ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

МУСТАҚИЛ ИШ

Мавзу: Тармоққа уланишни дастурлаш. Аутентификация, идентификация ва авторизация

ТОШКЕНТ 2017

Тармоққа уланишни дастурлаш. Аутентификация, идентификация ва авторизация

Режа

1. Асосий тушунчалар ва синфланиши
2. Пароллар асосида аутентификациялаш
3. Сертификатлар асосида аутентификациялаш
4. Қатъий аутентификациялаш

Таянч иборалар: *индентификатор, идентификация, аутентификация, маъмурлаш, маскарад, такрорий узатиш, узатишни қайтариш, мажбурий кечикиш, матн танлашли хужум.*

1. Асосий тушунчалар ва синфланиши

Компьютер тизимида рўйхатга олинган хар бир субъект (фойдаланувчи ёки фойдаланувчи номидан харакатланувчи жараён) билан уни бир маънода индентификацияловчи ахборотга боғлиқ.

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

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

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

Идентификация ва аутентификация субъектларнинг (фойдаланувчиларнинг) хақиқий эканлигини аниқлаш ва текширишнинг ўзаро боғланган жараёнидир. Муайян фойдаланувчи ёки жараённинг тизим ресурсларидан фойдаланишига тизимнинг рухсати айнан шуларга боғлиқ. Субъектни идентификациялаш ва аутентификациялашдан сўнг уни авторизациялаш бошланади.

Авторизация (Authorization) - субъектга 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 яхлитлиги бузилиши мумкин.

Аутентификация ва авторизация муолажалари билан фойдаланувчи харакатини 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 муҳимдир.

Маълумотларни узатиш каналларини химоялашда *субъектларнинг ўзаро аутентификацияси,* яъни алоқа каналлари орқали боғланадиган субъектлар хақиқийлигининг ўзаро тасдиғи бажарилиши шарт. Хақиқийликнинг тасдиғи одатда сеанс бошида, абонентларнинг бир-бирига уланиш жараёнида амалга оширилади. “Улаш” атамаси орқали тармоқнинг иккита субъекти ўртасида мантиқий боғланиш тушунилади. Ушбу муолажанинг мақсади - улаш қонуний субъект билан амалга оширилганлигига ва барча ахборот мўлжалланган манзилга боришлигига ишончни таъминлашдир.

Ўзининг хақиқийлигининг тасдикдаш учун субъект тизимга турли асосларни кўрсатиши мумкин. Субъект кўрсатадиган асосларга боғлиқ ҳолда аутентификация жараёнлари қуйидаги категорияларга бўлиниши мумкин:

- *бирор нарсани билиш асосида.* Мисол сифатида парол, шахсий идентификация коди PIN (Personal Identification Number) хамда “сўров жавоб” хилидаги протоколларда намойиш этилувчи махфий ва очиқ калитларни кўрсатиш мумкин;
- *бирор нарсага эгалиги асосида.* Одатда булар магнит карталар, смарткарталар, сертификатлар ва touch memory қурилмалари;
- *қандайдир дахлсиз характеристикалар асосида.* Ушбу категория ўз таркибига фойдаланувчининг биометрик характеристикаларига (овозлар,

кўзнинг рангдор пардаси ва тўр пардаси, бармоқ излари, кафт геометрияси ва ҳоказо) асосланган усулларни олади. Бу категорияда криптографик усуллар ва воситалар ишлатилмайди. Биометрик характеристикалар бинодан ёки қандайдир техникадан фойдаланишни назоратлашда ишлатилади.

Аутентификация жарёнларини таъминланувчи хавфсизлик даражаси бўйича хам туркумлаш мумкин. Ушбу ёндашишга биноан аутентификация жараёнлари қуйидаги турларга бўлинади:

- пароллар ва рақамли сертификатлардан фойдаланувчи аутентификация;
- криптографик усуллар ва воситалар асосидаги қатьий аутентификация;
- нуллик билим билан исботлаш хусусиятига эга бўлган аутентификация жараёнлари (протоколлари);
- фойдаланувчиларни биометрик аутентификацияси.

