул - фойдаланувчилар паролини гизимли файлларда, очиқ холда сақлаш усулидир. Бунда файлларга укиш ва ёзишдан химоялаш атрибутлари ўрнаеилади (масалан, операцион тизимдан фойдаланишни назоратлаш руйхатидаги мос имтиёзларни тавсифлаш ёрдамида). Тизим фойдаланувчи киритган паролни пароллар файлида сакланаётган езув билан солиштиради. Бу усулда шифрлаш ёки бир томонлама функциялар каби криптографик механизмлар ишлатилмайди. Ушбу усулпинг камчилиги - нияти бузуқ одамнинг тизимда маъмур имтиёзларидан, шу билан бирга тизим файлларидан, жумладан, парол файлларпдан фойдаланиш имкониятидир.

Хавфсизлик нуктаи назаридан паролларни бир томонлама функциялардан фойдаланиб узатиш ва сақлаш кулай хисобланади. Бу холда фойдаланувчи паролнинг очиқ шакли ўрнига унинг бир томонлама функция h(.) дан фойдаланиб олинган тасвирини юбориши шарт. Бу ўзгартириш ғаним томонидан паролни унинг тасвири орқали ошкор қила олмаганлигини кафолатлайди. чунки ғаним ечилмайдиган сонли масалага дуч келади.

Кўп мартали паролларга асосланган оддий аутентификациялаш тизимининг бардошлиги паст, чунки уларда аутентификацияловчи ахборот маъноли сўзларнинг нисбатан катта бўлмаган тупламидан жамланади. Кўп мартали паролларнинг таъсир муддати ташкилотнинг хавфсизлиги сиёсатида белгиланиши ва бундай паролларни мунтазам равишда алмаштириб туриш

лозим. Паролларни шундай танлаш лозимки, улар луғатда булмасин ва уларни гопиш кийин бўлсин.

Бир мартали паро.пларга асосланган аутентификациялашда фойдаланишга хар бир сўров учун турли пароллар ишлатилади. Бир мартали динамик парол фақат тизимдан бир марта фойдаланишга яроқли. Агар, хатто кимдир уни ушлаб қолса хам парол фонда бермайди. Одатда, бир мартали паролларга асосланган аугентфикациялаш тизими масофадаги фойдаланувчиларни текширишда кўлланилади.

Бир мартали паролларни генерациялаш аппарат ёки дастурий усул орқали амалга оширилиши мумкин. Бир мартали пароллар асосидаги фойдаланишнинг аппарат воситалари ташқаридан тўлов пластик карточкаларига ўхшаш микропроцессор ўрнатилганминиатюр курилмалар куринишда амалга оширади. Одатда, калитлар деб аталувчи бундай каргалар клавиатурага ва катта бўлмаган дисплей дарчасига эга.

Фойдаланувчиларни аугентнфикациялаш учун бир мартали паролларни кўллашнинг куйидаги усуллари маълум:

1. Ягона Вақт тизимига асосланган Вақт белгилари механизмидан фойдаланиш
2. Легал фойдаланувчи ва текширувчи учун умумий бўлган гасодифий пароллар руйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланиш.
3. Фойдаланувчи иа текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар гснсраторидан фойдаланиш.

Биринчи усулни амалга ошириш мисоли сифатида SecurlD аутентикациялаш тсхнологиясини кўрсатиш мумкин. Бу технология SecurityDynamics компанияси томонидан ишлаб чиқилган бўлиб. қатор компанияларнинг. хусусан CiscoSystems комианиясининг серверларида амалга оширилган.

Вақт синхронизациясидан фойдаланиб аутентификациялаш схемаси гасодифий сонларни Вақтниш маълум оралиғидан сўнг генерациялаш

алгоритмига асосланган. Аутентификация схемаси қуйидаги иккита параметрдан фойдаланади:

- Хар бир фойдаланувчига аталган аутентификация серверида хамда фойдаланувчининг аппарат калитида сақланувчи ноёб 64-битли сондан иборат махфий калит;
- Жорий вақти қиймати.

Масофадаги фойдаланувчи тармоқдан фойдаланишга уринганида ундан шахсий идентификация рақами PIN НИ киритиш таклиф этилади. PIN тўртта унли рақамдан ва аппарат калити дисплейида аксланувчи тасодифий сопнинг олтита рақамидан иборат. Сервер фойдаланувчи томонидан киригилган PlN-кодцан фойдаланиб маълумотлар базасидаги фойдаланувчининг махфий калити ва жорий вакг қиймати асосида тасодифий сонни генерациялаш алгоритмини бажаради. Сўнгра сервер генерацияланган сон билан фойдаланувчи киритган сонни таққослайди. Агар бу сонлар мос келса, сервер фойдаланувчига тизимдан фойдаланишга рухсат беради.

Аутентификациянинг бу схемасидан фойдаланишда аппарат калиг ва сервернинг катъий Вақтий синхронланиши талаб этилади. Чунки аппарат калит бир неча йил ишлаши ва демак сервер ички соати билан аппарат калитининг мувофиклиги аста-секин бузилиши мумкин.

Ушбу муаммони хал этишда SecurityDynamics компанияси куйидаги икки усулдан фойдаланади:

- аппарат калити ишлаб чиқилаётганида унинг таймер частотасининг меъёридан четлашиши аниқ ўлчанади. Четлашишнинг бу қиймати сервер алгоритми параметри сифатида хисобга олинади;
- сервер муайян аппарат калит генерациялаган кодларни кузатади ва зарурият тугилганида ушбу калитга мослашади.

Аутентификациянинг бу схемаси билан яна бир муаммо боглик. Аппарат калит генерациялаган тасодифий сон катта булмаган Вақт оралиги мобайнида хакикий парол хисобланади. Шу сабабли умуман, киска муддатли вазият содир бўлиши мумкинки, хакер PIN-кодни ушлаб колиши ва уни

тармоқдан фойдаланишга ишлатиши мумкин. Бу Вақт синхронизациясига асосланган аутентификация схемасининг энг заиф жойи хисобланади.

Бир мартали паролдан фойдаланувчи аугентификациялашни амалга оширувчи яна бир вариант - «сўров-жавоб» схемаси буйича аутентификациялаш. Фойдаланувчи тармоқдан фойдаланишга уринганида сервер унга тасодифий сон кўринишидаги сўровни узатади. Фойдаланувчининг аппарат калити бу тасодифий сонни, масалан, DES алгоритми ва фойдаланувчининг аппарат калити хоти- расида ва серверниг маълумотлар базасида сакланувчи махфий калити ёрдамида расшифровка қилади. Тасодифий сон - сўров шифрланган куринишда серверга кайтарилади. Сервер хам ўз навбатида ўша DESалгоритми васервернингмаълумотлар базасидан олинган фойдаланувчининг махфий калити ёрдамида ўзи генерациялаган тасодифий сонни шифрлайди. Сўнгра сервер шифрлаш натижасини аппарат калитидан келган сон билан таққослайди. Бу сонлар мос келганида фойдаланувчи тармоқдан фойдаланишга рухсат олади. Таъкидлаш лозимки, «сўров-жавоб» аутентификациялаш схсмаси ишлатишда вақт синхронизациясидан фойдаланувчи аутентификация схемасига қараганда мураккаброк.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг иккинчи усули фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар руйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланишга асосланган. Бир мартали паролларнинг булинувчи руйхати махфий пароллар кетма-кетлиги ёки тўплами бўлиб, хар бир парол фақат бир марта ишлатилади. Ушбу руйхат аутентификацион алмашинув тарафлар ўртасида олдиндан тақсимланиши шарт. Ушбу усулнинг бир вариантига биноан сўров-жавоб жадвали ишлатилади. Бу жадвалда ау- тентификацилаш учун тарафлар томонидан ишлатилувчи сўровлар ва жавоблар мавжуд бўлиб, хар бир жуфт фақат бир марта ишлатилиши шарт.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан

фойдаланишнинг учинчи усули фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар генераторидан фойдаланишга асосланган. Бу усулни амалга оширишнинг куйидаги вариантлари мавжуд:

- ***узгартирилувчи бир мартини пароллар кетма-кетлиги.*** Навбатдаги аутентификациялаш сессиясида фойдаланувчи айнан шу сессия учун олдинги сессия паролидан олинган махфий калитда шифрланган паролни яратади ва узатади;
- ***бир томонлама функцияга асосланган пароллар кетма-кетлиги.*** Ушбу усулнинг мохиятини бир томонлама функциянинг кетма-кет ишлатилиши (Лампартнинг машхур схемаси) ташкил этади. Хавфсизлик нуқтаи назаридан бу усул кетма-кет ўзгартирилувчи пароллар усулига нисбатан афзал хисобланади.

Кенг таркалган бир мартали паролдан фойдаланишга асосланган аутентификациялаш протоколларидан бири Internetда стандартлаштирилган S/Key (RFC 1760) протоколидир. Ушбу протокол масофадаги фойдаланувчиларнинг хакикийлигини текширишни талаб этувчи кўпгина тизимларда, хусусан, Cisco компаниясининг TACACS+тизимида амалга оширилган.

5-маруза:

Паролни эслаб қолишга асосланган аутентификациялаш усулларининг камчиликлари.

1. Паролга асосланган аутентификациялаш
2. Паролни эслаб қолишга асосланган аутентификациялаш усулларининг камчиликлари

Аутентификациянинг кенг таркалган схемаларидан бири ***оддий аутентификациялаш*** бўлиб, у анъанавий кўп мартали [аролларни ишлатишига асосланган. Тармоқдаги фойдаланувчини оддий аутентификациялаш муолажасини куйидагича тасаввур этиш мумкин. Тармоқдан фойдаланишга уринган фойдаланувчи компьютер клавиатурасида ўзининг идентификатори ва паролини теради. Бу маълумотлар аутентификация серверига ишланиш учун тушади. Аутентификация серверида сакланаётган фойдаланувчи идентификатори буйича маълумотлар базасидан мос ёзув топнлади, ундан паролни гопиб фойдаланувчи киритган парол билан таққосланади. Агар улар мос келса, аутентификация муваффакиятли ўтган хисобланади ва фойдаланувчи легал (конуний) макомини ва авторизация тизими орқали унинг макоми учун аниқланган хукукларни ва тармоқ ресурсларидан фойдаланишга рухсатни олади.

Равшанки, фойдаланувчининг паролини шифрламасдан узатиш орқали аутентификациялаш варианти хавфсизликнинг хатто минимал даражасини кафолатламайди. Паролни химоялаш учун уни химояланмаган канал орқали узатишдан олдин шифрлаш зарур.

Оддий аутентификацияни ташкил этиш нафақат паролларни узатиш, балки уларни сақлаш ва текшириш гурларига ажратади.

Энг кенг тарқалган усул - фойдаланувчилар паролини тизимли файлларда, очиқ холда сақлаш усулидир. Бунда файлларга уқиш ва ёзишдан химоялаш атрибутлари ўрнатилади (масалан, операцион тизимдан фойдаланишни назоратлаш руйхатидаги мос имтиёзларни тавсифлаш ёрдамида). Тизим фойдаланувчи киритган паролни пароллар файлида

сакланаётган езув билан солиштиради. Бу усулда шифрлаш ёки бир томонлама функциялар каби криптографик механизмлар ишлатилмайди. Ушбу усулпинг камчилиги нияти бузуқ одамнинг тизимда маъмур имтиёзларидан, шу билан бирга тизим файлларидан, жумладан, парол файлларпдан фойдаланиш имкониятидир.

