МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН
ИХ СУРГУУЛЬ
МЭДЭЭЛЭЛ ХОЛБОО ТЕХНОЛОГИЙН СУРГУУЛЬ

Баатарцогт ДАШЗЭВЭГ
(B140970433)

USB түлхүүр ашиглан үйлдлийн системийн нэвтрэх эрхийг баталгаажуулах нь

Мэргэжил: Системийн аюулгүй байдал

Систем хамгааллын төслийн ажил

Улаанбаатар хот 2017 он

МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ
МЭДЭЭЛЭЛ ХОЛБОО ТЕХНОЛОГИЙН СУРГУУЛЬ

Хамгаалалтанд орохыг зөвшөөрөв.
Холбооны салбарын эрхлэгч
Доктор (Ph.D), ... Я.Дашдорж

Удирдагч:
Компьютерийн ухааны магистр Г.Дашзэвэг
Гүйцэтгэсэн:
Компьютерийн систем хамгааллийн оюутан Б.Дашзэвэг

УШСК-ийн нарийн бичгийн дарга ...../Магистр Г.Дашзэвэг /

Улаанбаатар хот 2017 он

МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ
МЭДЭЭЛЭЛ ХОЛБОО ТЕХНОЛОГИЙН СУРГУУЛЬ

_____салбарын
_____мэргэжил
Овог нэр _____
Төслийн сэдэв _____
_____
_____
_____
_____ Тусгай бүлгийн
Сэдэв
_____
_____
_____
_____
_____
_____
_____
_____

Удирдагч _____

Төслийг эхэлсэн ___ он ___ сар ___ өдөр
Төслийн дуусгасан ___ он ___ сар ___ өдөр
Холбооны салбарын эрхлэгч
Доктор (Ph.D) ..... Я.Дашдорж

Гарчиг

Зургийн жагсаалт

0.1 Удиртгал

Хүн төрлөхтний нийгмийн хэрэгцээ өнөө үед улам бүр нэмэгдсээр байгаа билээ . Өдгөө компьютерийн салбар нийгмийг болон дэлхий ертөнцийг нэгэн бүхэл болгож байгаа юм. Тийм учраас хүн төрлөхтөн улам бүр илүү дэвшилтэд,илүү хялбар технилогийн төлөө тэмүүлсээр байгаа. Манай орны хувьд компютерийн салбар нь өдрөөс өдөрт улам бүр өргөжиж хүмүүс болон албан байгууллагууд техникийн гайхамшигийг илүү ихээр ашиглаж 21р зуунтай хөл нийлүүлэн алхаж байна. Харин хөгжихийн хирээр цахим орчин дахь аюул заналхийлэл ч мөн улам бүр ихсэж байгаа нь сөрөг тал юм .Хүмүүсийн хувийн мэдээлэл,байгууллагын албан тооцоо гэх мэт чухал зүйлс хувийн компьютерт хадгалагдаж байдаг билээ. Харин нууцлах шаардлагтай мэдээллийг илүү үр дүнтэйгээр давхар хяналттайгаар баталгаажуулснаар илүү эрсдэлгүй , хувийн мэдээллийг найдвартай хадглана гэсэн үг юм .Та өөрийн компьютерийн физик түлхүүрийг хүсч байсан уу? .Таны компьютерийг онгойлгох физик хэсэг байвал яг одоо хамгийн аюулгүй сонголт байх болно. Гэхдээ мэдээж энэ нь боломжгүй зүйл юм . Хэрвээ комьпютераас татгалзахыг хүсээгүй л бол та ямар нэгэн байдлаар мэдээллээ хамгаалах шаардлагатай тулгарна . Мэдээллийн аюулгүй байдлыг хангасан ирээдүй бидний хүсэл юм.

