ЭЛЕКТРОН ТЎЛОВЛАР ТИЗИМЛАРИНИ ҲИМОЯЛАШ УЧУН СМАРТ-КАРТАЛАРДАН ФОЙДАЛАНИШ

Араббаев Аробидин Хуснидинович
Андижон давлат университети

Аннотация: Электрон тўловлар тизимларида ахборот хавфсизлигини таъминлашни ошириш бўйича йўриқномалар ишлаб чиқилди. Бундан ташқари мавжуд протоколлардан фойдаланиб электрон тўловлар тизимининг хавфсиз моделини ва электрон транзакцияларнинг химоялаш бўйича йўриқнома ишлаб чиқиш тадқиқоти ўрганилган. Қўйилган масала хозирги ахборот тизимларининг характеристикаларини уларнинг хавфсизлигини таъминланиши нуқтаи назардан тахлил, электрон тўлов тизимларининг асосий тахлика ва бардошлилигини тахлил қилинган.

Калит сўзлар: тўлов, электрон, смарт-карта, хотира, ҳимоя, терминал, банк, тижорат, калит, карта.

Электрон тўловлар тизимларнинг мухим вазифаларидан бири хавфсизликни таъминловчи воситалардан фойдаланишдир. Бу масала комплекс характерга эга. Унинг бир аспектини кўриб чиқамиз – тўлов тизимининг аппарат-дастурий объектларида айланувчи ахборотни ҳимоялаш.

Тўлов тизимининг техник объектлари. Тўлов тизимининг техник объектларига қуйидагилар киради:

- тўлов смарт-картаси (бир кристалли махсуслаштирилган процессорли карточка, бу процессор узоқ муддатли ҳимояланган хотира, стандартлашган ўлчамлар ва интерфейсга эга бўлади);
- ўқиш/ёзиш қурилмаси (смарт-карта киритилувчи алохида интерфейс қурилмаси ёки терминал ичидаги қурилма, смарт-карта билан алоқа ўрнатувчи механик ва электр қурилмалар);
- бевосита смарт-карта билан амаллар бажарувчи ва транзакцияларни қайта ишлаш марказига ахборотни юбориш учун терминал жихозлар (савдо терминаллари, касса аппаратлари, банкоматлар ва бошқа қурилмалар);
- смарт-карталарни персонализация қилишни автоматлаштирилган иш жойи (АИЖ) (смарт-карталарга ахборотни ўқиш/ёзиш қурилмали шахсий компьютер);
- банк операционистини АИЖи (ўқиш/ёзиш қурилмали шахсий компьютер);
- банк-эквайер, банк-эмитент, процессинг марказларнинг ишчи станцияси (ўқиш/ёзиш қурилмали шахсий компьютер);
- банк-эквайер, банк-эмитент, процессинг марказларнинг сервери;

• юқорида айтилган компонентларни боғловчи алоқа каналлари.

Тўлов смарт-картасида одатда қуйидаги ахборот жойлаштирилади:

• шифрлаш ва имзо калитлари (бир нечта калит тўпламлари бўлиши мумкин: аутентификация калити, процессинг маркази билан алоқа ўрнатиш калитлари, кредитлаш ва дебетлаш учун калитлар ва б.);

• пул борлиги, бажарилган транзакциялар ва б. хақида ахборотлар.

Тўлов тизимининг хавфсизлигини таъминлашнинг асосий тамойиллари:

Тўлов тизимининг субъектларини идентификациялаш ва аутентификациялаш. Хар қайси амални бажаришдан олдин белгиланади: смарт-карталарни чиқарувчи ташкилот, банк, тижоратчи ташкилот, смарт-карта эгаси.

Смарт-карта чиқарувчи ташкилотни маълумотлари ва смарт карта рақами бир марта дастурланувчи хотирага ёзилади ва аппарат усулида ўзгартирилишдан ҳимояланади.

Банк ва смарт карта эгаси хақидаги маълумотлар эмитент банкнинг процессинг марказида керакли калитлар тақдим этилганда ўзгартирилиши мумкин.

Тижорат ташкилот хақидаги маълумотлар сервис ташкилотнинг терминалига бевосита тегишли технологик смарт-карталардан банклар калитлари билан ёки кассир ва сотувчиларни смарт-карталаридан киритилади.

Идентификациякелаш ва аутентификациялаш симметрик ва ассиметрик криптография усуллар асосида бажарилиши керак. Буларни бажариш учун дастурий ва аппарат усулларда амалга оширилган шифрлаш ва имитоқўйишни ҳисоблаш, хэшлаш ва электрон рақамли имзо функцияларни библиотекаларидан фойдаланиш мумкин.