Хавфсизлик нуктаи назаридан юқорида келтирилганларнинг хар бири ўзига хос масалаларни ечишга имкон беради. Шу сабабли аутентификация жараёнлари ва протоколлари амалда фаол ишлатилади. Шу билан бир қаторда таъкидлаш лозимки, нуллик билим билан исботлаш хусусиятига эга бўлган аутентификацияга қизиқиш амалий характерга нисбатан купроқ назарий характерга эга. Балким, якин келажакда улардан ахборот алмашинувини химоялашда фаол фойдаланишлари мумкин.

Аутентификация протоколларига бўладиган асосий хужумлар қуйидагилар:

- *маскарад* (impersonation). Фойдаланувчи ўзини бошка шахс деб кўрсатишга уриниб, у шахс тарафидан харакатларнинг имкониятларига ва имтиёзларига эга булишни мўлжаллайди;
- аутентификация алмашинуви *тарафини алмаштириб қўйиш* (interleaving attack). Нияти бузуқ одам ушбу хужум мобайнида икки тараф орасидаги аутенфикацион алмашиниш жараёнида трафикни модификациялаш ниятида қатнашади. Алмаштириб қўйишнинг қуйидаги хили мавжуд: иккита фойдаланувчи ўртасидаги аутентификация муваффакиятли ўтиб, уланиш ўрнатилганидан сўнг бузғунчи фойдаланувчилардан бирини чиқариб ташлаб, унинг номидан ишни давом эттиради;
- *такрорий узатиш* (replay attack). Фойдаланувчиларнинг бири томонидан аутентификация маълумотлари такроран узатилади;

- *узатишни қайтариш* (reflection attak). Олдинги хужум вариантларидан бири бўлиб, хужум мобайнида нияти бузуқ одам протоколнинг ушбу сессия доирасида ушлаб қолинган ахборотни орқага қайтаради.

- *мажбурий кечикиш* (forced delay). Нияти бузуқ одам қандайдир маълумотни ушлаб қолиб, бирор вақтдан сўнг узатади.

- *матн танлашли хужум* (chosen text attack). Нияти бузуқ одам аутентификация трафигини ушлаб қолиб, узоқ муддатли криптографик калитлар хусусидаги ахборотни олишга уринади.

Юқорида келтирилган хужумларни бартараф қилиш учун аутентификация протоколларини қуришда қуйидаги усуллардан фойдаланилади:

- “сўров-жавоб” вақт белгилари, тасодифий сонлар, индентификаторлар, рақамли имзолар каби механизмлардан фойдаланиш;

- аутентификация натижасини фойдаланувчиларнинг тизим доирасидаги кейинги харакатларига боғлаш. Бундай мисол ёндашишга тариқасида аутентификация жараёнида фойдаланувчиларнинг кейинга ўзаро алоқаларида ишлатилувчи махфий сеанс калитларини алмашишни кўрсатиш мумкин;

- алоқанинг ўрнатилган сеанси доирасида аутентификация муолажасини вақти-вақти билан бажариб туриш ва хоказо.

Вақтни белгилаш механизми хар бир хабар учун вақтни қайдлашни кўзда тутади. Бунда тармоқнинг хар бир фойдаланувчиси келган хабарнинг канчалик эскирганини аниқлаши ва уни қабул килмаслик карорига келиши мумкин, чунки у ёлғон бўлиши мумкин. Вактни белгилашдан фойдаланишда сеанснинг хақиқий эканлигини тасдиқлаш учун *кечикишнинг жоиз вақт оралиғи* муаммоси пайдо бўлади. Чунки, “вақт тамғаси”ли хабар, умуман, бир лахзада узатилиши мумкин эмас. Ундан ташқари, қабул қилувчи ва жўнатувчининг соатлари мутлақо синхронланган бўлиши мумкин эмас.

Аутентификация протоколларини таққослашда ва танлашда қуйидаги характеристикаларни ҳисобга олиш зарур:

- *ўзаро аутентификациянинг мавжудлиги.* Ушбу хусусият аутентификацион алмашинув тарафлари ўртасида иккиёклама аутентификациянинг зарурлигини акс эттиради;

- *ҳисоблаш самарадорлиги.* Протоколни бажаришда зарур бўлган амаллар сони;

