Каримов М.М., Файзиева Д.С., Ҳакимов Ҳ.

Масофавий таълимда ахборот хавфсизлигининг иерархик тизими

Аннотация. Масофавий таълим тизимининг ахборот ресурслари иерархик схемага асосланган рухсатли структура сифатида қаралмоқда. Иерархик класслар ва класс ости класслари ҳамда вақт интервали асосида очиқ ва ёпиқ калит генерацияси алгоритми ишлаб чиқилди. Ахборот-коммуникацион структура ва ахборот алмашиниш учун иккита протокол таклиф этилди.

Калит сўзлар: Масофавий таълим, иерархик тизим, тизим маъмури, синфлар иерархияси, спуфинг

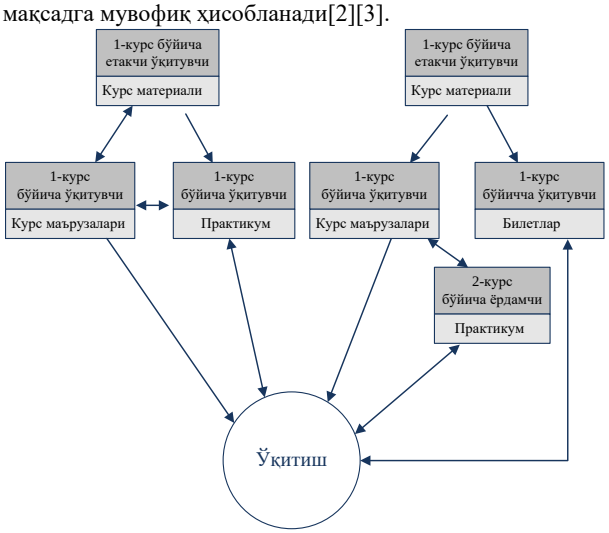
Кириш

Охирги йилларда масо- фавий таълим тизимлари айтарли даражада ривожланди. Ушбу тизимлар назарий ахборотни оператив тарзда олишга, амалий машғулотларни бир неча километр узоқдаги ўқитувчи кўмагида бажаришга, интернет-маърузалар, семинарларда ва ҳ. иштирок этишга имкон беради [1].

Масофавий курслар кўпинча пуллик бўлганлиги сабабли, ахборотни рухсатсиз фойдаланишдан ҳимоялаш зарурати туғилади. Албатта, энг ишончли ҳимоялаш усули – ахборотни шифрлаш, аммо бу усул ҳам бўлиши мумкин бўлган ахборотнинг сирқиб чиқишининг (утечка) бартараф эта олмайди.

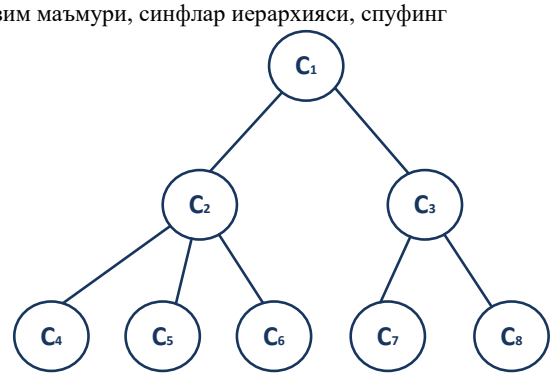
Масофавий таълим тизимида фойдаланувчиларнинг аниқ иерархияси мавжуд. Тизим маъмури масофавий таълим тизимини назорат қилади ва, одатда, барча маълумотлардан фойдалана олади. Тизимдаги етакчи ўқитувчилар эса ўқув фанларини олиб уни қисман модификациялаш, ўқув дастурларини яратиш имкониятларига эга бўлишлари лозим. Амалий машғулотларини олиб борувчилар курс маърузаларидан фойдалана олишлари ва амалий топшириқларини яратиш имкониятига эга бўлишлари лозим. Таълим олувчилар эса фақат шахсий маълумотларига тегишли ахборотдан (ҳисоботлар, назорат натижалари ва ҳ.) фойдаланишлари мумкин 1-расм.

Ушбу ҳолда оддий шифрлаш билан масалани ҳал қилиб бўлмайди, чунки кўпгина фойдаланувчилар калитларини билишларига тўғри келади. Бунда калитларнинг “сирқиб чиқиши, калитларнинг катта сони бўйича чалкашликлар муқаррар. Натижада, маъмур вазифалари ортади ва ахборотдан рухсатсиз фойдаланиш содир бўлади. Шифрлашнинг иерархик схемасига асосланган ҳимоянинг иерархик тизимдан фойдаланиш мақсадга мувофиқ ҳисобланади[2][3].