Маълумотларни бутунлигини текшириш. Тизим тизимдаги ёки смарт картадаги маълумотлар хуқуқи йўқ фойдаланувчилар томонидан ўзгартиришини олдини олинганлигини кафолатлаши керак. Шифрланувчи тизимларда маълумотларни бутунлигини банкларни махфий калитлар асосида ҳисобланган имитоқўйииш билан тасдиқлаш мумкин. Бажарилган амаллар (транзакциялар) хақидаги ахборотни бутунлиги амал қатнашувчилари (мижоз, кассир, сотувчи) махфий калитлари асосида ҳисобланган имитоқўйишлар билан тасдиқланади. Электрон имзоли тизимлар учун имито қўйиш ўрнига электрон рақамли имзодан фойдаланиш ва уни хақиқийлигини аввал сертификатланган очиқ калитлар ёрдамида текшириш мумкин. Ишлатилаётган қурилмаларнинг имкониятига кўра иккала усулни комбинациясидан фойдаланиш мумкин.

Ахборот келиб чиқишини аниқлаш. Тизимнинг барча келишув ва маълумотлари уларнинг келиб чиқиши ва мақсадини идентификацияловчи

ахборот билан таъминланган бўлиши керак. Хар бир амал бажарилганда сана ва вақти, унда қатнашадиган субъект ва объектлар фиксацияланади. Операция хақидаги ахборот хар бир қатнашувчининг сертификатлари билан тасдиқланади (имито қўйиш ёки электрон имзо билан). Операциянинг хақиқийлигини унинг қатнашчиларини тегишли калитлари асосида текшириш мумкин бўлади. Бу калитларни қатнашувчи ва банк билади.

Маълумотларни махфийлигини таъминлаш. Тизим маълумотларни конфиденциаллигини кафолатлаши керак. Маълумотларни фақат тизимга киришга рухсати бор фойдаланувчи кўриши мумкин бўлиши керак. Махфийлик алоқа каналларида ва қурилмалар ичида шифрлашдан фойдаланиш билан кафолатланади.

ШК базасидаги жихозларга рухсатни чегаралаш учун рухсат этилмаган киришдан ҳимояловчи тизимдан фойдаланиш керак. ШКни тармоқ ва алоқа каналлари томонидан ҳимоялаш учун “мусаффо” шифрловчи коммуникацион дастурлардан ёки криптошлюз ва криптомаршрутизаторлардан фойдаланиш керак.

Кредит операцияларни ҳимоялаш. Кредит операциялари бевосита банкда ёки on-line режимида ўтказилиши керак. Уларни кредитни маълум миқдорлари учун off-line режимида ўтказишга хам рухсат берилади. Тизим кредит операцияларини ўтказилишини (пулни ҳисобдан смарт картага ўтказиш) қуйидаги йўллар билан ҳимоялаши керак:

- смарт-карта хақиқийлигини банк томонидан текшириш;
- банк терминалини хақиқийлигини текшириш;
- PIN код бўйича карточка эгасини анифлаш;
- тасдиқловчи электрон сертификатни яратиш;
- бажарилган операцияни сертификат билан тасдиқлаш;
- фирибгарлик уринишида смарт картани вақтинча ўчириш ва тиклаш имкони.

Off-line режимида ишловчи терминаллар электрон имзони текширишни билса кредит миқдори банкнинг махсус калити билан имзоланади (сертификат яратиш). Бўлмаса банк ва мижоз хамма маълумотларига, бунинг ичида кредит миқдорига хам, ититоқўйиш шакллантирилади. Бажарилган операцияни сертификат билан тасдиқланиши банк ишчисини электрон имзоси кўринишида амалга оширилади.

Дебит операцияларни ҳимоялаш. Махсулот ёки хизматлар харид этилаётганида қуйидагилар бажарилади:

- савдо корхонасининг терминали томонидан смарт карта хақиқийлиги текширилади;
- карта томонидан савдо терминали хақиқийлиги текширилади;

- PIN код бўйича смарт карта эгаси аниқланади;
- смарт картада маблағ борлигини текшириш;
- тасдиқловчи электрон сертификатни яратиш;
- бажарилган операцияни сертификат билан тасдиқлаш;
- фирибгарликка уриниш пайтида смарт картани ўчириш (тиклаш имкони билан).

Хамма текширувлар кредитлаш операцияси каби бажарилади, фақат банк ишчиси сифатида кассир бўлади. Смарт картада маблағ борлигини текшириш хизматлар нархини смарт картадаги пул қолдиғи билан таққослаш йўли билан бажарилади. Смарт картада ўсиш билан сарфланган пуллар миқдори ёзилиб боради. У берилган кредит миқдори билан солиштирилади. Кредит миқдори фақат эмитент банк томонидан ўзгартирилиши мумкин.

Бажарилган операцияларни келишуви. Хар бир магазинда кун давомида амалга оширилган хамма кредит ва дебет операциялар тўпланади, келишув ва банкга юборилади. Бунда:

- Савдо терминал хақиқийлиги тасдиқланади;
- Келишув хақиқийлиги текширилади;
- Келишув хақидаги маълумотларни бутунлиги текширилади.

Текширувлар келишувлар сертификатларини криптографик функциялар библиотекалари ёрдамида бахолаш асосида амалга оширилиши керак.