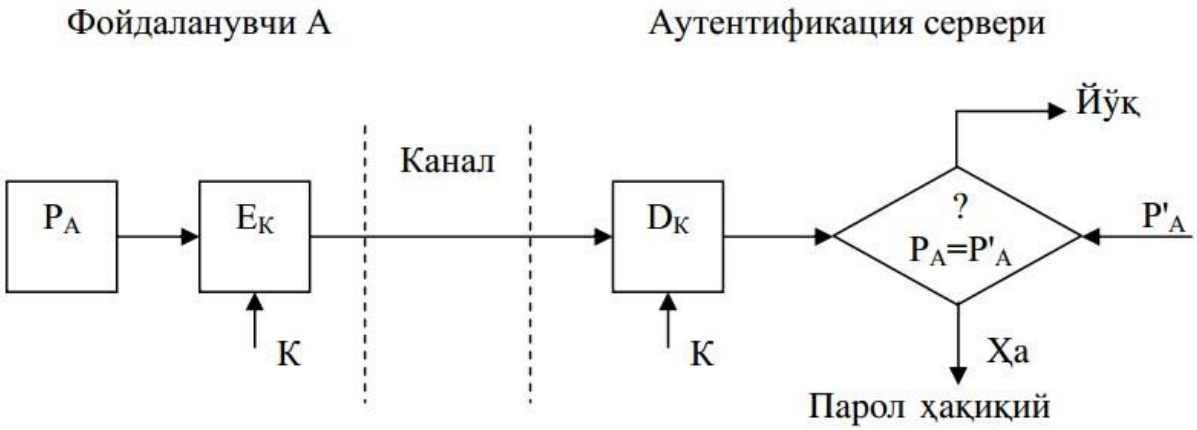
- *коммуникацион самарадорлик.* Ушбу хусусият аутентификацияни бажариш учун зарур бўлган хабар сони ва узунлигини акс эттиради;

- *учинчи тарафнинг мавжудлиги.* Учинчи тарафга мисол тариқасида симметрик калитларни тақсимловчи ишончли серверни ёки очиқ калитларни таксимлаш учун сертификатлар дарахтини амалга оширувчи серверни курсатиш мумкин;

- *хавфсизлик кафолати асоси.* Мисол сифатида нуллик билим билан исботлаш хусусиятига эга бўлган протоколларни кўрсатиш мумкин; - *сирни сақлаш.* Жиддий калитли ахборотни сақлаш усули кузда тутилади.

2. Пароллар асосида аутентификациялаш

Аутентификациянинг кенг тарқалган схемаларидан бири *оддий аутентификациялаш* бўлиб, у анъанавий кўп мартали паролларни ишлатишига асосланган. Тармоқдаги фойдаланувчини оддий аутентификациялаш муолажасини қуйидагича 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 бўйича маълумотлар базасидан мос ёзув топилади, ундан паролни топиб фойдаланувчи киритган парол билан таққосланади. Агар улар мос келса, аутентификация муваффакиятли ўтган хисобланади ва фойдаланувчи легал (қонуний) мақомини ва авторизация тизими орқали унинг мақоми учун аниқланган худудларни ва тармоқ ресурсларидан фойдаланишга рухсатни олади. Паролдан фойдаланган холда оддий аутентификациялаш схемаси 19.1-расмда келтирилган.



19.1-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_K ва расшифровка қилиш D_K воситалари киритилган. Бу воситалар бўлинувчи махфий калит К орқали бошқарилади. Фойдаланувчининг хақиқийлигини текшириш фойдаланувчи юборган парол P_A билан аутентификация серверида садланувчи дастлабки диймат P_A ни таддослашга асосланган. Агар P_A ва P_A қийматлар мос келса, парол P_A хақиқий, фойдаланувчи A эса қонуний хисобланади.

Оддий аутентификацияни ташкил этиш схемалари нафакат паролларни узатиш, балки уларни сақлаш ва текшириш турлари билан ажралиб туради. Энг кенг тарқалган усул - фойдаланувчилар паролини тизимли файлларда, очиқ ҳолда сакдаш усулидир. Бунда файлларга ўқиш ва ёзишдан химоялаш атрибутлари ўрнатилади (масалан, операцион тизимдан фойдаланишни назоратлаш рўйхатидаги мос имтиёзларни тавсифлаш ёрдамида). Тизим фойдаланувчи киритган паролни пароллар файлида сақланаётган ёзув билан солиштиради. Бу усулда шифрлаш ёки бир томонлама функциялар каби криптографик механизмлар ишлатилмайди. Ушбу усулнинг камчилиги - нияти бузуқ одамнинг тизимда маъмур имтиёзларидан, шу билан бирга тизим файлларидан, жумладан парол файлларидан фойдаланиш имкониятидир.