1-расм.Масофавий таълим тизими фойдаланувчиларининг қисқартирилган схемаси

Умумий ҳолда синфлар иерархияси 2-расмда келтирилган кўринишга эга.



2-расм. Синфлар иерархиясининг кўриниши

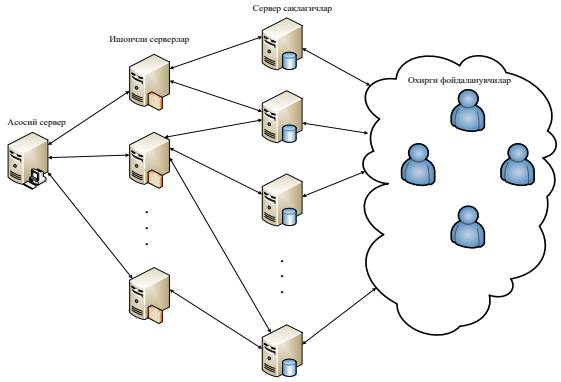
Иерархик ахборотдан фойдаланишни бошқариш масаласини кўрайлик. Айтайлик, $C_i(i=\overline{1,m})$ ахборот синфлари. Фараз қилайлик синфлар қандайдир бинар муносабат " $\leq$ " ёрдамида тартибланган. Бу ҳолда қуйидаги талаб ўринли: агар фойдаланувчи C_i синфидан фойдалана олса, у $C_j \in C_i$ каби ҳар қандай синфдан фойдалана олиши лозим.

Ахборотни рухсатсиз фойдаланишдан ҳимоялаш учун ҳар бир C_i синфга k_i. калит белгиланади ва ушбу синфдаги барча ахборот k_i калит ёрдамида шифрланади. Шундай қилиб, фойдаланувчи C_i синфдан фойдаланиш ҳуқуқини олиб, k_i калит билан бирга барча пастки синфлар калитларини сақлаши лозим. Бу жуда ноқулай[4].

Яна бир муаммо пайдо бўлади – C_i синфга k_i калитни шундай белгилаш лозимки, уни фақат $C_j \in C_i$ шартни қаноатлантирувчи синфлар учун k_j калитни ҳисоблаб аниқлашда ишлатиш имкони бўлсин. Бунда ҳар бир фойдаланувчи, ўзининг мақомига кўра, қандайдир синфга рўйхатдан ўтиши лозим. Сўнгра у калитни олиб синфдаги маълумотларни дешифрлаши мумкин. Унинг устига, у C_j синфдаги маълумотларни ҳам, агар $C_j \in C_i$ шарти бажарилса, дешифрлаши мумкин.

Масофавий таълим тизимидаги маълумотлар сақлагичида курс материаллари, амалий топшириқлар, уларнинг ечими, фойдаланувчиларнинг шахсий маълумотлари, имтихон натижалари хусусидаги ва ҳ. маълумотлар сақланади. Фойдаланишни ажратиш, синфларни ва фойдаланиш ҳуқуқларини эътиборга олиш ҳамда маълумотлардан умумий фойдаланиш –ушбу тизимнинг ишга лаёқатлигини белгиловчи асосий жиҳатлар. Хавфсизликнинг иерархик тизими фойдаланувчиларнинг катта сонида ва маълумотларнинг умумийлигида маълумотларни ҳимоялаш учун етарлича қулай восита ҳисобланади.

Маълумки, шифрлаш ҳимоя тизимининг энг муҳим қисми ҳисобланади. Аммо, компьютер тармоғида ҳимоя тизимининг амалга оширилишида қатор омиллар пайдо бўладики, бу омиллар ҳимоянинг мураккаб серверлар схемасини ишлаб чиқишни талаб этади. 1–расмда хавфсизликнинг иерархик тизими серверларининг структураси келтирилган[5].



3-расм. Хавфсизликнинг иерархик тизими серверларининг структураси

Хавфсизликнинг асосий сервери тамомила физик изоляцияланган ва ундан фақат “ишончли” деб аталувчи серверлар фойдалана олади.

Ишончли серверлар маълумот сақлагичлари учун авторизацияловчи сервер вазифасини ҳам бажаради ва зарурият туғилганда охирги фойдаланувчиларга калитларни тақдим этади. Бу ишончли серверга хужумнинг калитларнинг ва бошқа тизим параметларининг йўқолишига ёки сирқиб чиқишига (утечка), ҳамда асосий сервер фаолиятининг тўхташига олиб келмаслигига ишонч ҳосил қилишга имкон беради. Қандайдир ишончли сервер ишламай қолганида унинг вазифасини бошқа ишончли сервер олиши мумкин. Бу ишончли серверларга юкламани мувозанатлашга имкон беради, чунки улар тенг ҳуқуқли ҳисобланади.