Хавфсизлик нуктаи назаридан паролларни бир томонлама функциялардан фойдаланиб узатиш ва сақлаш қулай хисобланади. Бу холда фойдаланувчи паролнинг очиқ шакли ўрнига унинг бир томонлама функция h(.) дан фойдаланиб олинган тасвирини юбориши шарт. Бу узгартириш ғаним томонидан паролни унинг тасвири орқали ошкор қила олмаганлигини кафолатлайди. чунки ғаним ечилмайдиган сонли масалага дуч келади.

Кўп мартали паролларга асосланган оддий аутентификациялаш тизимининг бардошлиги паст, чунки уларда аутентификацияловчи ахборот маъноли сўзларнинг нисбатан катта бўлмаган тўпламидан жамланади. Кўп мартали паролларнинг таъсир муддати ташкилотнинг хавфсизлиги сиёсатида белгиланиши ва бундай паролларни мунтазам равишда алмаштириб туриш лозим. Паролларни шундай танлаш лозимки, улар луғатда булмасин ва уларни гопиш кийин бўлсин.

6-маруза:

Биометрик характеристикаларга асосланган идентификация ва аутентификация.

1. Биометрик аутентификация
2. Биометрик характеристикаларга асосланган аутентификациялаш

Ҳозирги вақтга келиб, ахборот -коммуникация технологиялари кундан-кунга тез ривожланиб бормоқда. Шу сабабли ҳам компютер технологиялари кириб бормаган соҳанинг ўзи қолмади, десак хато бўлмайди. Айниқса таълим, банк, молия тизимларида ушбу замонавий технологияларни қўллаш юқори самара бермоқда. Шу билан бирга ахборот ҳавфсизлигига бўлган таҳдид ҳам тобора кучайиб бораётгани ҳеч кимга сир эмас. Демак, ҳозирги даврнинг энг долзарб муаммолардан бири ахборот ҳавфсизлигини таъминлашдан иборат.

Ҳозирга қадар тизимга рухсациз киришни тақиқлашнинг энг кенг тарқалган усули сифатида «парол» қўйиш принципи ҳисобланиб келмоқда. Чунки ушбу усул жуда содда, фойдаланиш учун қулай ва кам ҳаражат талаб этади. Лекин, ҳозирга келиб «парол» тизими тўлақонли ўзини оқлай олмаяпти. Яъни ушбу усулнинг бир қатор камчиликлари кўзга ташланиб қолди.

Биринчидан, кўпчилик фойдаланувчилар содда ва тез эсга тушадиган паролларни қўллайдилар. Масалан, фойдаланувчи ўз шахсига оид саналар, номлардан келиб чиққан ҳолда парол қўядилар. Бундай паролларни бўзиш эса, фойдаланувчи билан таниш бўлган ихтиёрий шахс учун унчалик қийинчилик туғдирмайди.

Иккинчидан, фойдаланувчи паролни киритиши жараёнида, кузатиш орқали ҳам киритилаётган белгиларни илғаб олиш мумкин.

Учинчидан, агар фойдаланувчи парол қўйишда мураккаб, узундан-узоқ белгилардан фойдаланадиган бўлса, унинг ўзи ҳам ушбу паролни эсидан чиқариб қўйиши эхтимолдан ҳоли эмас ва ниҳоят, ҳозирда ихтиёрий паролларни бузувчи дастурларнинг мавжудлиги кўзга ташланиб қолди.

Юқоридаги камчиликлардан келиб чиққан ҳолда айтиш мумкинки, ахборотниҳимоялашнинг паролли принципидан фойдаланиш тўла самара бермаяпти. Шу сабабли ҳам ҳозирда ахборотлардан рухсациз фойдаланишни чеклашнинг биометрик усулларини қўллаш дунё бўйича оммавийлашиб бормоқда ва ушбу йўналиш биометрия номи билан юритилмоқда.

Биометрия – бу инсоннинг ўзгармайдиган биологик белгиларига асосан айнан ўхшашликка текширишдир (идентификация). Ҳозирда биометрик тизимлар энг ишончли ҳимоя воситаси ҳисобланади ва турли хил махфий объектларда, муҳим тижорат ахборотларини ҳимоялашда самарали қўлланилмоқда.

Ҳозирда биометрик технологиялар инсоннинг қуйидаги ўзгармас биологик белгиларига асосланган:

1. Бармоқ изи орқали;
2. Юзнинг геометрик ўлчамлари орқали;
3. Кўз ёйи ва кўз тўр пардаси орқали;
4. Овоз орқали;

Фойдаланувчиларни биометрик аутентификациялаш

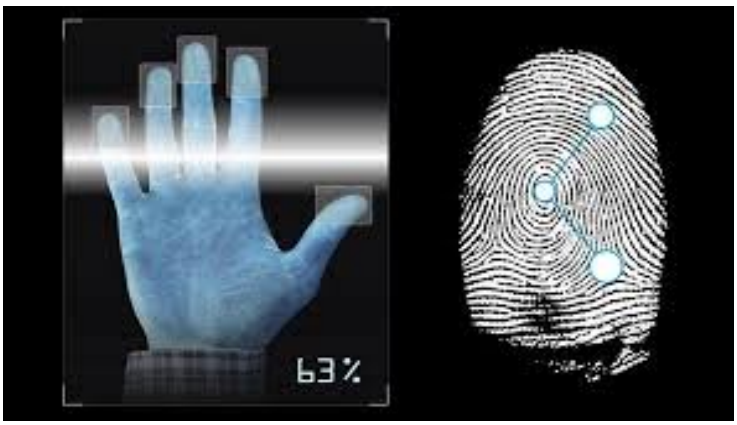
Фойдаланувчиларни биометрик аутентификациялаш корхона ташкилотнинг қай даражада махфийлиги хавфсизлиги жиҳатдан ва унинг иқтисод томонлама қанчалик қониқтира олишига қараб биометрик аутентификация қилиш усуллари танланади. Хавфсизлик жиҳатидан биометрик аутентифктасиялаш усуллари юқори даражали ҳиоблангани боис уни давлат миқёсида оммалаштириш ички ва ташқи таьсирларни бир хил ушлашга ёрдам беради. Биометрик аутентификациялаш усулларини муассасаларда қо`ллаётган пайтда фойдаланувчи белгиларининг натижалари фақат “ҲА” ёки “ЁҚ” натижалари билан амалга оширилади. ”ҲА” натижаси асосида фойдаланувчи муссасага кириши мумкин, агарда унинг белгиларида ўзгариш бўладиган бўлса ёки бошқа шахс бўлса “ЁҚ” натижа ёки биометрик эшик очилмаслигидан билиш мумкин.

Бармоқ излари ёрдамида аутентификациялаш.

“Бармоқ излари буйича инсонни идетификациялаш” ҳозирда энг кенг тарқалган усул бўлиб, ахборотни ҳимоялаш биометрик тизимларида кенг қўлланилмоқда. Бу усул ўтган асрларда ҳам кенг қўлланилганлиги хеч кимга янгилик эмас. Ҳозирги кунга келиб бармоқ излари бўйича идентификациялашнинг учта асосий технологияси мавжуд. Уларнинг биринчиси кўпчиликка маълум оптик сканерлардан фойдаланишдир. Ушбу қурилмадан фойдаланиш принципи одатий сканердан фойдаланиш билан бир хил. Бу эрда асосий ишни ички нур манбаи, бир нечта призма ва линзалар амалга оширади. Оптик сканерларни қўллашнинг эътиборли томони унинг арзонлигидир. Лекин, камчилик томонлари бир мунча кўп. Ушбу қурилмалар тез ишдан чиқувчи ҳисобланади. Чу сабабли фойдаланувчидан авайлаб ишлатиш талаб этилади. Ушбу қурилмага тушган чанг, турли хил чизиқлар шахсни аниқлашда хатоликка олиб келади, яъни фойдаланувчининг тизимга киришига тўсқинлик қилади. Бундан ташқари, оптик сканерда тасвири олинган бармоқ изи фойдаланувчи терисининг ҳолатига боғлиқ. Яъни, фойдаланувчи терисининг ёғлилиги ёки қуруқлиги шахсни аниқлашга халақит беради.

Бармоқ излари бўйича идентификациялашнинг иккинчи технологияси электрон сканерларни қўллашдир. Ушбу қурилмадан фойдаланиш учун фойдаланувчи 90 минг конденсатор пластинкаларидан ташкил топган, кремний моддаси билан қопланган маҳсус пластинкага бармоғини қўяди. Бунда ўзига хос конденсатор ҳосил қилинади.

Биометрик аутентификациялаш тизимларнинг ичида энг кўп ва оммавий тарқалгани бармоқ ёрдамида идентификациялаш ва уни



аутентификациялаш. Бу тизим биометрик аутентификация қилишда “Дактилоскопик” усули деб айтилади.

1-расм. Бармоқ изини ссанерлаш.

Бугунги кунда 3 хил бармоқ изларини олиш технологияси бор улар қуйидагича:

-ултратовушлар ёрдамида ;

-оптик нурлар ёрдамида (фтир);

-ярим о`тказгич ёрдамида;

Бармоқ изларининг сканерлари. Бармоқ изларини сканерловчи ан`анавий қурилмаларда асосий элемент сифатида бармоқнинг характерли расмини ёзувчи кичкина оптик камера ишлатилади.

2-расм. Бармоқ изини сканерлаш аппарат қурилмаси.

Биометрик аутентификация қилиш тизимининг аппарат қурилмалари орасида энг ишончли ҳамда оммабоплиги билан ажралиб турадигани “БИОЛИНК” компониясининг биометрик аутентификация қилиш аппарат қурилмасидир.

Бармоқ изларини сканерлашда ишлатиладиган дактилоскоп қурилмаларини ишлаб чиқарувчиларнинг кўп қисми асосан интерграл схемаларда фойдаланмоқда. Бундай технологияларни ишлаб чиқарувчи компаниялар бармоқ изларини олишда хар хил турдаги электрик, электромагнит ва бошқа усуллар орқали амалга оширадилар. Бунинг асосий сабаби бармоқ изини олиш вақтида тери қисмларининг сиғим қаршилиги олинади ва таҳлил қилинади. Таҳлил вақтида Дактилоскопик қурилмаси эса яримо`тказгичли датчик орқали сиг`им қаршилигини аниқлаш мақсадида барча ахборотларни йиғилади.

Юзнинг тўзилиши бўйича аутентификацияловчи тизимлар.

Юзнинг тўзилиши бўйича аутентификация қилиш ҳамма тамонлама яьни арзон ва барча компютерларнинг видео хусусиятга эга эканлиги боис бу тизим ҳамма жойда ишлатила олиши билан фарқ қилади. Бу тизим асосан масофавий идентификация қилиш вақтида ишлатилади. Қуйида (3-расм) даги нуқталар асосида юзнинг ўлчамлари ҳисобланади. Ушбу нуқталар юзнинг семирганини ҳисобига ҳам ўзгариб туради. Аммо юз семирган пайтда ҳам озган пайтда ҳам унинг тузулиши геометрик ўлчамлари ва бурчаги ўзгармайди. Шу боис бу тизим энг ишончлиларидан бири ҳисобланади. Бунда унинг қуйидаги нуқталари ўлчамлари олинади:

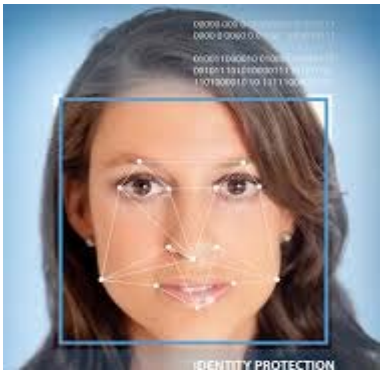
-лаб тўзилиши унинг бурчаги ;

-бурун учи ва ўлчамлари ;

-кўзнинг маркази ва кўз бурчаги ;

Бунда унинг ўлчамлари маьлумотлар омборидаги шахсларнинг ўлчамлари билан солиштирилиб унинг ҳақиқатда муассасада ишлайдиган

шахс ёки шахс эмаслигини кўрсатади. Аммо бу тизимга ҳалақит берадиган омиллар ҳам йетарли: Кўзойнак, соқол, юзга безак бериш кабилар.