Хавфсизлик нуқтаи назаридан паролларни бир томонлама функциялардан фойдаланиб узатиш ва сақлаш қулай хисобланади. Бу ҳолда фойдаланувчи паролнинг очиқ шакли ўрнига унинг бир томонлама функциядан фойдаланиб олинган тасвирини юбориши шарт.

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 бўлмасин ва уларни топиш қийин бўлсин.

Бир мартали паролларга асосланган аутентификациялашда фойдаланишга хар бир сўров учун турли пароллар ишлатилади. Бир мартали динамик парол факат тизимдан бир марта фойдаланишга ярокди. Агар, хатто кимдир уни ушлаб крлса х,ам парол фонда бермайди. Одатда бир мартали паролларга асосланган аутентфикациялаш тизими масофадаги фойдаланув-чиларни текширишда кулланилади.

Бир мартали паролларни генерациялаш аппарат ёки дастурий усул орқали амалга оширилиши мумкин. Бир мартали пароллар асосидаги фойдаланишнинг аппарат воситалари ташқаридан тўлов пластик карточкаларига ухшаш

микропроцессор ўрнатилган миниатюр қурилмалар қуринишда амалга оширади. Одатда калитлар деб аталувчи бундай карталар клавиатурага ва катта бўлмаган дисплей дарчасига эга.

Фойдаланувчиларни аутентификациялаш учун бир мартали паролларни қўллашнинг қуйидаги усуллари маълум:

1. Ягона вақт тизимига асосланган вақт белгилари механизмидан фойдаланиш.
2. Легал фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар рўйхатидан ва уларнинг ишончли синхронлаш механиз мидан фойдаланиш.
3. Фойдаланувчи ва текширувчи учун умумий бўлган бир хил даст-лабки кийматли псевдотасодифий сонлар генераторидан фойдаланиш.

Биринчи усулни амалга ошириш мисоли сифатида SecureID аутентикациялаш технологиясини кўрсатиш мумкин. Бу технология Security Dynamics компанияси томонидан ишлаб чиқилган бўлиб, қатор компанияларнинг, хусусан Cisco Systems компаниясининг серверларида амалга оширилган.

Вақт синхронизациясидан фойдаланиб аутентификациялаш схемаси тасодифий сонларни вақтнинг маълум оралигидан сунг генерациялаш алгоритмига асосланган. Аутентификация схемаси қуйидаги иккита параметрдан фойдаланади:

- хар бир фойдаланувчига аталган ва аутентификация серверида ҳамда фойдаланувчининг аппарат калитида сакданувчи ноёб 64-битли сондан иборат махфий калит;
- жорий вақт қиймати.

Масофадаги фойдаланувчи тармоқдан фойдаланишга уринганида ундан шахсий идентификация номерини киритиш таклиф этилади. PIN тўртта ўнли рақамдан ва аппарат калити дисплейида аксланувчи тасодифий соннинг олтита рақамидан иборат. Сервер фойдаланувчи томонидан киритилган PIN-коддан фойдаланиб маълумотлар базасидаги фойдаланувчининг махфий калити ва жорий вақт киймати 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 калит ва сервернинг қатъий вақтий синхронланиши талаб этилади. Чунки аппарат калит

бир неча йил ишлаши ва демак сервер ички соати билан аппарат калитининг мувофиқлиги аста-секин бузилиши мумкин.

Ушбу муаммони ҳал этишда Security Dynamics компанияси қуйидаги икки усулдан фойдаланади:

- аппарат калити ишлаб чикилаётганида 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 туғилганида ушбу калитга мослашади.

Аутентификациянинг бу схемаси билан яна бир муаммо боғлиқ. Аппарат калит генерациялаган тасодифий сон катта бўлмаган вақт оралиғи мобайнида хақиқий парол хисобланади. Шу сабабли, умуман, қисқа муддатли вазият содир бўлиши мумкинки, хакер PIN-кодни ушлаб қолиши ва уни тармоқдан фойдаланишга ишлатиши мумкин. Бу вақт синхронизациясига асосланган аутентификация схемасининг энг заиф жойи хисобланади.