Ишончли серверлар фақат транспорт вазифасини ўтайди. Уларнинг сақлагичга ёки муайян фойдаланувчига йўлланган маълумотларни дешифрлашлари мумкин эмас. Аммо,ишончли сервер тармоқ трафигининг сохталаштирилишини (спуфинг) бартараф этиш мақсадида доимо баъзи назорат маълумотларини олади.

Маълумотлар сақлагичлар туб маънода сақлагич ҳисобланади. Уларнинг ишончли серверлар билан фаол ўзаро таъсирига қарамай,уларда сақланувчи маълумотлар хавфсизлик синфлари иерархияси тизимига боғлиқ эмас. Маълумотларнинг сервер-сақлагичи қандайдир иерархиянинг мавжудлигини “билмайди”, у фойдаланувчининг аутентификациясини/авторизациясини ўтказади ва унга, ишончли сервердан олинган вақтинча калит ёрдамида шифрланган маълумотларни узатади.

Маълумотлар электрон почта орқали дискетда файллар ва ҳ. кўринишида тарқатилиши мумкин. Бу ҳолларда битта ҳам ихтисослаштирилган сервер керак бўлмайди. Кўпчилик фойдаланувчиларга тарқатишда битта пакет ишлатилиши мумкин. Ҳар бир фойдаланувчи фақат ўзига ва қуйи синфларга аталган пакет қисмини дешифрлаши ва ўқитиши мумкин [6].

EFS (Encrypting Files System) каби кенг ёйилган тизимлар фойдаланувчи калити йўқолганида маълумотларни тиклаш мумкин эмас, чунки фойдаланувчи калити “юқори” фойдаланувчилар калитидан ҳисоблаб аниқланмайди, балки хавфсизликнинг маълумотлар базасида сақланади. Ундан ташқари, EFS иерархик эмас, балки фойдаланиш бўйича ажратилган тизим ҳисобланади, яъни унда фойдаланувчи синфлари мавжуд эмас.

Хавфсизликнинг иерархик тизимида махфий калитлар йўқолганида маълумотларни тиклаш шахсий калит ва маъмурнинг ёки “юқори” фойдаланувчиларнинг очиқ маълумотлари ёрдамида амалга оширилиши мумкин. Ушбу калитлардан “қуйи” фойдаланувчилар маълумотларини дешифрлаш учун барча калитлар осонгина ҳисоблаб аниқланади. Шу сабабли, хавфсизлик тизими иерархияси тикланганидан сўнг барча маълумотларни янги калитлар ёрдамида дешифрлаш ва қайта шифрлаш имконияти доимо мавжуд. Масофавий таълим тизимида маълумотларни дешифрлаш учун курсни олиб борувчи барча ўқитувчиларнинг калитлари керак бўлади, чунки маъмур тизимнинг “юқори” фойдаланувчиси ҳисобланмайди.

Асосий сервер, моҳиятан, тизим ядроси ҳисобланади. Тизимни ишга тушириш босқичида асосий серверда, фойдаланувчилар синфлари иерархиясининг редактори ёрдамида иерархик тизим структураси яратилади. Сўнгра хавфсизликнинг асосий серверининг хизмати ишга туширилади. Ушбу хизмат ишончли серверларнинг (фақат ишончли серверларнинг) сўровларига жавоб беради. Асосий серверининг ташқи тармоқдан изоляцияланганлиги “сохта” сўровларнинг йўқлигига ишонч ҳосил қилишга имкон беради. Аммо, бари бир маълумотларни асосий сервер ва ишончли сервер орасида узатишда ушбу ишончли сервер синфининг калити ёрдамида шифрлаш ишлатилади[7].

Асосий сервер ва сервер-сақлагичлар ҳамда охирги фойдаланувчилар орасида маълумотларни узатишда ушбу серверлар фойдаланувчилар калитлари ёрдамида шифрлаш ишлатилади. Бу ишончли сервер операторига маълумотларни ўқишга имкон бермайди. Хавфсизликнинг иерархик тизимида махсус ишлаб чиқилган протоколлар билан бир қаторда стандарт протоколлардан фойдаланиш имконияти мавжуд. Бу HTTP (Hyper Text Transfer Protocol-гиперматнли файлларни узатиш протоколи) ва ёки XML (Extensible Markup Language-белгилашнинг кенгайтирилган тили) билан қўшилувчи ҳар қандай муҳитда тизимни ишга туширишга имкон беради:

Ишончли серверлар “ташқи дунё” серверларининг асосий сервер билан алмашинишида “воситачи” вазифасини бажаради. Масалан, ишончли сервер маълумотларни сақловчи сервердан фойдаланувчини аутентификациялаш сўровини олиб, ушбу сўровни хавфсизликнинг асосий серверига йўллайди, сўнгра олинган шифрланган натижани аутентификацияни сўраган серверга жўнатади.