3-расм. Юз тўзилиши бўйича аутентификациялаш.

Расмдаги ҳолатда асосан кўз, бурун лаб ўлчамлари олинади ва идентификацияланади. Юз тўзилишини аниқловчи қурилмаларни ишлаб чиқарувчилар фойдаланувчини идентификациялашда хусусий математик алгоритмлардан фойдаланадилар.

Кўз тўр пардаси ёрдамида аутентификациялаш.

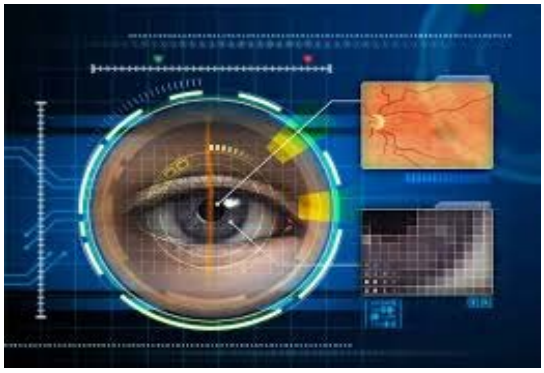
Кўз тўр пардаси ёрдамида аутентификациялаш усули асосан икки хил тартибда амалга оширилади.

1. Кўз ёйи ;
2. Кўз тўр пардаси қон томирлари жойлашув ўрни ;

Кўз ёйи ёрдамида аутентификациялаш асосан кўз ёйининг радиуси ва унинг ўлчамлари билан аутентификацияланади. Қуйидаги расмда кўз ёйи радиуси ва унинг жойлашган ўрни ўлчамлари олинган ҳолда аутентификация қилиш усули кўрсатилган.

4-расм. Кўз ёйи ёрдамида аутентификациялаш.

Кўз ёйи ёрдамида аутентифктасия қилишда анча мураккаб ва сезиларли даражада вақтни олиши қон томирлар билан ишлаш вақтида кўзнинг



юмилиш ҳолатлари аутентификациялаш жараёнида бир қанча муаммолар келтириб чиқаради.

5-расм. Кўз тўр пардаси ёрдамида аутентификациялаш.

Ушбу биометрик аутентификациялаш усули хавфсизлик жиҳатдан энг юқори даражада ҳисобланади. Шу биосдан бу биометрик аутентификациялаш усули давлатларнинг юқори даражада хавфсизлиги таьминланиши зарур бўлган идораларга қўйилади.

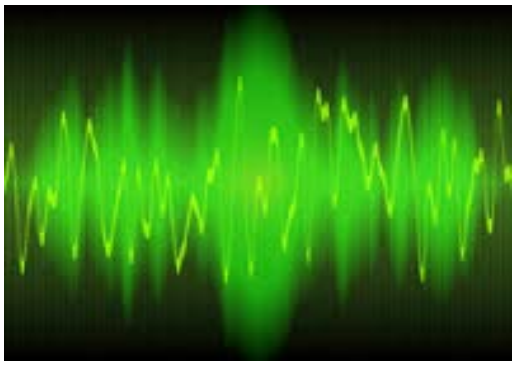
6-расм. Кўзни биометрик аутентификациялашнинг аппарат қурилмаси.

Биолинк компанияси томонидан ишлаб чиқилган кўз ёрдамида аутентификациялашнинг аппарат қурилмаси.

Кўз тўр пардасидаги томирларнинг жойлашуви ҳаттоки эгизакларда жуда катта фарқ қилиниши аниқланган. Аммо кўз айланаси қанчадир шахсда бир-бирига ўхшаш бўлганлиги сабабли кўпинча кўз пардасидан фойдаланилади.

Овоз бўйича аутентификациялаш тизимлари

Бу тизимларни ҳамма мултимедиага эга бўлган компютерлар асосида амалга ошириш мумкин. Шу сабабли бу биометрик тизимлар арзонлиги тарафи билан бошқа биометрик тизимлардан ажралиб туради. Бу тизимни ишлатиш учун микрофон йетарли. Бу тизим шахснинг товуш частотасига асосланиб ишлайди.



7-расм. Овоз ёрдамида аутентификациялаш.

Ушбу биометрик аутентификациялаш усули асосан, замонавий бизнес марказлари ишлатилади ва айни пайтда бу технология, жадал ривожланмоқда. Овоз билан бир андозани қуришнинг кўп йўллари бор. Одатда, бу усул частота ва унинг турли тўзилмалари ва овозли статистик хусусиятларга эга. Шу биосдан унинг муаммо томони бир кишининг овози хилма: овозли саломатлиги, ёши, кайфият ва ҳоказо ҳолига қараб фарқ қилиши мумкин. Ушбу хилма-хиллик, инсон овози ўзига хос хусусиятлари ажратиш жиддий қийинчиликлар тўлдиради. Бундан ташқари, шовқин ҳам овоз билан амалий фойдаланиш аутентификация қилиш вақтида яна бир муҳим ва ҳал этилмаган муаммо ҳисобланади.

7-маруза:

Биометрик характеристикаларга асосланган идентификация ва аутентификациялашнинг камчиликлари.

1. Биометрик характеристикаларга асосланган аутентификациялаш
2. Биометрик характеристикаларга асосланган аутентификациялашнинг камчиликлари

Охирги Вақтда инсоннинг физиологик параметрлари ва характеристикаларини, хулкининг хусусиятларини улчаш орқали фойдаланувчини ишончли аутентификациялашга имкон берувчи биометрик аутентификациялаш кенг тарқалмокда.

Биометрик аутентификациялаш усуллари аньанавий усулларга нисбатан куйидаги афзалликларга эга:

- биометрик аломатларни ноёблиги туфайли аутентификациялашнинг ишончлилик даражаси юқори;
- биометрик аломатларнинг ишга лаёкатли шахсдан ажратиб булмаслиги;
- биометрик аломатларни сохталаштиришнинг кийинлиги.

Фойдаланувчини аутентификациялашда фаол ишлатиладиган биометрик аломатлари куйидагилар:

- бармоқ излари;
- қўл панжасининг геометрик шакли;
- юзнинг шакли ва улчамлари;
- овоз хусусиятлари;
- куз ёйи ва тур пардасининг нақши.
- Аутентификациянинг биометрик тизими ишлашининг намунавий схемаси куйидагича. Тизимда руйхатга олинишида фойдаланувчидан ўзининг характерли аломатларини бир ёки бир неча марта намойиш килиниши талаб этилади. Бу аломатлар (хакикий сифатида маълум) тизим томонидан конуний фойдаланувчининг киёфаси сифатида руйхатга олинади. Фойдаланувчининг бу киёфаси тизимда электрон шаклда сакланади ва ўзини

конуний фойдаланувчи деб даъво килган хар бир одамни гекширишда ишлатилади. Тақдим этилган аломатлар мажмуаси билан руйхатга олинганларининг мослиги ёки мос келмаслигига караб карор кабул килинади. Истеъмолчи нуқтаи назаридан биометрик аутенфикациялаш тизими куйидаги иккита параметр орқали харак- терланади:

- хатолик инкорлар коэффициента FRR (false-rejectrate);
- хатолик тасдиклар коэффициента FAR (false-alarmrate).

Хатолик инкор тизим конуний фойдаланувчи шахсинитасдикламаганда пайдо бўлади (одатда FRR қиймати гахминан 100 дан бирни ташкил этади). *Хатолик тасдщ* тизим ноконуний фойдаланувчи шахсини тасдиклаганида пайдо бўлади (одатда, FAP қиймати тахминан 10000 дан бирни ташкил этади). Бу иккала коэффициент бир бири билан боглик: хатолик инкор коэффициентининг хар бирига маълум хатолик тасдик коэффициента мос келади. Мукаммал биометрик тизимда иккала хатоликнинг иккала параметри нолга тенг бўлиши шарт. Афсуски, биометрик тизим идеал эмас, шу сабабли ниманидур курбон қилишга тугри келади. Одатда, тизимли параметрлар шундай созланадики, мос хатолик инкорлар коэффициентини аниқловчи хатолик тасдикларнинг исталган коэффициентига эришилади.

Биометрик аутентификациялашнинг дактилоскопиктизими

Биометрик тизимларнинг аксарияти идентификациялаш параметри сифатида бармоқ изларидан фойдаланади (аугентификациянинг дактилоскопик тизими).

Бармоқ изларидан фойдаланишни афзалликлари:

- бундай тизимлар содда ва қулай; аутентификациялашнинг юқори ишончлилигига эга.
- бундай тизимларнинг кенг таркалишига асосий сабаб бармоқ излари буйича катта маълумотлар баъзасининг мавжудлигидир.

Юқоридаги қурилмалар тез ишдан чиқувчи ҳисобланади. Шу сабабли фойдаланувчидан авайлаб ишлатиш талаб этилади. Ушбу қурилмага тушган чанг, турли хил чизиқлар шахсни аниқлашда хатоликка олиб келади, яъни

фойдаланувчининг тизимга киришига тўсқинлик қилади. Бундан ташқари, оптик сканерда тасвири олинган бармоқ изи фойдаланувчи терисининг ҳолатига боғлиқ. Яъни, фойдаланувчи терисининг ёғлилиги ёки қуруқлиги шахсни аниқлашга халақит беради.

Қўлпанжасининг геометрик шакли буйича аутентификациялаштизимларини камчиликлари:

Қўл панжасини сканерловчи курилмалар нархининг юкорилиги ва улчамларининг катталиги сабабли тармоқ мухитида камдан-кам ишлатилсада,

Юзнинг тўзилиши ва овоз буйича аутентификацияловчи тизимларАфзалликлари:

Бу тизимлар арзонлиги туфайли энг фойдаланувчан хисобланадилар. чунки аксарият замонавий компьютерлар видео ва аудео воситаларига эга.

Камчиликлари ***:***

Юз тўзилишини аниқловчи курилмаларни ишлаб чиқарувчилар фойдаланувчини идентификациялашда хусусий математик алгоритмлардан фойдаланадилар ва бунда бизга маълумки инсон ташқи қиёфасида турли ўзгаришлар бўлиш табиий хол бу ўзгаришлар яъни юз қисмидаги ўзгаришлар идентификация ва аутентификация жараёнларида мофаққиятли ўтишга қаршилик кўрсатади.

Овоз буйича аутентификациялаш тизимлар

Афзаллиги:

- бу тизимлар арзонлиги туфайли фойдаланувчан хисобланганлиги.
- хусусан уларни кўпгина шахсий компьютерлар стандарт комплектидаги ускуна (масалан, микрофонлар) билан бирга урнагиш мумкин.

Камчиликлари***:***

- турли одамлар ўхшаш овозлар билан гапириши мумкин, хар қандай одамнинг овози вақт мобайнида кайфияти, чиссиётлик холати ва ёшига боғлиқ холда ўзгариши мумкин ва бу ўзгаришлар идентификация ва

аутентификация жараёнларида мофаққиятли ўтишга қаршилик кўрсатади.

Куз ёйи тур пардасининг шакли буйича аутентификациялаш тизимини

Афзаллиги:

- Хавфсизликюкори даражада таъминланганлиги

Камчиликлари*:*

- фойданиладиган технологиялари нархи юқорилиги хисобланади.
- Қуйидаги жадвалда биометрик аутентификациялаш тизимлариги хужум қилишнинг маълум усуллари ва бундай хужумардан ҳимоя усуллари кўрсатилган.