Бир мартали паролдан фойдаланувчи аутентификациялашни амалга оширувчи яна бир вариант – “сўров-жавоб” схемаси бўйича 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 хотирасида ва серверниг маълумотлар базасида сақланувчи махфий калити ёрдамида расшифровка қилади. Тасодифий сон - сўров шифрланган кўринишда серверга қайтарилади. Сервер хам ўз навбатида ўша DES алгоритми ва серверниг маълумотлар 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 схемаси ишлатишда вақт синхронизациясидан фойдаланувчи аутентификация схемасига қараганда мураккаброқ.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг иккинчи усули фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар рўйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланишга асосланган. Бир мартали паролларнинг бўлинувчи рўйхати махфий пароллар кетма-кетлиги ёки тўплами бўлиб, хар бир парол фақат бир марта ишлатилади. Ушбу рўйхат аутентификацион алмашинув тарафлар ўртасида олдиндан таксимланиши шарт. Ушбу усулнинг бир вариантига биноан

сўров-жавоб жадвали ишлатилади. Бу жадвалда аутентификацилаш учун тарафлар томонидан ишлатилувчи сўровлар ва жавоблар мавжуд бўлиб, хар бир жуфт факат бир марта ишлатилиши шарт.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг учинчи усули фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки кийматли псевдотасодифий сонлар генераторидан фойдаланишга асосланган. Бу усулни амалга оширишнинг қуйидаги вариантлари мавжуд:

- *ўзгартирилувчи бир мартали 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 ташкил этади. Хавфсизлик нуктаи назаридан бу усул кетма-кет ўзгартирилувчи пароллар усулига нисбатан афзал ҳисобланади.

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

3. Сертификатлар асосида аутентификациялаш

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

Рақамли сертификатлар ишлатилганида компьютер тармоғи фойдаланувчилари хусусидаги хеч қандай ахборотни сакламайди. Бундай ахборотни фойдаланувчиларнинг ўзи сўров-сертификатларида тақдим этадилар. Бунда махфий ахборотни, хусусан махфий калитларни сақлаш вазифаси фойдаланувчиларнинг ўзига юкланади.

Фойдаланувчи шахсини тасдикдовчи рақамли сертификатлар фойдаланувчилар сўрови бўйича махсус ваколатли ташкилот-сертификация маркази CA (Certificate Authority) томонидан, маълум шартлар бажарилганида

берилади. Таъкидлаш лозимки, сертификат олиш муолажасининг ўзи хам фойдаланувчининг хақиқийлигини текшириш (яъни, аутентификациялаш) боскичини ўз ичига олади. Бунда текширувчи тараф сертификацияловчи ташкилот (сертификация маркази СА) бўлади.

Сертификат олиш учун мижоз сертификация марказига шахсини тасдиқловчи маълумотни ва очиқ калитини тақдим этиши лозим. Зарурий маълумотлар рўйхати олинадиган сертификат турига боғлиқ. Сертификацияловчи ташкилот фойдаланувчининг хақиқийлиги тасдиғини текширганидан сўнг ўзининг рақамли имзосини очиқ калит ва фойдаланувчи хусусидаги маълумот бўлган файлга жойлаштиради ҳамда ушбу очиқ калитнинг муайян шахсга тегишли эканлигини тасдиқлаган ҳолда фойдаланувчига сертификат беради.

Сертификат электрон шакл бўлиб, таркибида қуйидаги ахборот бўлади:

- ушбу сертификат эгасининг очиқ калити;
- сертификат эгаси хусусидаги маълумот, масалан, исми, электрон почта адреси, ишлайдиган ташкилот номи ва ҳоказо;
- 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 нафакат аутентификациялашда, балки фойдаланишнинг маълум хукукларини тақдим этишда ишлатилиши мумкин. Бунинг учун сертификатга қўшимча хошиялар киритилиб уларда сертификация эгасининг фойдаланувчиларнинг у ёки бу категориясига мансублиги кўрсатилади.

Очиқ калитларнинг сертификатлар билан узвий боғлиқлигини алохида таъкидлаш лозим. Сертификат нафакат шахсни, балки очиқ калит мансублигини тасдиқловчи хужжатдир. Рақамли сертификат очиқ калит ва унинг эгаси ўртасидаги мосликни урнатади ва кафолатлайди. Бу очиқ калитни алмаштириш хавфини бартараф этади.