0.2 Зорилго

Хүн төрөлхтөн хувийн болон албан байгууллагынхаа алдах эрсдэл бүхий нууцлах шаардлагатай мэдээллийг өдгөө амьдралын салшгүй нэг хэсэг болоод буй комьпютерт ихээхэн хадгалах болсон . Комьпютер нь хэрэглэгч нэвтрэх үед нууц үг болон хэрэглэгчийн нэр зэрэгийг асууж хэрэглэгчийн үйлдлийн системд нэвтрэх эрхийг баталгаажуулдаг. Хэрвээ хэрэглэгч санаатай болон санамсаргүй байдлаар нууц үгээ алдах , хэрэглэгчийн нууц үгийг таах гэх мэтийн үйлдлүүд хийгдсэн бол таны компьютерт өөр хүн нэвтрэн таны хувийн мэдээллийг авах боломжтой болж байна . Мөн нууц үгээ урт төвөгтэй байдалаар өгснөөр нууц үгийг мартах зэрэг эрсдэлч учирч болзошгүй . Иймээс USB түлхүүрийг ашиглан үйлдлийн системд хандах эрхээ баталгаажуулж дээрх эрсдэлүүдээс зайлсхийх мөн үйлдлийн системд хялбар хандах боломжтой болгохыг зорилоо.Танд түр зуурын хугцаанд компьютерийг орхиж гарах асуудал байнга тулгарж байдаг бол USB түлхүүрийг ашигласнаар энэ үйлдэл нь илүү амархан болох юм . Бас та компьютертээ санаа зовохгүй байж болно USB түлхүүрээл өөртөө байлгах шаардлагатай .

0.3 Зорилт

Цаашидийн зорилт нь USB key-ийн ажиллагаа мөн USB key-ийн цааш-дын хөгжүүлэлт зэргийг судлах болно. Мөн хэрэгжүүлэлтийн хэсэг дээр үйллийн систем тухайн хугцааны дараа түгжигдэх , үйлдийн систем флаш салгасан үед түгжигдэх , түгжээгээ тайлах хэрэглэгчийн интер-фэйстэй болгох , олон хэрэглэгчийн мэдээллийг хадгалах, аплекэйшн-ийг USb key -ээр authentication хийхийг зорьж байна.

0.4 Онолын хэсэг

Энэ хэсэгт USB түлхүүрийн тухай болон түүнийг хэрхэн ашиглах , мөн USB түлхүүр үүсгэхэд ашиглагдах зүйлсийн талаар тайлбарлахыг зорилоо.

0.4.1 Үйлдлийн систем гэж юу вэ ??

Үйлдлийн систем гэдэг нь хэрэглэгч компьютер хоёрыг хооронд нь холбож, компьютерийн үйл ажиллагааг удирдаж, мэдээллийг зохион байгуулж байдаг суурь систем юм.
Үйлдлийн Системийн гүйцэтгэх үүргийг дурдвал:

- Диалог буюу хэрэглэгчтэй харьцах
- Оролт-гаралт, өгөгдлийг удирдах
- Програм боловсруулах процессын төлөвлөлт, зохион байгуулалт
- Санах ой, кэш, процессор, гадаад төхөөрөмжүүд г.м. компьютерын хэсгүүдтэй ажиллах
- Сонгосон програмыг ажиллуулах
- Боломжит бүх төрлийн үйлчилгээ (сервис)
- Дотоод төхөөрөмжүүдийн хооронд мэдээлэл дамжуулах
- Дэлгэц, гар, дискүүд, хэвлүүр г.м. залгах төхөөрөмжүүдийн ажиллагааг програмын түвшинд дэмжих зэрэг болно.

Үйлдлийн систем нь олон төрөл бөгөөд Үүнд : Линукс , Windows , Unix зэрэг томоохон үйлдлийн системүүдийг дурдаж болно . Мөн үйлдлийн системүүд нь командын хэл,командын процессор,драйверууд ,файлын систем зэрэг үндсэн бүрэлдхүүнтэй юм.

Windows үйлдлийн системд гэж юу вэ ?

Microsoft бол Microsoft-ын хөгжүүлж, худалдаалдаг үйлдлийн системийн цуврал юм.Анх 1985 он 11 дүгээр сарын 20-нд Microsoft MS-DOS-т зориулсан график шейлл (graphical operating system shell) болох Windows 1.0-г танилцуулжээ. Улмаар Windows нь персонал компьютерийн зах зээлийг эзлэх болж, дэлхий дээрх нийт компьютерийн 90 гаруй хувь нь Windows үйлдлийн систем дээр ажиллах болжээ.Microsoft компанийг анх 1975 онд Харвардын их сургуулийг төгссөн Билл Гэйтс өөрийн багын найз Пол Аллентай хамтран байгуулсан түүхтэй. Үүнээс хойш 38

жилийн турш хэдэн зуун удаа сайжруулан шинэчилсэн хувилбарыг гаргасаар ирсэн. Өдгөө windows 8 , windows 95 ,windows 7 ,windows XP зэрэг олон олон хувилбарыг бүтээсэн бөгөөд үйлдлийн систем хэрэглэгчдийн 80 гаруй хувь нь энэхүү үйлдлийн системийг хэрэглэдэг болоод байна. График интерфэйстэй ,хүнд ойлгомжтой маузыг(хулгана) түлхүү ашигладаг энэ үйлдлийн системийг сайжруулагч энэ компани томоохон зах зээлийн нийлүүлэгч болсон байна.Windows system нь хэргэлхэд хамгийн хялбар үйлдлийн систем юм.