Ҳуужумнинг таъифи	Ушбу хужумдан ҳимоя
Аҳамиятли хусусиятни сохталаштириш.	
Тажовузкор қонуний фойдаланувчининг физик фарқлаш хусусиятидан нусха олади ва ушбу нусхани биометрик сенсорга тақди этади.	Кўрсаткичларни юқори даражада аниқланган ҳолда олиб ташлаш. Маълумот шаблонини илаб чиқаришда қонуний фойдаланувси томонидан қўшимча биометрик кўрсаткичлар олиб ташланади, шунинг учун қонуний фойдаланувчи физик хусусиятининг барча параметрларини акс эттирмайди.
Фойдаланувчи харакатларини такрорлаш.	
Тажовухкор фойдаланувчининг хатти-ҳаракати билан ажралиб турадиган хусусиятни ёзади ва биометрик сенсорда қайти ишлайди.	Ўзгаришларни ўзгартириш. Аутентификация қилишда ҳар бир ташаббус билан, тизим фойдаланувчи биометрик характеристикасининг ўзига хос намоён бўлишини талаб қилади, шунинг учун оддий рўйхатга олиш ва ижро этиш талаб қилинмайди.
Биометрик кўрсаткичларни сақлаб қолиш.	
Тажовузкор қурилмалар ўртасида маълумотлар узатиш вақтида қонуний фойдаланувчи биометрик кўрсаткичларини ушлаб қолади.	Биоетрик аълумотларни шифрлаш. Биомтрик маълумотлар фойдалнувчи томонида тақдим этилгандан сўнг дарҳол шифрланади, уларнинг қурилмалари ўртасида алмашиниш фақат шифрланган шаклда амалга ошириладию.
Биометрик имзони кўпайтириш.	
Тажовузкор биометрик сенсорнинг кўрсаткичини яъни имзони такрорлайди. Бу кўрсаткич тизим томонидай ҳақиқий шахсдан оинганидек қайта ишланади.	Биометрик имзонинг ҳақиқийлигини текшириш. Аутентификация қилиш чоралари биометрик маълумотлар бўйича олинади, бу уларнинг ишончли манбаалардан олинганлигини кафолатлайди. Биметрик имзонинг бутунлигини таъминлаш учун электрон рақамли имзодан фойдаланиш.

8-маруза:
Авторизация ҳамда электрон хужжатларнинг юридик мақомини ҳимоялаш.

1. ЭРИ ни криптография соҳасига тегишли стандартлари.
2. ЭРИ ни шакллантириш ҳамда текшириш жараёни

Жисмоний ёки юридик шахслар ўртасида ўзаро маълумот алмашув жараёнида авторизация масаласи ҳамда электрон хужжатларнинг юридик мақомини ҳимоялаш мақсадида ЭРИ жорий қилинган. ЭРИ ни шакллантириш ҳамда текшириш алгоритми криптография соҳасига тегишли стандартларга асосланган.

- ***ГОСТ Р 34.10-94.*** "Ахборот технологиялари. Ахборотни криптографик ҳимоялаш. Асимметрик криптографик алгоритмлар базасига асосланган ҳолда ЭРИ ни текшириш ҳамда шакллантириш"(Ушбу стандарт 31.12.2007 гача тан олинган). Ушбу стандартда криптографияда экспоненциал мантиққа асосланган ҳолда ЭРИ ни шакллантириш ва текшириш кетма-кетлиги келтирилган.
- ***ГОСТ Р 34.10-2001.*** "Ахборот технологиялари. Ахборотни криптографик ҳимоялаш. ЭРИ ни шакллантириш ҳамда текшириш жараёни". Ушбу стандартга кўра ЭРИ ни шакллантириш ҳамда текшириш криптографиянинг эллиптик эгри чизиққа асосланган бўлимига асосланган.
- ***ГОСТ Р 34.11-94.*** "Ахборот технологиялари. Ахборотни криптографик ҳимоялаш. Хешлаш функцияси." Ушбу стандартда имзоланадиган маълумотларни хешлаш жараёни келтирилган.

ЭРИ ни шакллантириш ҳамда текшириш жараёни

Қуйдаги модификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш каби алоқа тизими қоидаларининг бузилишини олдини олиш мақсадида рақамли сигнатурадан – рақамли имзо ва узатиладиган маълумотнинг бирор қисмини тўла ўз ичига олувчи рақамли шифрматндан иборат бўлган маълумотдан фойдаланилади.

Такрорлаш- Фойдаланувчи (В) фойдаланувчи (А) томонидан

фойдаланувчи (Б)га жўнатилган маълумотни такроран (Б)га жўнатади. Бундай ноқонуний хаттиҳаракат алоқа усулидан банклар тармоқларида электирон ҳисоб–китоб тизимидан фойдаланишда ноқонунийлик билан ўзгалар пулларини талон-тарож қилишда фойдаланилади. Ана шундай ноқонуний усуллардан муҳофазаланиш учун қуйидаги чора - тадбирлари кўрилади.

криптотизимга кираётган маълумотларни муҳофаза мақсадларидан келиб чиқиб тартиблаш.

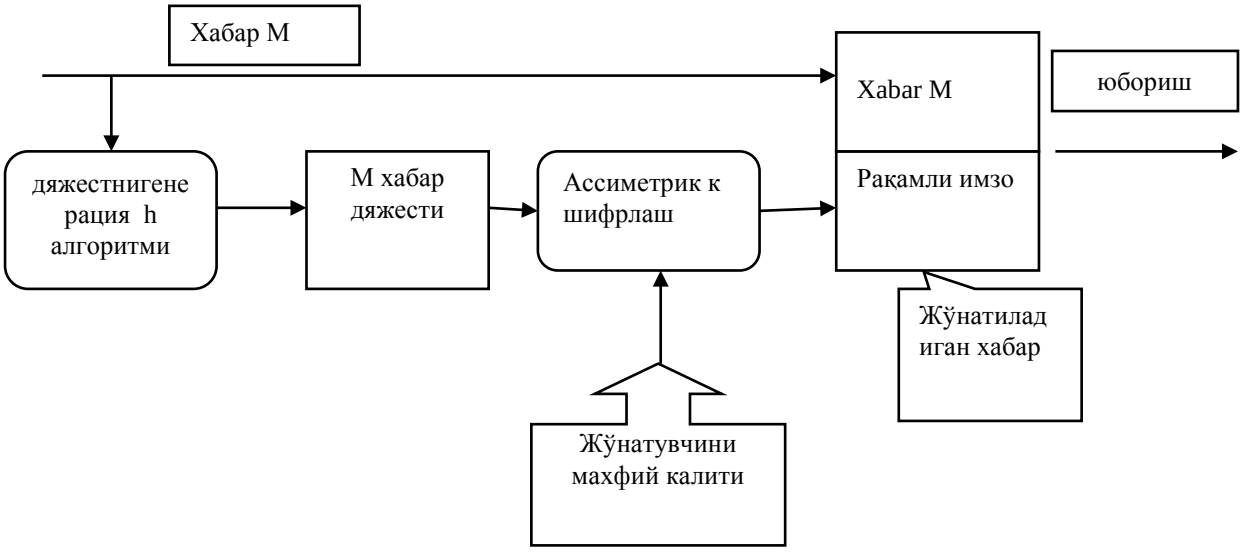
- Електрон рақамли имзо алоқа тизимларида бир неча тур қоида бузилишларидан муҳофаза қилинишни таъминлайди, яъни махфий калит фақат фойдаланувчи (А)нинг ўзигагина маълум бўлса, у ҳолда фойдаланувчи (Б) томонидан қабул қилиб олинган маълумотни фақат (А) томонидан жўнатилганлигини рад этиб бўлмайди
- қонун бузар (рақиб томон) махфий калитни билмаган ҳолда модификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш ва бошқа шу каби алоқа тизими қоидаларининг бузилишига имконият туғдирмайди
- алоқа тизимидан фойдаланувчиларнинг ўзаро боғлиқ ҳолда иш юритиши муносабатидаги кўплаб келишмовчиликларни бартараф этади ва бундай келишмовчиликлар келиб чиққанда воситачисиз аниқлик киритиш имконияти туғилади.

Кўп ҳолларда узтилаётган маълумотларни шифрлашга ҳожат бўлмай, уни электрон рақамли имзо билан тасдиқлаш керак бўлади. Бундай ҳолатларда очиқ матн жўнатувчининг ёпиқ калити билан шифрланиб, олинган шифрматн очиқ матн билан бирга жўнатилади. Маълумотни қабул қилиб олган томон жўнатувчининг очиқ калити ёрдамида шифрматнни дешифрлаб, очиқ матн билан солиштириши мумкин.

Рақамли имзони шакллантириш муолажаси: Ушбу муолажани тайёрлаш босқичида хабар жўнатувчи абонент А иккита калитни генерациялайди: махфий калит А ва очиқ калит А очиқ калит А унинг жуфти

бўлган махфий калити А ҳисоблаш орқали олинади. Очиқ калит А тармоқнинг бошқа абонентларига имзони текширишда фойдаланиш учун тарқатилади.

Рақамли имзони шакллантириш учун жўнатувчи А аввало имзо чекилувчи матн М нинг хеш функсияси Л(М) қийматини ҳисоблайди (1-расм). Хеш-функсия имзо чекилувчи дастлабки матн “М” ни дайджест “м”га зичлаштиришга хизмат қилади. Дайджест М бутун матн “М” ни характерловчи битларнинг белгиланган катта бўлмаган сонидан иборат нисбатан қисқа сондир. Сўнгра жўнатувчи А ўзининг махфий калити кА билан дайджест “м” ни шифрлайди. Натижада олинган сонлар жуфти берилган “М”матн учун рақамли имзо ҳисобланади. Хабар “М” рақамли имзо билан биргаликда қабул қилувчининг адресига юборилади.

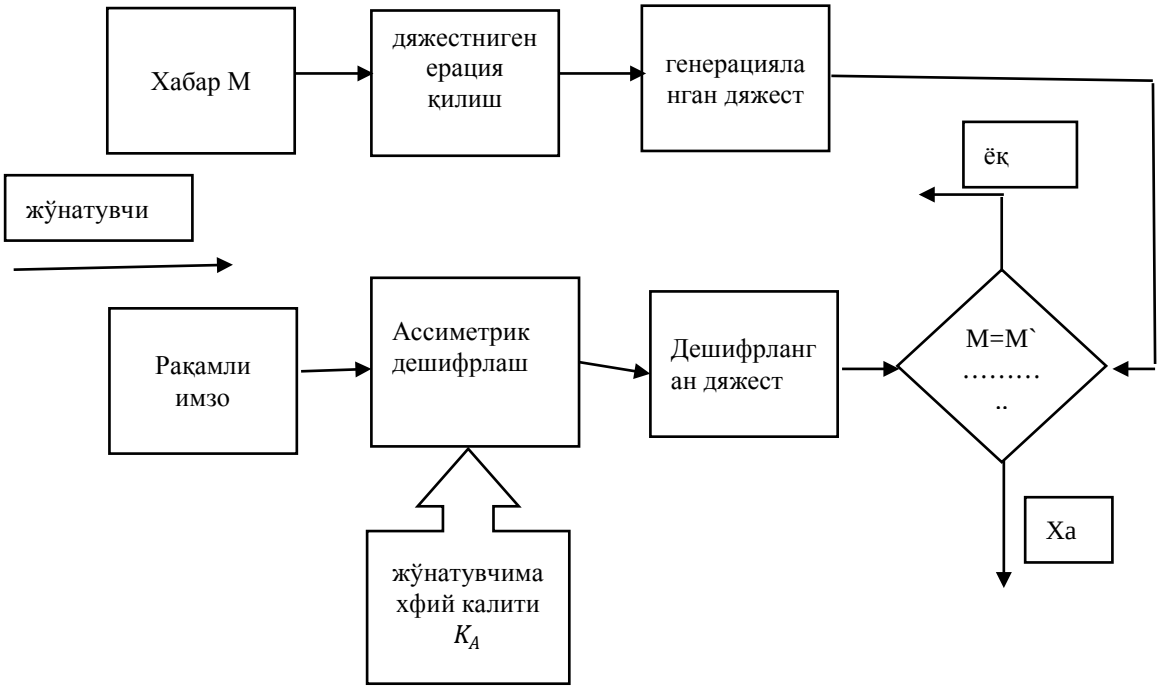


1–расм. Электрон рақамли имзони шакллантириш схемаси.