Агар абонент ахборот алмашинуви бўйича шеригидан сертификат таркибидаги очиқ калитни олса, у бу сертификатдаги сертификация марказининг рақамли имзосини ушбу сертификация марказининг очиқ калити ёрдамида текшириш ва очиқ калит адреси ва бошқа маълумотлари сертификатда кўрсатилган фойдаланувчига тегишли эканлигига ишонч ҳосил қилиши мумкин.

Сертификатлардан фойдаланилганда фойдаланувчилар рўйхатини уларнинг пароллари билан корпорация серверларида сақлаш зарурияти йуқолади. Серверда сертификацияловчи ташкилотларнинг номлари ва очиқ калитларининг бўлиши етарли.

Сертификатларнинг ишлатилиши сертификацияловчи ташкилотларнинг нисбатан камлигига ва уларнинг очиқ калитларидан қизиққан барча шахслар ва ташкилотлар фойдалана олиши (масалан, журналлардаги нашрлар ёрдамида) тахминига асосланган.

Сертификатлар асосида аутентификациялаш жараёнини амалга оширишда сертификацияловчи ташкилот вазифасини 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 берилишидаги дастлабки аутентификациялаш муолажасини осонлаштиради. Корхоналар сертификатларни генерациялаш, бериш ва уларга хизмат курсатиш жараёнларини автоматлаштиришни таъминловчи мавжуд дастурий махсулотлардан фойдаланишлари мумкин. Масалан, Netscape Communications компанияси серверларини корхоналарга шахсий сертификатларини чикариш учун таклиф этади.

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

4. Қатъий аутентификациялаш

Криптографик протоколларида амалга оширилувчи қатъий аутентификациялаш ғояси қуйидагича. Текширилувчи (исботловчи) тараф қандайдир сирни билишини намойиш этган ҳолда текширувчига ўзининг ҳақиқий эканлигини исботлайди. Масалан, бу сир аутентификацион алмашиш тарафлари ўртасида олдиндан хавфсиз усул билан таксимланган бўлиши мумкин. Сирни билишлик исботи криптографик усул ва воситалардан фойдаланилган ҳолда сўров ва жавоб кетма-кетлиги ёрдамида амалга оширилади.

Энг мухими, исботловчи тараф фақат сирни билишлигини намойиш этади, сирни ўзи эса аутентификацион алмашиш мобайнида очилмайди. Бу текширувчи тарафнинг турли сўровларига исботловчи тарафнинг жавоблари ёрдами билан

таъминланади. Бунда якуний сўров фақат фойдаланувчи сирига ва протокол бошланишида ихтиёрий танланган катта сондан иборат бошланғич сўровга боғлиқ бўлади.

Аксарият холларда қатъий аутентификациялашга биноан ҳар бир фойдаланувчи ўзининг махфий калитига эгалиги аломати бўйича аутентификацияланади. Бошкдча айтганда фойдаланувчи унинг алоқа бўйича шеригининг тегишли махфий калитга эгалигини ва у бу калитни ахборот алмашинуви бўйича хақиқий шерик эканлигини исботлашга ишлата олиши мумкинлигини аниқлаш имкониятига эга.

Х.509 стандарти тавсияларига биноан қатъий аутентификациялашнинг қуйидаги муолажалари фарқланади:

- бир томонлама аутентификация;
- икки томонлама аутентификация; − уч томонлама аутентификация.

Бир томонлама аутентификациялаш бир томонга йўналтирилган ахборот алмашинувини кўзда тутади. Аутентификациянинг бу тури қуйидагиларга имкон яратади:

- ахборот алмашинувчининг фақат бир тарафини хақиқийлигини тасдиқлаш;
- узатилаётган ахборот яхлитлигининг бўзилишини аниқлаш;
- “узатишнинг такрори” типидаги хужумни аниқлаш;
- узатилаётган аутентификацион маълумотлардан фақат текширувчи тараф фойдаланишини кафолатлаш.

Икки томонлама аутентификацилаш бир томонлилигига нисбатан исботловчи тарафга текширувчи тарафнинг қўшимча жавоби бўлади. Бу жавоб текширувчи томонни алоқанинг айнан аутентификация маълумотлари мўлжалланган тараф билан ўрнатилаётганига ишонтириш лозим.