Linux үйлдлийн систем гэж юу вэ?

Линукс буюу Linux бол Юникс-төст, POSIX стандартыг баримталдаг, чөлөөт, нээлттэй эхийн програм хангамж хөгжүүлэлт, түгээлтийн зарчимд тулгуурлан бий болсон үйлдлийн систем юм. Линуксийн голлох хэсэг бол Линукс цөм хэмээх үйлдлийн системийн цөм бөгөөд анхлан 1991 оны 10-р сарын 5-д Линус Торвалдс гаргасан байдаг. Линуксийн хөгжүүлэлт бол чөлөөт, нээлттэй эхийн програм хангамжийн хамтын ажиллагааны нэгэн том жишээ юм. Линуксийн цаад эх кодыг ГНУ Нийтийн Ерөнхий Зөвшөөрөл зэрэг зөвшөөрлийн дагуу хэн дуртай нь арилжааны болон арилжааны бус зорилгоор хэрэглэж, өөрчилж, тараах боломжтой.

Линуксийг хэрэглэхэд бэлэн болгон багцалсан хэлбэрийг Линукс тархац гэдэг.
Тэдгээрээс дурьдвал :

- Redhat
- CentOS
- Ubuntu
- Suse
- Debian
- Kali гэх мэт байдаг.

0.4.2 USB flash drive гэж юу вэ ?

USB флаш drive нь өгөгдөл хадгалах боломж бүхий зөөврийн төхөөрөмж юм. USB флашыг ашигласнаар мэдээллийг өөртөө хадгалах боломжтой мөн уг төхөөрөмжийг ашиглан мэдээллийн хурдан хугацаанд зөөвөрлөх боломжтой байдаг .USB флаш диск нь 2000 оноос хойш зах зээлд нэвтэрч байгаа бөгөөд тэдгээрийн хэрэглээ ихсэж байна.Тиймч учраас үйлдвэрлэгчид өгөгдлийг хадгалах чадавхитай илүү хурдан төхөөрөмж үйлдвэрлэсээр байгаа билээ.Мөн USB флашын хадгалах хэмжээ ихэссээр байгаа юм.

0.4.3 Authentication гэж юу вэ ?

Authentication гэдэг нь итгэмжлэгдсэн хэрэглэгчдийн мэдээллийг локал үйлдлийн систем дээр эсвэл нэвтрэлт танилтын серверийн дотор өгөгдөлд байгаа файлтай харьцуулсан үйл явц юм. Хэрэв итгэмжлэлүүд таарч байвал процесс дууссан бөгөөд хэрэглэгч хандалтыг зөвшөөрөх зөвшөөрөл олгох процесс юм. Authentication-ийг өдгөө олон систем дээр хэрэглэх болсон бөгөөд хэрэглэгчийн нэр нууц үг , мөн хурууны хээ , нүүр царай зэргээр нь шалгалт хийгддэг болсон. Мэдээж хэрэглэгч зөвшөөрөл түрүүлж авсан байх шаардлагатай.