Смарт картани хавфсизлигини таъминлаш. Смарт картани хавфсизлигини таъминлаш унинг хаётий циклининг хамма босқичида амалга оширилиши керак – кристаллни ишлаб чиқишдан, транспортировкасидан, персонализациялашдан карта эгасидан ундаги ахборотни ҳимоялашгача. Ишлаб чиқишда ва транспортировкада тўлов тизим ресурсларига рухсат олиш ёки уни ишлашини бузиш мақсадида картанинг характеристикалари ўзгартирилиши мумкин.

Ишлаб чиқаришда карточкани сифатини аниқлаш учун кристалл топологияси ва ОТ ичидагилари эталонга мослиги танлаб назорат қилиниши мумкин. Бунда фақат ўз давлатидаги смарт картани шлатилиши етарли даражада назорат ишончлилигини кафолатлаши мумкин.

Карта эгаси хақидаги конфиденциал ахборотни ташқарига чиқишига асосий хавф картани персонализациялаш босқичида мавжуд бўлади. Карталарни персонализациялаш ишчи жойи рухсат этилмаган киришдан ишончли ҳимоя тизимига эга бўлиши керак.

Карточкадаги конфиденциал ахборот эгасидан ва фирибгардан (ўғирланганда) ҳимояланиши кристалл ва ОТга РЭКдан физик-технологик ҳимоялаш усуллари, ва эгасини аутентификациялаш механизмидан фойдаланиш билан таъминланади.

Жихоз ва дастурий таъминотни ҳимоялаш. Тизимда ишлатиладиган жихоз ва дастурий таъминот ёмон ниятда ишлатилишини олдини олиш учун текширилиб туриши керак. Хамма терминаллар аппарат ва дастурий воситалар ёрдамида рухсат берилмаган киришдан ҳимояланган бўлиши керак. Терминаллар маълум калитлар юкланмагунча ишлаши мумкин эмас. Рухсат этилмаган киришларни ва рухсатсиз қурилмаларни ишлатишга уринишларни рўйхатга олиш журналини юритиш керак.

Ўқиш/ёзиш қурилмасини ҳимоялаш. Асосий хавфлар алоқа канали бўйича юборилаётган ахборотни ўғирлаш, ўзгартириш, иккинчи марта ишлатиш ва қурилмадан калит ахборотни ўқиб олишда бўлади. Симметрик криптографик усулл смарт карталар учун вазият битта қурилмадаги калитни компрометацияси хамма қурилмаларда калитларни алмаштиришга мажбур қилиши билан оғирлашади.

Қурилма хавфсизлигини таъминлаш алоқа каналини симметрик ва асимметрик криптография усуллари ёрдамида беркитишга асосланади.

Терминал жихозларини ҳимоялаш. Терминал жихозлари учун ўқиш қурилмаларига тегишли хавфлар мавжуд. Бундан ташқари, дастурий таъминот бутунлигини бузиш хавфи ва терминал – банкнинг ишчи станцияси каналида ахборотни ўғирлаш, ўзгартириш ва йўқ қилиш хавфлари бор.

ШК асосида амалга оширилган терминал жихозларини ҳимоялаш учун қуйидагилар таклиф қилинади:

- РЭКдан ҳимоялаш тизими;
- IP пакетларни мусаффо шифрлаш ва тармоқ орқали компьютерга рухсат этилишни чегаралаш коммуникацион дастурлари;
- Хар хил операцион тизимлар учун шифрлаш ва электрон рақамли имзо функциялар библиотекалардан фойдаланиш.

Шахсий компьютерлар, ишчи станциялар, процессинг марказ ва банклар серверлари ва алоқа каналлари. Бу жихозларга хавфлар ва уларга мос ҳимоялаш усулларини батафсил таснифи юқорида берилган. Ҳимоялаш воситаси сифатида қуйидагиларни ишлатиш мумкин:

- IP-пакетларни мусаффо шифрлаш ва компьютерга тармоқ орқали рухсатни чеклашнинг коммуникацион дастурлари;
- криптойўналтирувчилар (тармоқ сервер ва сегментларини ҳимоялаш учун);
- хар хил операцион тизимлар учун шифрлаш ва электрон рақамли имзолаш функциялар библиотекалари.

Фойдаланилган адабиётлар

1. И. Голдовский. Безопасность платежей в Интернете. – СПб: Питер, 2001. – 240 с.

2. Дж.Фостер. Зашита от взлома: сокеты, эксплойты shell-код: Пер.с англ. Слинкина А.А. -М.:Издательский Дом ДМК-Пресс, 2006. -784 с.

3. А. В. Соколов, В. Ф. Шаньгин. Зашита информации в распределенных корпоративных сетях и системах. ДМК Пресс, 2002. -656 с.

X. Остерлох. TCP/IP. Семейство протоколов передачи данных в сетях компьютеров. «ДиаСофтЮП», 2002. -576 с.