Уч томонлама аутентификациялаш таркибида исботловчи тарафдан текширувчи тарафга қўшимча маълумотлар узатиш мавжуд. Бундай ёндашиш аутентификация утказишда вақт белгиларидан фойдаланишдан воз кечишга имкон беради.

Таъкидлаш лозимки, ушбу туркумлаш шартлидир. Амалда ишлатилувчи усул ва воситалар тўплами аутентификация жараёнини амалга оширишдаги муайян шарт-шароитларга боғлиқ. Қатъий аутентификациянинг ўтказилиши ишлатиладиган криптографик алгоритмлар ва қатор қўшимча параметрларни тарафлар томонидан сўзсиз мувофиқлаштиришни талаб этади.

Қатъий аутентификациялашнинг муайян вариантларини қуришдан олдин бир мартали параметрларнинг вазифалари ва имкониятларига тўхташ лозим. Бир мартали параметрлар баъзида “nonces” - бир мақсадга бир мартадан ортиқ ипшатилмайдиган катталик деб аталади.

Хозирда ишлатиладиган бир мартали параметрлардан тасодифий сонлар, вақт белгилари ва кетма-кетликларнинг номерларини кўрсатиш мумкин.

Бир мартали параметрлар узатишнинг такрорланишини, аутентификацион алмашинув тарафларини алмаштириб қўйишни ва очиқ матнни танлаш билан хужум қилишни олдини олишга имкон беради. Бир мартали параметрлар ёрдамида узатиладиган хабарларнинг ноёблигини, бир маънолилигини ва вақтий кафолатларини таъминлаш мумкин. Бир мартали параметрларнинг турли хиллари алоҳида ишлатилиши, ёки бир-бирини тўлдириши мумкин.

Бир мартали параметрларнинг қуйидаги ишлатилиш мисолларини курсатиш мумкин:

- “сўров-жавоб” принципида қурилган протоколларда ўз вақтидалигини текшириш. Бундай текширишда тасодифий сонлар, соатларни синхронлаш билан вақт белгилари ёки муайян жуфт (текширувчи, исботловчи) учун кетмакетликларнинг номерларидан фойдаланиш мумкин;
- ўз вақтидалигини ёки ноёблик кафолатини таъминлаш. Протоколнинг бир мартали параметрларини бевосита ёки билвосита назоратлаш орқали амалга оширилади;
- хабарни ёки хабарлар кетма-кетлигини бир маъноли идентификациялаш. Бир охангда усувчи кетма-кетликнинг бир мартали қийматини ёки мос узунликдаги тасодифий сонларни тўзиш орқали амалга оширилади.

Таъкидлаш лозимки, бир мартали параметрлар криптографик протоколларнинг бошқа вариантларида хам кенг қўлланилади.

Қатъий аутентификациялаш протоколларини қўлланиладиган криптографик алгоритмларига боғлиқ ҳолда қуйидаги гуруҳдарга ажратиш мумкин:

- шифрлашнинг симметрик алгоритмлари асосидаги катъий аутентификациялаш протоколлари;
- бир томонлама калитли хеш-функциялар асосидаги катъий аутентификациялаш протоколлари;
- шифрлашнинг асимметрик алгоритмлари асосидаги қатъий аутентификациялаш алгоритмлари;

- электрон рақамли имзо асосидаги катъий аутентификациялаш алгоритмлари.

Назорат саволлари

1. Идентификация нима?
2. Индентификаторлар нима?
3. Аутентификация нима?
4. Авторизация нима?
5. Маъмурлаш нима?
6. Пароллар асосида аутентификациялаш.
7. Сертификатлар асосида аутентификациялаш
8. Қатъий аутентификациялаш.

Адабиётлар ва интернет ресурслар

1. Computer networking : a top-down approach / James F. Kurose, Keith W. Ross.—6th ed. 2013. by Pearson Education, Inc., publishing as AddisonWesley.
2. TCP/IP protocol suite / Behrouz A. Forouzan.—4th ed. Published by McGraw-Hill, a business unit of The McGraw-Hill Companies, Inc., 1221 Avenue of the Americas, New York, NY 10020. Copyright © 2010
3. Java Network Programming, Fourth Edition by Elliotte Rusty Harold. 2014. Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol
4. www.security.uz
5. www.cert.uz