Рақамли имзони текшириш муолажаси: Тармоқ абонентлари олинган хабар “М”нинг рақамли имзосини ушбу хабарни жўнатувчининг очиқ калити КА ёрдамида текширишлари мумкин Электрон рақамли имзони текширишда хабар “М” ни қабул қилувчи “Б” қабул қилинган дайджестни жўнатувчининг очиқ калити “КА” ёрдамида расшифровка қилади. Ундан ташқари, қабул қилувчини ўзи хеш функсия х(М) ёрдамида қабул қилинган хабар “М” нинг

дайджести “м” ни ҳисоблайди ва уни расшифровка қилингани билан таққослайди. Агар иккала дайджест “м” ва “мъ” мос келса рақамли имзо ҳақиқий ҳисобланади. Акс ҳолда имзо қалбакилаштирилган, ёки ахборот мазмуни ўзгартирилган бўлади. Ҳар бир имзо қуйидаги ахборотни ўз ичига олади:

- имзо чекилган сана ;
- ушбу имзо калити таъсирининг тугаши муддати ;
- файлга имзо чекувчи шахс хусусидаги ахборот (ф. и. ш, мансаби, иш жойи) ;
- имзо чекувчининг индентификатори (очиқ калит номи) ;
- рақамли имзонинг ўзи.



2–расм. Электрон рақамли имзони текшириш схемаси.

ЭРИ ахборот коммуникация тармоғида электрон ҳужжат алмашинуви жараёнида қуйидаги учта масалани йечиш имконини беради:

- електрон ҳужжат манбаининг ҳақиқийлигини аниқлаш ;
- електрон ҳужжат яхлитлигини (ўзгармаганлигини) текшириш ;

- электрон ҳужжатга рақамли имзо қўйган субъектни муаллифликдан бош тортмаслигини таъминлайди.

9-маруза:

Очиқ калитга асосланган сертификатлар ёрдамида аутентификациялаш.

1. Сертификатлар асосида аутентификациялаш
2. Очиқ калитларнинг сертификатлар билан узвий боғлиқлиги

Тармоқдан фойдаланувчилар сони миллионлаб ўлчанганида фойдаланувчилар паролларининг тайинланиши ва сақланиши билан боғлиқ фойдаланувчиларни дастлабки руйхатга олиш муолажаси жуда катта ва амалга оширилиши кийин бўлади. Бундай шароитда рақамли сертификатлар асосидаги аутентификациялаш пароллар қўлланишига рационал альтернатива хисобланади.

Рақамли сертификатлар ишлатилганида компьютер тармоғи фойдаланувчилар хусусидаги хеч қандай ахборотни сақламайди. Бундай ахборотни фойдаланувчиларнинг ўзи сўров-сертификат- ларида тавдим этадилар. Бунда махфий ахборотни, хусусан махфий калитларни сақлаш вазифаси фойдаланувчиларнинг ўзига юкланади.

Фойдаланувчи шахсини тасдикловчи рақамли сертификатлар фойдаланувчилар сўрови буйича махсус ваколатли ташкилот- сертификация маркази С А (CertificateAuthority) томонидан, маълум шартлар бажарилганида берилади. Таъкидлаш лозимки, сертификат олиш муолажасининг ўзи хам фойдаланувчининг хакикийлигини текшириш (яъни, аугентификадиялаш) боскичини ўз ичига олади. Бунда текширувчи тараф сертификацияловчи ташкилот (сертификация маркази СА) бўлади.

Сертификат олиш учун мижоз сертификация марказига шахсини тасдикловчи маълумотни ва очиқ калитини такдим этиши лозим. Зарурий маълумотлар руйхати олинадиган сертификат турига боглик. Сертификацияловчи ташкилот фойдаланувчининг хакикий-лиги тасдиғини текширганидан сўнг ўзининг рақамли имзосини очиқ калит ва фойдаланувчи хусусидаги маълумот бўлган файлга жойлаштиради хамда ушбу очиқ калитнинг муайян шахсга тегишли эканлигини тасдиклаган холда

фойдаланувчига сертификат беради.

Сертификат электрон шакл бўлиб, таркибида куйидаги ахборот бўлади:

- ушбу сертификат эгасининг очиқ калити;
- сертификат эгаси хусусидаги маълумот, масалан, исми, электрон почта манзили, ишлайдиган ташкилот номи ва х.;
- ушбу сертификатни берган ташкилот номи;
- сертификацияловчи ташкилотнинг электрон имзоси - ушбу ташкилотнинг махфий калити ёрдамида шифрланган сертификациядаги маълумотлар.

Сертификат фойдаланувчини тармоқ ресурсларига мурожаат этганида аутентификацияловчи восита хисобланади. Бунда текширувчи тараф вазифасини корпоратив тармоқнинг аутентификация сервери бажаради. Сертификатлар нафақат аутен гификациялашда, балки фойдаланишнинг маълум хукукларини такдим этишда ишлатилиши мумкин. Бунинг учун сергификатга кушимча хошиялар киритилиб уларда сертификация эгасининг фойдаланувчиларнинг у ёки бу категориясига мансублиги к>фсатилади.

Очиқ калитларнинг сертификатлар билан узвий богликлигини алохида таъкидлаш лозим. Сертификат нафақат шахсни, балки очиқ калит мансублигини тасдикловчи хужжатдир. Рақамли сертификат очиқ калит ва унинг эгаси ўртасидаги мосликни ўрнаеади ва кафолатлайди. Бу очиқ калитни алмаштириш хавфини бартараф этади.

Агар абонент ахборот алмашинуви буйича шеригидан сертификат таркибидаги очиқ калитни олса, у бу сертификагдаги сертификация марказининг рақамли имзосини ушбу сертификация марказининг очиқ калити ёрдамида текшириши ва очиқ калиг манзили ва бошқа маълумотлари сертификатда курсатилгаи фойдаланувчига тегишли эканлигига ишонч хосил қилиши мумкин. Сертификатлардан фойдаланилганда фойдаланувчилар руйхатини уларнинг пароллари билан корпорация серверларида сақлаш зарурияти йуколади. Серверда сертификацияловчн гашкилотларнинг номлари ва очиқ калитларининг бўлиши егарли.

Сертификатларнинг ишлатилиши сертификацияловчн гашкилотларнинг нисбатан камлигига ва уларнинг очиқ калитларидан кизиккан барча шахслар ва ташкилотлар фойдалана олиши (масалан, журналлардаги нашрлар ёрдамида) гахминига асосланган.

Сертификатлар асосида аугентификациялаш жараснини амалга оширишда сертификацияловчн ташкилот вазнфаеннн ким бажариши хусусидаги масалани ечиш мухим хисобланади. Ходимларни сертификат билан таъминлаш масаласини корхонанинг ўзи ечиши жуда табиий хисобланади. Корхона ўзининг ходимларини яхши билади ва улар шахсини тасдиклаш вазифасини ўзига олиши мумкин. Бу сертификат берилишндагн дастлабки аугентификациялаш муолажасини осоплаштиради. Корхоналар сертификатларни генерациялаш, бериш ва уларга хизмат кўрсатиш жараёнларини автоматлаштиришни таъ.минловчи мавжуд дастурий махсулотлардан фойдаланишлари мумкин. Масалан, NetscapeCommunications компанияси серверларини корхоналарга шахсий сертификатларини чиқариш учун таклиф этади.

Сертификацияловчн ташкилот вазифасини бажаришда тижорат асосида сертификат бериш буйича мустакил марказлар хам жалб этилиши мумкин. Бундай хизматларни, хусусан, Verisign компаниясининг сертификацияловчн маркази таклиф этади. Бу компаниянинг сертификатлари халкаро стандарт X.509 талабларига жавоб беради. Бу сертификатлар маълумотлар химоясининг қатор махсулотларида, жумладан, химояланган канал SSL протоколида ишлатилади.

10-маруза:

Ёпиқ калитни сақлашга асосланган аутентификациялаш усуллари.

1. Фойдаланувчининг профили реестр.
2. Ҳимояланмаган ахборот ташувчилар.
3. Touch-Memory, Memory-карталар.
4. Смарт-карталар ва USB-калитлар.

Криптографияда очиқ калит ёрдамида фойдаланувчиларни ишончли аутентификацидан, яъни ёпиқ калитга боғлиқ бўлмасдан ўтказиш мумкин. Шу сабабли ёпиқ калитни хавфсизликни таъминлаш мақсадида сақлаш лозим. Ёпиқ калитни сақлашнинг бир нечта усули мавжуд.

1. Фойдаланувчининг профили реестр

Ёпиқ калитни хавфсиз сақлашнинг энг содда усули операцион тизим таркибида фойдаланувчиларнинг пароль ва логинлари криптографик методлар ёрдамида ҳимояланишидир. Одатда бу ечим фойдаланувчи билан унинг ёпиқ калитини авторизациядан сўнг операцион тизим таркибида бирлаштирилади, бироқ ушбу калитни дастлабки аутентификация учун ишлатиш мумкин эмас. Чунки ёпиқ калит доимо конкрет компъютер боғлиқ бўлади. Шунга қарамасдан ёпиқ калит компъютернинг қаттиқ дискида сақланса ҳам, яъни ушбу калит фақатгина компъютер эгасига тегишли бўлса ҳам унга нисбатан тўғридан-тўғри ёки тармоқ хужумлари уюштирилиши мумкин. Нияти бузуқ одам ушбу ёпиқ калитни тизимга ўзини фойдаланувчи сифатида кўрсатиб олиш имконияти мавжуд.

2. Ҳимояланмаган ахборот ташувчилар

Ёпиқ калитни қўлда олиб юришнинг бир нечна усули мавжуд яъни дискетада, хотира картасида, USB-флешкада. Ушбу ҳолатда ахборот ташувчида калитли контейнер ҳосил бўлади ва у шифрланган кўринишда хотирада сақланади. Аммо бу усул унчалик эффектив ҳисобланмайди. Чунки ушбу пароллар контейнери шифрланган бўлсада уни бошқа бир флеш-картага кўчириб ўтказиш мумкин, бундай ҳолатда тизимни бузиш нияти

бузуқ одам учун хеч қандай қийинчилик туғдирмайди.

3. Touch-Memory, Memory-карталар

Ҳудди ахборот ташувчи сингари махсус аутентификацияловчи қурилма touch-memory ҳамда memory-карталарни қўлласа бўлади. Ушбу қурилмалар пластик карталар кўринишида ясалиб, кридит карталарга ўхшаш ва микросхемадан иборат бўлади. Ушбу қурилмалар шу типга мансуб бошқа қурилмалар сингари ўзиниг уникал номерига, фойдаланувчига тегишли шахсий маълумотларни сақловчи хотирага эга.