0.5 USb key authentication

Үйлдлийн системд хүмүүс ихэвчлэн Username , Password гэсэн үндсэн 2 баталгааажуулалтыг хийж нэвтэрдэг. Харин өдгөө хурууны хээ , нүдний бүрхүүл гэсэн хүний давтагдашгүй шинжээр адилтган танилт хийж нэвтэрдэг болсон билээ . Ихэнх компьютер нь хэрэглэгчид суурьлсан нууц үгийг ашигладаг . Гэсэн хэдийч нууц үгийн хамгаалалтыг аюултай гэж үздэг. Хэдийгээр та хүчтэй нууц үгийг олон төрлөөр үүсгэж, аюулгүй байдлын сайн баталгааажуулалт хийдэг байсан ч гэсэн нэг дутагдалтай тал үлдсэн түүнийг ямар нэгэн байдлаар таах боломж бий.Хэрвээ таах боломжгүйгээр нууц үгийг хийх юм бол танд нууц үгээ санахад төвөг учирч болно. Ийм учраас илүү аюулгүйгээр USB key ашиглан адилтган танилт хийж болно. Authentication-ийг ашиглан нэвтрэлт хийж байгаа үед таны нууцлах шаардлага бүхий мэдээлэл найдвартай хамгаалагдах ёстой . Та USb түлхүүрийг ашигласнаар давхар шалгалт хийх боломжтой болж байгаа юм . Нууц үг болон USB Flash Drive. USB кеу -ийг алдах , гэмтээх эрсдэл байж болох ч алдсан usb-ний нууц үгийг оруулах боломжтой . Харин системийн администрууд олон жилийн турш байгууллагын төхөөрөмжинд USB флаш зэргийг залгахгүй байхыг уриалсаар байгаа билээ. Энэ нь ч шаардлага бүхий зүйл бөгөөд байгууллагийн нууц мэдээллийг хадгалах дотоодын халдлагаас зайлсхых аргуудын нэг мөн. Хөдөлгөөнт технологи, гар утас гэх мэт мобайл технологийг өргөнөөр ашигласнаар компаниуд "өөрийн төхөөрөмжийг бий болгох"буюу (BYOD) загвартай тулгараад байгаа бөгөөд үүнд гар утасны төхөөрөмжийг ажлын байр руу авчирч USB-ээр дамжуулан тэднийг холбох боломжтой болгосон . Энэ нь зарим төрлийн компаниуд USB холболтгүйгээр компьютерийн системийг суулгахаар сонгосон шалтгаануудын нэг бөгөөд BYOD төрлийн холболтоос сэргийлэхийн тулд юм.Гэсэн хэдий ч сүүлийн үеийн хөгжил нь вэбсайт, програм хангамж, систем, сүлжээнд зориулсан аж ахуйн нэгжийн хэрэглэгчийн бүртгэлд хандах хандалтыг хамгаалдаг баталгаат аюулгүй байдлыг хангахын тулд зарим компаниуд USB холболтруу шилжих замыг сонгож буй билээ . Жишээгээр нь Google компанийн хувьд Universal 2nd Factor (U2F) стандаартыг

ашиглан USB нэвтрэлтийг дэмждэг.U2F стандарт нь баталгаажсан данс эсвэл үйлчилгээнд хандах эрхийг баталгаажуулахын тулд нэвтрэлтийн аюулгүй байдлын хоёр хүчин зүйлийр баталгаажуулахын тулд мэдлэгийн хүчин зүйл (нууц үг), физик хүчин зүйл (USB түлхүүр) хоёуланг нь шаарддаг. Нэвтрэх сайт эсвэл үйлчилгээ нь үнэхээр хууль ёсны өмч гэдгийг баталгаажуулсны дараа л нэвтрэх эрхийг олгодог. Тэгвэл USB холболтыг ашигласнаар та болон танай байгууллага ямар ашигтай вэ гэдгийг тайлбарлъя.

Үйлдлийн системд нэвтрэхэд USB флаш дискийг яагаад ашиглах ёстой вэ ??

- Та компьютерийн нууц үгээ санаж, бичиж оруулах шаардлагагүй (гэхдээ таны систем нууц үгээр хамгаалагдсан хэвээр байна).
- Та "аюулгүй байдлыг сайжруулах"зарчмуудад нийцсэн урт аюулгүй нууц үгийг ашиглаж болно.Хэдэнч тэмдэгтээс тогтож болно санах боломжтой таний ойрийн хэрэглэдэг зүйл байх шаардлаггүй .
- Үйлдлийн системрүү хурдан нэвтрэх боломжтой. Хэрэглэгчид USB флашийг USB порт руу оруулах үед автоматаар нэвтэрч болно.
- Хэрэглэгч компьютерээс USB disk-ийг салгах үед автоматаар түгжигдэнэ.
- PIN код + USB түлхүүр бүхий хоёр хүчин зүйлийг таньж баталгаажуулах .
- Нэг USB дискийг нь олон компьютерийг түгжих / нээх боломжтой байдаг.
- Олон USB дискийг -ийг та нэг компьютерийн олон хэрэглэгчид оноож өгж болдог.
- Өдрийн тодорхой цагт компьютерийн нэвтрэх боломжийг хязгаарлаж болох хуваарь бий болгох .
- Алдагдсан, эвдэрсэн USB түлхүүрийн хувьд, хэрэглэгчийн нууц үгийг оруулж болно.