Маълумотларни сервер-сақлагичлари охирги фойдаланувчиларга маълумотлардан фойдаланиш хизматини тақдим этувчи оддий серверлардир. Сервер-сақлагичлар учун ишончли серверга сўров ёрдамида фойдаланувчининг аутентификацияси ишлатилади. Фойдаланувчига узатилувчи маълумотлар, унга берилган вақтинчалик калит ёрдамида шифрланади. Сервер-сақлагичлар фойдаланувчи билан мулоқотда HTTPдан фойдаланади.

Фойдаланувчилар маълумотларни сўраши ёки уларни серверга жойлаши мумкин. Фойдаланувчининг маълумотларни сўраш /жойлаш ҳуқуқи сервер воситалари ёрдамида белгиланади. Хавфсизликнинг иерархик тизими фойдаланувчининг ҳар қандай маълумотларни олиши мумкинлигини, аммо маълумотлар сақланганида синфни чеклаш кучга киришини кўзда тутади.

Хулоса

Масофавий таълим тизимларидаги маълумот сақлагичларида курс материаллари амалий машғулотлар, уларнинг ечими (ўқитувчилар ва фойдаланувчиларнинг), фойдаланувчиларнинг шахсий маълумотлари, имтихон натижалари ва уларнинг хусусидаги маълумотлар бўлади. Фойдаланишнинг ажратилиши, синфлар ва

фойдаланувчилар ҳуқуқларининг аниқ ҳисобга олиниши ҳамда маълумотлардан умумфойдаланишлик ушбу тизимнинг ишга лаёқатлигини белгиловчи асосий жиҳатларидир. Хавфсизликнинг иерархик тизими фойдаланувчиларнинг катта сони ва маълумотларнинг умумийлиги ҳолида маълумотларни ҳимоялаш учун етарлича қулай восита ҳисобланади.

Фойдаланилган адабиётлар

[1] Mason, R. and Rennie, F. (2006), E-learning: the key concepts, Routledge, Abingdon Great Britain.

[2] Cyber security and universities: managing the risk Universities UK, November 2013.

[3] May M. and George S. (2011). Privacy concerns in e-Learning: Is using a tracking system a threat? International Journal of Information and Education Technology 2011, Volume 1, Number 1.

[4] Alw N. and Fan I.-S. (2010). E-Learning and Information Security Management. International Journal of Digital Society, vol. Volume 1, no. Issue 2.

[5] Yong Chen and Wu He. Security Risks and Protection in Online Learning: A Survey. Old Dominion University, USA.

[6] Najwa Hayaati Mohd Alwi, Ip-Shing Fan. E-Learning and Information Security Management. Cranfield University, UK. International Journal of Digital Society (IJDS), Volume 1, Issue 2, June 2010

[7] Balta, O.C., N. Simsek, N. Tezcan. 2009. A Web Based Generation System for Personalization of E-Learning Materials. WCSET- World Congress on Science, Engineering, and Technology, Dubai, United Arab Emirates.

Каримов Мажид Маликович
т.ф.д., профессор
Тел: +998 (94) 667-29-37
Эл. почта: dr.mmkarimov@rambler.ru
Файзиева Дилсора Салимовна
таянч докторант
Тел: +998 (90) 971-64-46
Эл. почта: dilsora.salimovna@gmail.com
Ҳакимов Ҳожиакбар Бахром ўғли
Мухаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети “Ахборот хавфсизлигини таъминлаш” кафедраси магистри
Тел: +998 (97) 407-29-37
Эл. почта: hakimovhojiakbarb@gmail.com

Annotation. Information resources of remote training system are considered a structure with hierarchical access scheme. There was developed the open and secret keys generation algorithm, based on hierarchical classes and subclasses, and also on a time interval. The infocommunication structure is suggested along with two protocols of information interchange.

Key Words: Distance learning, hierarchical system, system administrator, class hierarchy, spufing

Тел: +998 (97) 407-29-37
Эл. почта: hakimovhojiakbarb@gmail.com