Айрим типдаги аутентификацияловчи қурилмалар икки факторли аутентификацияни қўллаб қувватлайди, яъни фойдаланувчи шахсий маълумотлари турадиган хотирага кириш учун ҳам PIN-код талаб этилади.

4. Смарт-карталар ва USB-калитлар

Смарт карталар худди memory-карталар сингари пластик карталар кўринишида қурилади ва таркиби микросхемадан иборат бўлади. Смарт-карталарнинг муҳим жиҳати шундан иборатки, смарт-карталар мураккаб аутентификациялаш қисмлардан ташкил топган бўлиб, яъни ўзининг микропроцессорига, операцион тизимига, назоратловчи қурилмасига ва объектнинг хотирасига кириш учун рухсатларни бошқариш тизимига эга. Бундан ташқари смарт-карталар криптографик амалларни ҳисоблаш имкониятига ҳам эга.

Смарт-карталарни ўқиб олувчи қурилма бевосита компъютерга боғланган бўлади, яъни:

- ✓ порт орқали;
- ✓ PCMCIA слот орқали;
- ✓ USB порт орқали.

Смарт-карталарни ўқиб олувчи қурилма клавиатура билан интеграллашган бўлади.

Айрим ишлаб чиқарувчилар шундай аппарат воситаси ишлаб чиқишганки, унга кўра смарт-карталар билан уларни ўқиб олувчи қурилма бирлаштирилган. Ишлаш принципига кўра ушбу смарт-карталар оддийлари

билан бир хил ҳисобланади.

Машхур фирмаларнинг аппарат воситалари калитни ўқиб олувчи қурилма сифатида асосан USB портни ишлатишади. USB калитлар қўллаш ҳар қандай компания ёки фирмалар учун бир мунча қулайликлар яратади, чунки ҳозирги кунда USB порт стандарт портга айланиб улгурган, ҳамда уни ишлатиш энг қулай усул ҳисобланади.

Смарт-карталар ва USB калитлар имкониятидан келиб чиққан ҳолда интеллектуал қурилмалар ҳисобланади.

11-маруза:

Очиқ калит ёрдамида аутентификациялаш ҳамда интеллектуал қурилмалар

1. Ишчи станцияда калитларни генерация қилиш
2. Қурилмага асосланган ҳолда калитларни генерация қилиш

Смарт-карталар ҳамда USB калитлар очиқ калитлар инфраструктураси хизматининг ишончлилигини тпъминлаши мумкин. Смарт-карта ёрдамида фойдаланувчининг ёпиқ калитини хавфсиз сақлашимиз, ундан ташқари криптографик амалларни ҳам хавфсиз амалга ошириш мумкин. Шуни таъкидлаб ўтиш жоизки, интеллектуал қурилмалар ёрдамида аутентификациялаш тўла қонли хавфсизликни таъминлай олмайди, лекин одатий компъютердаги хавфсизликка нисбатан бир мунча юқорироқ.

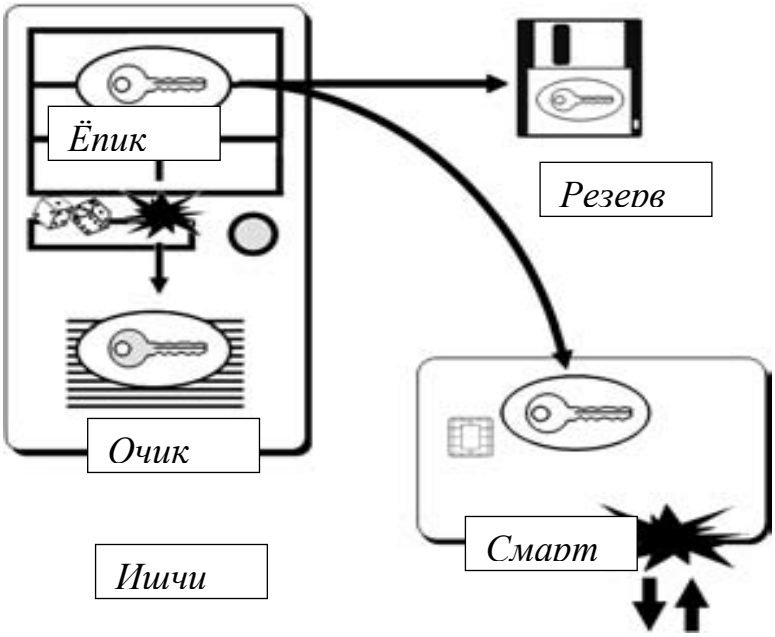
Ёпиқ калитни қўллашга ва хавфсиз сақлашга ишлаб чиқарувчилар бир мунча йўриқномалар тавсия қилишади. Уларнинг ичида энг содда усул дискеталарни интеллектуал қурилма сифатида ишлатиш. Ушбу ечим хавфсизлик нуқтаи назаридан хақиқий ҳисобланмасада, оддий тизимлар учун осон ташкил қилиш мумкин.

Қуйида келтирилган иккита усул юқоридаги усулга нисбатан бир мунча самаралироқ ҳисобланади. Биринчи усулда фойдаланувчи ишчи станцида калитни генерация қилади ва қурилма хотирасига сақлаб олади. Иккинчи усулда фойдаланувчи калитни қурилманинг ўзида генерация қилади ҳамда уни қурилманинг ўзида сақлайди. Иккала усулда ҳам ёпиқ калит яхши сақланган, уни хеч қандай қурилма ёки бошқа усул билан олиб бўлмайди.

1.Ишчи станцияда калитларни генерация қилиш

Ушбу ҳолатда фойдаланувчи ёпиқ калитдан резерв олиш имкониятига эга бўлади. Агар қурилма авария ҳолатида бўлса, йўқолса, иш ҳолатида бўлмаса ҳам фойдаланувчи ўзининг ёпиқ калитини янги картада сақлаши мумкин. Ушбу имконият эвазига фойдаланувчи талаб этилган маълумотларни ўзининг янги резерв олинган калити ёрдамида дешифрлаб

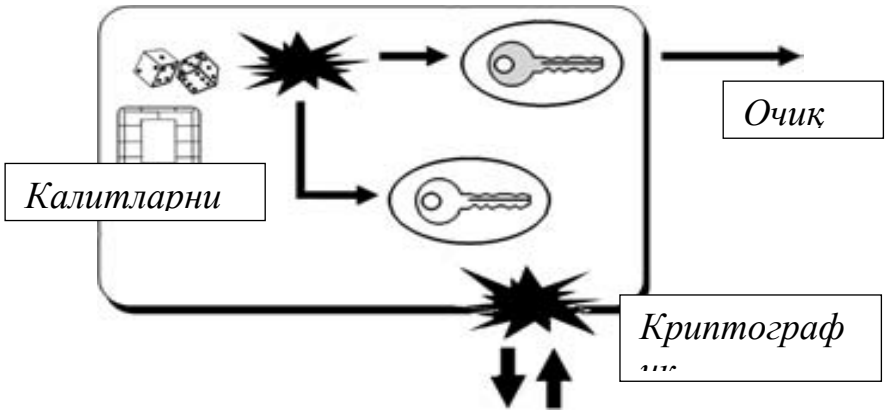
фойдаланиши мумкин.



1-расм.Ишчи станцияда калитларни генерация қилиш

2.**Қурилмага асосланган ҳолда калитларни генерация қилиш**

Ушбу ҳолатда ёпиқ калит қурилмадан ташқарига чиқмайди ва калитга нисбатан хеч қандай хавф-хатар мавжуд эмас, ундан ташқари нияти бузуқ одам ёпиқ калитдан резерв нусха олиш имкониятига эга эмас. Ёпиқ калитни ишлатиш учун интеллектуал қурилмага эга бўлиш талаб этилади. Ушбу ечим интеллектуал қурилмалар имкониятларига катта талаб қўяди. У калитларни генерация қилиши ҳамда криптографик операцияларни бемалол бажариши шарт. Шуни таъкидлаб ўтиш жоизки, ёпиқ калит агар қурилма таркибидан ўчирилган бўлса уни тиклашнинг хеч қандай имконияти мавжуд эмас.



2-расм. Қурилмага асосланган ҳолда калитларни генерация қилиш

12-маруза:

Очиқ калит ёрдамида аутентификациялашнинг камчиликлари. Мавжуд хужумлар.

Қуйида очиқ калитлар асосида аутентификацияловчи тизимларга уюштирилувчи машхур хужумлар ҳамда улардан ҳимояланиш усуллари келтирилган.

Калитни факторизациялаш. Нияти бузуқ одам кобинаторика орқали калитни комбинациялаб, фойдаланувчининг калитига эга бўлиши мумкин. Ушбу хужумга қарши калитнинг узунлигини ошириш билан ҳимояланиш мумкин. Калитни камида 512 бит узунликдагисини ишлатиш лозим. Сертификат марказлар учун калит узунлиги 2048 бит бўлиши шарт.

Муҳим хабарга асосланган хужум. Нияти бузуқ одам фойдаланувчига муҳим хабар жўнатиб, уни шахсий калити билан имзолашни талаб қилади. Ушбу хужумга қарши калитни хешлаш орқали жавоб қайтариш мумкин.

Қалбаки очиқ калитга асосланган хужум.Нияти бузуқ одам ўзининг шахсий очиқ калитини тақдим қилиш орқали, агар қабул қилувчи аутентификациядан ўтмаган калитни қабул қилса. Сертификатланган очиқ калитни қўллаш орқали ушбу хужумдан ҳимояланиш мумкин.

“Ўртадаги одам” хужуми. Нияти бузуқ одам ўзининг шахсий очиқ калитини бошқа калит ўрнига тақдим қилади ва объектлар ўртасида хабарни қайтадан шифрлаб жўнатади. Ушбу хужумга қарши ҳам сертификатланган очиқ калитларни қўллаш мумкин.

Сертификатларни алмаштиришга асосланган хужум. Нияти бузуқ одам қонуний сертификат ишлатиб, қалбаки сервернинг IP адресидан фойдаланади. Ушбу хужумга қарши сертификатга эга хостларнинг номини ишончлилигини текшириш орқали ҳимояланиш мумкин, сертификатдаги исм хост-машинанинг исми билан солиштирилади, яъни қабул қилинган сертификатга кўра.

Шахсий калитни ишлатишга асосланган хужум. Нияти бузуқ одам ўғирланган шахсий калитни ишлатади. Ушбу хужумга қарши бир нечта чора-

тадбирлар мавжуд, яъни:

- ✓ Тақриздан ўтган сертификатлар рўйҳати-даврий сертификатлар рўйҳати чиқиб туради.
- ✓ Интерактив чакирилган сертификаттлар – сертификатнинг хақиқийлигини текширувчи механизм мавжуд бўлиб, у сертификатнинг тақриздан ўтган ёки ўтмаганлигини аниқлиди.
- ✓ Даврий сертификатлаш орқали.

Шахсий калитни актив разведка қилиш. Нияти бузуқ одам тизимни бузувчи дастурий таъминот қўллаш орқали фойдаланувчининг тизимга кириш моментида киритган паролини ўқиб олиш орқали паролга эга бўлиши мумкин. Смарт-карталарни қўллаш ҳамда шифрлаш функциясидан фойдаланиш орқали ушбу хужумга тўсқинлик қилиш мумкин. Чунки шахсий калит хеч қачон смарт-карта хотирасидан ўчмайди, ўқиб олинмайди.

Шахсий калитни ўғирлаш орқали ундан резерв нусҳа олиш хужуми. Нияти бузуқ одам дискетадаги ёки бошқа қурилмадаги шахсий калитнинг резерв нусҳасини ўғирлаш орқали тизимга кириши мумкин. Смарт-картанинг ўзида шахсий калитни генерация қилиш орқали ушбу хужумдан ҳимояланиш мумкин.

Одатда ахборот алмашувчи томонлар мулоқотни янада юқсакроқ поғонага кўтариш мақсадида моҳият аутентификацияси протоколини ишга туширадилар. Замонавий криптографияда ҳимояланган алоқа каналларини ташкил этишда криптографик калитлардан фойдаланилади. Бинобарин, моҳият аутентификацияси протоколи ҳимояланган алоқа каналлари орқали ахборот алмашиш учун таркибий қисм сифатида *аутентификацияланган калитларни генерациялаш*ёки **калит** *алмашиш* **(**keyexchange**)** ёки *калитларни мувофиқлаштириш*(keyagreement) механизмларини ўз ичига олиши лозим.

Аутентификацияланган калитларни генерациялаш протоколида протокол маълумотлари ўзида калитлар параметрларини акс эттиргани боис, уларнинг манбаини ҳам аутентификациядан ўтказиш лозим.

Адабиётларда аутентификацияланган калитларни генерациялаш

протоколи, моҳият аутентификацияси протоколи, маълумотларни ҳимоялаш протоколи, ҳаттоки криптографик протоколлар ҳам кўпинча алоқа протоколлари деб номланади.

Барча аутентификациялашпротоколларини уч синфга бўлиш мумкин:

- Бирон нарсани билиш асосида. Энг кенг тарқалган варианти – пароллар;
- Бирон нарсага эгалик қилиш асосида (магнит карталар, смарт-карталар ва ҳоказо);
- Ажралмас хусусиятлар асосида (овоз, кўзнинг тўр пардаси, бармоқ излари). Бу категорияда криптографик усуллар одатда қўлланилмайди.

Аутентификациялаш протоколларини таққослашда ва танлашда қуйидаги характеристикаларни ҳисобга олиш зарур:

- -ўзаро аутентификациянинг мавжудлиги. Ушбу хусусият аутентификацияли алмашинув тарафлари ўртасида иккиёқлама аутентификациялашнинг зарурлигини акс эттиради;
- -ҳисоблаш самарадорлиги. Протоколни бажаришда зарур бўлган амаллар сони;
- -коммуникацион самарадорлик. Ушбу хусусият аутентификациялашни бажариш учун зарур бўлган хабарлар сони ва узунлигини акс эттиради;
- -иккинчи тарафнинг мавжудлиги. Ушбу тарафга мисол тариқасида симметрик калитларни тақсимловчи ишончли серверни ёки очиқ калитларни тақсимлаш учун сертификатлар дарахтини амалга оширувчи серверни кўрсатиш мумкин;
- -хавфсизлик кафолат асоси. Мисол сифатида ноллик билим билан исботлаш хусусиятига эга бўлган протоколларни кўрсатиш мумкин;
- сирни сақлаш. Жиддий калитли ахборотни сақлаш усули кўзда тутилади.

13-маруза:

Калит сўзли ахборотларни сақлаш ҳамда аутентификацияловчи аппарат воситаларини қўлланилишининг аҳамияти

1. Ёпиқ калитларнинг хавфсизлиги.
2. Ёпиқ калитларни ҳимоялашнинг усуллари.
3. Ёпиқ калитлар учун асосий таҳдидлар.
4. Криптографик имкониятларга эга бўлган аппарат воситалари.

Криптографиянинг асимметрик алгоритмларида бир-бирига боғлиқ бўлмаган иккита калитдан фойдаланилади. Улардан бири очиқ калит, яъни шифрлаш, ЭРИ хақиқийлигини текшириш учун ишлатилади. Иккинчиси ёпиқ калит ёпиқ операциялар учун, яъни маълумотни дншифрлаш, ЭРИ ни генерация қилиш каби. Ушбу имконият орқали биз нафақат махфий маълумотларни ўзга фойдаланувчилардан яшира оламиз, балки авторлик хуқууини ҳам ҳимоялашимиз мумкин.

Ёпиқ калитларнинг хавфсизлиги

Криптографиянинг асосий постулати шундан иборатки, ёпиқ калит доимо унинг эгасига тегишли бўлади. Агар нияти бузуқ одам ушбу ёпиқ калитни қўлга киритадиган бўлса, ахборот алмашишда иштирок этадиган исталган томоннинг ахборотини дешифрлаш имкониятига эга бўлади. Бундан ташқари у ихтиёрий хабарни қонуний фойдаланувчи номидан жўнатиши, хабар қабул қилиши умуман информацион жараёнда қатнашиши мумкин. Ушбу хужумлар оқали нияти бузуқ одамлар ЭРИ тизимининг хуқуқий қисмига жиддий зарар етказадилар. Чунки ёпиқ калитни унинг фойдаланувчиси ёки нолегал фойдаланувчи фойдаланганлигини аниқлаш бир мунча мураккабликларни келтириб чиқаради.

Шу сабабли ёпиқ калитнинг ҳимояланганлик даражаси ҳаёт цикли каби ҳар бир этапда таъминланиши шарт, яъни:

- ✓ Калитлар жуфтини генерация қилишда (ёпиқ ва очиқ калитни);
- ✓ Ёпиқ калитни сақлашда;

- ✓ Ёпиқ калитни ишлатишда;
- ✓ Ёпиқ калитни йўқотиш жараёнида.

Калитларни генерация қилиш жараёнида, нияти бузуқ одамнинг генерация қилувчи тизимга кира олмаслиги таъминланиши шарт.

Ёпиқ калитни сақлашда унинг конфеденциаллиги ҳамда бутунлигининг таъминланганлиги, яъни ноқонуний кириш ва рухсатлардан, модификацияланишлардан ҳимояланганлиги.

Ёпиқ калитдан фойдаланишда унинг ўғирланишининг олди олинганлиги, нолегал фойдаланишдан чекланиши лозим.

Хуллас иш охирисида, яъни ёпиқ калитни йўқотиш жараёнида ундан қайта фойдаланиш ёки тиклаш имконияти чекланиши шарт.

Ёпиқ калитларни ҳимоялашнинг усуллари

Ҳозирги кунда ёпиқ калитларни ҳимоялашнинг кўпгина усуллари мавжуд бўлиб, улар қаторига қуйидагиларни киритиш мумкин:

1. Дастурий таъминот ёрдамида сақлаш. Дастурий таъминот ёпиқ калитларни компъютернинг қаттиқ дискида шифрланган кўринишда сақлайди. Бундай дастурий таъминотларга мисол сифатида Windows операцион тизими таркибига кирувчи Microsoft Enhanced CSP, Mozilla/Netscape келтириш мумкин. Дастурий таъминот ёрдамида фойдаланувчининг ёпиқ калитларини сақлашда уларнинг хавфсизлиги таъминланмайди. Улар ҳимояланганлик тасаввурини яратади.

2. Аппарат воситалар. Аппарат воситалари ёпиқ калитларни сақлаш ҳамда криптографик операциялар бажариш учун мўлжалланган. Ушбу аппарат воситалари қаторига смарт-карта, USB-калит ва Aladdin компаниясининг eToken PRO ларни киритиш мумкин.

3. Репозиторлар. Бир нечна фойдаланувчиларнинг ёпиқ калитларни марказлаштирилган асосда сақлаш учун серверлардан фойдаланилади. Фойдаланувчи ёпиқ калитдан фойдаланишдан олдинсервердан аутентификациядан ўтиши лозим бўлади. Ушбу усул хавфсизлик нуқтаи

назаридан энг эффектив ҳисобланади.

Ёпиқ калитлар учун асосий таҳдидлар

Ҳар қандай шахсий компъютерга нисбатан иккита асосий потенциал даражадаги хавф мавжуд, яъни:

Компъютерга физик руҳсатнинг борлиги. Ушбу хавфнинг асосида қуйидаги факт, яъни кўпгина ҳолатларда компъютерга нисбатан физик руҳсатнинг борлиги натижасида унинг ҳимояланганлик даражаси тушиб кетишига сабаб бўлади. Бу ерда гап компъютернинг ўғирланиши ёки бузилиши ҳақида бормаяпти, лекин ушбу хафвлврнинг умуман йўқ деб ҳисоблаб бўлмайди. Кўпгина компанияларда ходимлар смена асосланган ҳолда ишлайди. Бундан келиб чиқадики бир нечта ходим айнан битта компъютердан фойдаланишади. Шу сабабли ходимлар ушбу компъютер билан қандай ҳолат юз бераётганлигини тўлиқ англаб етмайдилар. Бунга мисол сифатида корхона котибаси махсус чақириқ билан ўз иш ўрнидаги компъютерни очиқ ҳолда ташлаб кетиши (компанияга котибанинг олдига қандайдир мижоз келган бўлса). Ушбу ҳолатда келган мижоз нима мақсадда келганини аниқлаш қийин.

Заракунанда дастурлар. Иккинчи жиддий хавфни зараркунанда дастурлар, яъни вируслар, тармоқ червлари, троянлар. Зараркунанда дастурларнинг тез вақт ичида тарқалиши ҳамда кўпайиши компания иқтисодига жиддий зарар етказади.

Ушбу зараркунанда дастурлар операцион тизимнинг иш фаолиятини бузиб қолмай, унда сақланаётган ёпиқ калитларга ҳам жиддий зарар етказиши мумкин.

Криптографик имкониятларга эга бўлган аппарат воситалари

Юқоридаги фикрлардан кўриниб турибдики, ёпиқ калитни генерация қилиш компъютернинг хавфсиз бўлмаган жойида амалга оширилмоқда, яъни калитга нисбатан бир мунча хавфлар мавжуд.Ушбу муаммони ечиш мақсадида криптографик операцияларни амалга оширирувчи аппарат воситаларини қўллаш самарали ҳисобланади. Ахборот ташувчи шифрлаш ва

хабарни тескарисига жўнатиш каби амалларни бажарувчи микропроцессорга эга бўлиши талаб этилади. Криптографик операцияларни ушбу аппарат воситаларида мавжудлиги калит сўзли ахборотнинг ҳимояланганлик даражасини оширади. Бундан келиб чиқадики ёпиқ калит хеч қачон қурилмадан ташқарига экспортация қилинмайди. Ушбу факт ёпиқ калитнинг қурилманинг хотирасида муқим, хавфсиз сақланишидан далолат беради.

14-маруза:
Аутентификациялаш воситалари ва калит сўзли ахборотларни сақлашга қўйиладиган талаблар

1. Криптография соҳасида мавжуд миллий стандартларнинг қўллаб қувватланиши.
2. Халқаро криптографик стандартларнинг қўллаб қувватланиши.
3. Аутентификация воситаларини сертификатлаш ва калит сўзли ахборотларни сақлаш.
4. Қурилманинг ҳаётий циклини бошқариш учун қўйиладиган талаблар.

Замонавий аутентификациялаш ҳамда калит сўзли ахборотни сақлаш воситалари фойдаланувчиларнинг махфий маълумотларини қурилманинг хотирасида хавфсиз сақлаб қолмасдан, криптографик операцияларни миллий стандартлар талабларига асосланган ҳолда амалга ошириши лозим. Ушбу ҳолатдан сўнгина фойдаланувчиларнинг маълумотлари ишончли ҳимояланганлигига ишониш мумкин.

Ахборот хавфсизлиги соҳасида миллий талаблар турли мамлакатларда турлича ҳисобланади. Миллий аутентификациялаш ҳамда калит сўзли ахборотни сақловчи қурилмаларни ишлаб чиқишда анолог қурилмалардан фойдаланиш каби ечимдан фойдаланилади.

Аутентификациялаш ҳамда калит сўзли ахборотларни сақловчи воситалари миллий бозорда қуйидаги минимал талабларга жавоб бериши лозим:

- миллий ҳамда халқаро криптография соҳасидаги мавжуд стандартларни қўллаб-қувватлаши;
- сертификациядан ўтганлиги;
- дастурни клиент қисмида ишлатиш учун қўшимча дастурий таъминотларнинг талаб қилинмаслиги;
- қурилмада бир нечта иловадан фойдаланиш имкониятининг мавжудлиги;

- қурилманинг ҳаёт циклини бошқариш учун инфраструтурали ечимларнинг мавжудлиги;
- USB калит ҳамда Смарт карталарни қўллаб-қувватлаши.

Криптография соҳасида мавжуд миллий стандартларнинг қўллаб қувватланиши

Ушбу қўллаб қувватлаш қуйидагича ташкил қилиниши лозим:

- аппарат даражасида (қурилманинг ўзида миллий криптографик алгоритмларнинг шакллантирилганлиги);
- дастурий таъминот даражасида (криптопровайдерлар, турли бошқа қурилмалар билан синхрон ишлай олиши ва компаниянинг миллий дастурий маҳсулотларини қўллаб қувватлаши).

Аппарат воситасини ишлаб чиқарувчи биринчи ўринда миллий криптографик алгоритмлар билан биргаликда мамлакатнинг миллий ЭРИ стандартини ҳам ҳисобга олиш шарт.

Халқаро криптографик стандартларнинг қўллаб қувватланиши

Халқаро информацион жараёнларда, яъни хориж билан ахборот алмашиниш жараёнлари учун ишлаб чиқарилган қурилма халқаро стандартларга жавоб бериши,яъни халқаро криптографик алгоритмларни қўллаб қувватлаши лозим. Мисол учун ҳозирда RSA алгоритми халқаро стандарт асосида қурилган алгоритм ҳисобланади. МДҲ давлатлари ўртасида ишончли ахборот алмашиш учун ЭРИ ни ҳосил қилувчи ҳамда текширувчи алгоритм ГОСТ Р 34.310-2004 стандарти асосида ишлаб чиқилган.

Аутентификация воситаларини сертификатлаш ва калит сўзли ахборотларни сақлаш

Қонунчилик талабларига кўра фойдаланувчиларнинг аутентификация жараёни учун тақдим қилувчи калит сўзли ахборотлари сир сақланади, яъни ушбу ахборотлар конфеденциал ахборотлар қаторига киритилади.

Ахборотларни ишончли ҳимоялаш учун аутентификациялаш ҳамда калит сўзли ахборотларни сақловчи қурилмалар сертификатлаш тизимидан ўтган бўлиши лозим.

Қурилманинг ҳаётий циклини бошқариш учун қўйиладиган талаблар

Аутентификациялаш воситаларнинг асосий характери ундан катта масштабдаги фойдаланувчилар гуруҳи фойдаланишлари мумкин. Бундан келиб чиқадики ушбу қурилмалар ягона марказий бошқарув системасига эга бўлиши шарт:

- Чиқарилган қурилмаларни реестрдан ўтказиш;
- Уларнинг ҳаёт циклини бошқариш ;
- Қурилма устида аудит ўтказиш;
- ИТ ва ИБ бўлимлари учун ҳисобот тайёрлаш.

15-маруза:

Калит сўзли ахборотларни сақлаш ва шахсий аутентификациялаш воситаларини корпоратив қўлланилишининг афзалликлари.

1. Юқори даражали ролли модели.
2. Биноларга СКУД тизимини интеграция қилиш.
3. Марказий бошқарув системаси.

Юқори даражали ролли модели

Корпоратив бошқарув тизимида руҳсатларни назорат қилишда юқори даражали ролли моделидан фойдаланилса самарали ҳисобланади. Ушбу модель қуйидаги даражаларни ўз таркибига олади:

- ***Фойдаланувчилар даражаси.*** Оҳирги фойдаланувчи тизимга кириб, маълумотлардан фойдаланиши учун PIN коддан фойдаланади.
- ***Администратор даражаси.*** Ахборот хавфсизлиги администратори ташкилот хавфсизлиги учун қўлланиладиган барча қонун қоидаларни, яъни ахборот хавфсизлиги сиёсатига асосланган ҳолда ўрнатади. Администратор бирон-бир фойдаланувчини блоклаш ёки руҳсат бериш учун махсус PIN коддан фойдаланади.
- ***Ишлаб чиқарувчи даражаси.*** Ушбу даражада PIN код қуйидагилар учун қўлланади:
  - ✓ Қурилма хотирасидан барча аутентификацияловчи маълумотларни форматлашдан олдин;
  - ✓ Ташкилотдаги ахборот хавфсизлиги сиёсатига асосланиб қонун қоидалар ўрнатиш жараёнида.

Биноларга СКУД тизимини интеграция қилиш

Смарт карта ҳамда USB калитлар турли ахборот тизимларига киришда ягона восита ҳисобланади. Смарт карталарда фойдаланувчи ҳақида ахборот билан биргаликда унинг расми жойлашган бўлади.(1-расм)

1-расм. Смарт карта кўриниши

2-расм. USB калитнинг кўриниши

Смарт карта ҳамда токенлар қўшимча алоқасиз радио-меткалардан ҳам иборат бўлиши мумкин. Бундай смарт карталар электрон кириш-чиқишларни бошқарувчи тизимларда ишлатилади.

Марказий бошқарув системаси

Корпоратив бошқарув тизимида кўп ҳолларда PKI технологияси қўлланилади. Бу технология асосида смарт карталар, USB калитлар, бир мартали пароль генераторлари, кобнацияли қурилмалар ишлатилади.

Марказий бошқарув системаси қуйидаги талабларга жавоб бериши шарт:

- фойдаланувчиларнинг маълумотларини қурилма хотирасидан марказий автоматик равишда тиражлаш, янгилаш, ўчириш;
- йўқолган калит сўзли ахборотларга асосланган аутентификацияловчи воситаларни блоклаш;

- гуруҳга асосланган сиёсат олиб бориш, PIN кодларга нисбатан ягона сиёсат юргизиш;
- ахборот хавфсизлиги нуқтаи назаридан руҳсатларни бошқариш;
- статистик маълумотларни йиғиш ҳамда тизимни аудит қилиш;
- хизматлар каталоги билан интеграллашган бўлиши(мисол учун microsoft Active Directory ёки OpenLDAP);
- клиент қисмдаги дастурий таъминотларнинг янгиланганлик даражасини назорат қилиш.

16-маруза:
Марказий бошқарув тизимида аутентификациялаш воситалари ва фойдаланувчиларнинг калит сўзли ахборотларини сақлаш

1. Марказий бошрув тизимида аутентификациялаш воситаларинг ҳаёт циклини бошқаришдаги мавжуд муаммолар.
2. Токенларнинг ҳаёт цикли.
3. Токенларни регистрациядан ўтказиш.

Кўпгина ташкилотлар бошқарув жараёнида ишончли аутентификациялаш воситалари ҳамда калит сўзли ахборотларни сақловчи қурилмаларни ишлатишади(USB калитлар, Смарт карталар ҳамда токенлар). Ушбу қурилмаларни марказий бошқарув тизимисиз бошқариш хеч қандай фойда бермайди. Токенлар билан ишлаш тизимлари токенларнинг ҳаёт циклини бошқариш ва қўллаб қувватлаш каби аппарат воситанинг реаллаштирувчи имкониятларни тақдим қилади.

Марказий бошрув тизимида аутентификациялаш воситаларинг ҳаёт циклини бошқаришдаги мавжуд муаммолар.

Аутентификацияловчи воситаларини қўллаш фойдаланувчиларнинг калит сўзли ахборотларини назорат қилиш ҳамда бошқариш каби вазифаларни қўяди корхона бошчилиги асосида. Бу тизимсиз бошқарувдвги ўзаро алоқалар қийинлашиши, вақтнинг кўп сарфланиши, кўп маблағ сарфланишига ва бир қанча хатоликлар эҳтимолликларини келиб чиқиши мумкин.

Мисол учун ташкилотга янги ишга кирган ходимни олайлик.

Аутентификация воситасини яратиш ва регистрациядан ўтказиш. Ишни бошлаш учун ходим ўз токенига эга бўлиши лозим. Бошқарув системасиз тизим администратори ходимнинг шахсий маълумотларини токеннинг хотирасига киритиши шарт. Бунга ўхшаш ҳолат оқибатида, яъни

маълумотларни қўлда киритиш оқибатида бир талай хатоликлар келиб чиқиши мумкин. Бунинг оқибатида янги олинган ходим билан ахборот хавфсизлиги бўлими ўртасида муаммо келиб чиқиши мумкин.

Токеннинг PIN кодини тиклаш. Агар ходим ўз PIN-кодини унутиб қўйса, аутентификациядан ўта олмайди ва натижада тизим тармоғига улана олмай ўз ишини бажара олмайди. PIN – кодни мустақил тиклаш учун фойдаланувчиларни қўллаб – қувватлаш тизимига уланиши лозим. Бундай ҳолат оқибатида биринчидан вақт кетади, иккинчидан компаниянинг ресурси.

Йўқолган токенни алмаштириш. Ходим ўз токенини йўқотиб қўйиши мумкин. Бунинг оқибатида администратор қуйидагиларни қўлда бажаришга мажбур:

- Ходимнинг рухсати бор барча информацион тизимлардаги шахсий маълумотларини чақириш ҳамда блоклаш;
- Янги шахсий маълумотларни киритиш;
- Ходимга янги токен бериш ҳамда унинг шахсий маълумотларини токеннинг хотирасига киритиш.

Ушбу жараёнда администратор ходимнинг шахстй маълумотларини шакллантириш жараёнида хато маълумот киритиб қўйиши, ёки эсдан чиқариб қўйиши каби эҳтимолликлар мавжуд. Ушбу хатоликлардан исталган одам тизимдан нолегал фойдаланиш каби имкониятга эга бўлиши мумкин.

Токенларнинг ҳаёт цикли

Регистрация. Токен фойдаланувчи билан боғланган ҳолда тизимга фойдаланувчининг корхонадаги ролига қараб ахборот хавфсизлиги сиёсатига мувофиқ регистрация қилинади. Токеннинг хотирасига аутентификация учун ахборотлар билан калит сўзли ахборот ёзилади.

Фойдаланиш ва қўллаб қувватлаш. Аутентификация учун маълумотлар билан калит сўзли ахборот даврий ўзгариб туриши мумкин. Мисол учун бу ходимнинг мансаби ошиши ҳисобига ёки бир бўлимдан

бошқасига ўтиши ҳисобига ўзгартирилиши мумкин.

Чиқариш. Ходим агар ишдан бўшаса аутентификацияловчи маълумотлар ҳамда калит сўзли ахборот токен хотирасида ўчирилади ҳамда ушбу токен бекор қилинади.

Эксплутацияга қайтиш. Токен янги ходимга берилиши мумкин. Регистрациядан олдин токен киритиш ҳолатига келтирилиши ҳамда янги ходимнинг маълумотлари билан узвийлаштирилган бўлиши лозим.

Токенларни регистрациядан ўтказиш

Ҳар бир токен корхонанинг ҳар бир ходими учун тайёрланиши ҳамда регистрациядан ўтказилиши лозим. Регистрация жараёнида токеннинг хотираси фойдаланувчининг маълумотлари, рақамли сертификат ва парол билан тўлдирилади. Токенлар махсус PIN кодлар ёрдамида ҳимояланади.

Бошқарув тизими мустақил регистрациядан ўтказиш каби имкониятларга эга бўлиши мумкин. Ушбу усул хатоликликларни камайтиришнинг энг самарали усули ҳисобланади.