USB key-ийн сул тал нь юу вэ ?
2014 оны 7 сард мэдээлсэнээр аюулгүй байдлын профессор Карстен Нохл, Жокоб Лел нарын аюулгүй байдлын хяналт хийсний дагуу USB төхөөрөмжүүд нь HARD disk-нд хадаглагдсан мэдээллийг хуулахаар дахин програмчлагдсан байсан байна. Энэ нь USB залгахад эрсдэл хүлээх гол

хүчин зүйл мөн .
Бас Goossens-ийн мэдээлэлснээр USB түлхүүр нь дараах сул талтай гэж үзжээ . Үүнд :

- USB баталгаажуулах технологиуд нь мэдээллийн аюулгүй байдлын хувьд аюултай, бүрэн хуучирч болох баталгаажуулалтын үйл явцын нэг хэсэг болсон нууц үгс дээр тулгуурладаг. Хэрэв та нэвтрэх процессод шаардагдах ID, нууц үгийн хослолыг шаарддаг технологи ашигладаг, шаардлагатай USB төхөөрөмжийг хоёр дахь таних фактор болгон ашиглаж байгаа бол таныг нэвтрэх серверт халдлага хийх боломжтой юм . Довтлогч нарын хувьд таны анхны баталгаажуулалтын хүчин зүйл хэвээр байгаа юм.

- USB баталгаажуулалтын та хангсан боловч кибер гэмт хэрэгтнүүд нь фишинг, вирусын эсрэг програм зэргээр дайралт хийхэд нэвтрэх, эсвэл дамжин өнгөрөх үеэр эмзэг нууцлалын нэвтрэх эрхийг хулгайлж чадна.

0.6 USB key-ээр үйлдлийн системд яаж нэвтэрдэг вэ ??

Хэрэглэгч USB флаш-аа компьютер руу залгаснаар нууц үгийг флаш дээр тохируулсан нууц үгтэй адилтган танилт хийж ижил байвал LOCK тайлагдах болно .(Хэрвээ флаш залгахад ПИН кодыг тохируулсан бол асуух болно). Хэрэв хүчингүй пин 3-аас олон удаа оруулбал USB дискийг хаах боломжтой тул USB-ийн нэвтрэх түлхүүр цаашид боломжгүй болно . Хэрэглэгчид түр хугацаагаар компьютерээ орхих болгонд тэд зүгээр л USB флаш дискээ салгах замаар компьютерээ түгжих боломжтой. Мөн USB Key-ийг салгасны дараа дэлгэцийг унтраах эсвэл идэвхжүүлэх боломжтой болно. Бүр mouse болон keyboard-ийг ч түгжих боломжтой юм.

USB key -ийг үүсгэхээс өмнө таны мэдэж байх ёстой дараах зүйлс бий

- Таны port -д USB флаш байнга хийгдэнэ.
- USB түлхүүрээ алдах.
- Таны USB дээр байгаа түлхүүрийн мэдээллийг хэн нэгэн хуулж авах эрсдэлтэй.

Дээр дурьдсан зүйлс нь эрсдэл мөн боловч шийдэх арга зам байдаг.

Хэрвээ таны компьютер USB портын нөөцгүй бол та USB порт-ийг олшруулах төхөөрөмж ашиглаж болно . Жишээ нь Multiport гэх мэтийн салаалсан USB хөрвүүлэгчид байдаг.
Та USB түлхүүрээ хэн нэгэнд санаатайгаар алдаж болох юм. Энэ нь танд эдийн засгийн хувьд хохиролтой боловч таны компьютер дээр үнхээр нууцлах шаардлага бүхий мэдээлэл байдаг бол та нууц үгээ алдсан гэдгээ мэдэж болох юм(Хэрвээ USB key-гүй бол та нууц үгээ алдсан гэдгээ мэдэх боломжгүй). Харин USB флашаа алдсанаа мэдмэгцээ нууц үгээ солих эсвэл компьютераа орхиж явахгүй байх шаардлагатай.
Таны флаш дээрх мэдээллийг хуулах нь хамгийн том эрсдэл юм. Танд мэдэгдэхгүйгээр хуулсан тохиолдолд таны системд нэвтрэх боломжтой болж байгаа юм. Үүнээс сэргийлэхийн тулд флаш дискээ хүнд хэрэглүүлэхээс татгалзах мөн нууц үгээ тогтмол сольж байх шаардлагатай. Нууц үгийг та байнга санж байх шаардлагагүй учир нууц үгийг тогтмол солих нь танд төдийлөн төвөгтэй биш юм.Мөн флаш диск дахь Файлын агуулга нь шифрлэгдсэн байна.

Таны хийж болох ажилууд :

- Нууц үг тохируулах
- Override lock хийх сүлжээний команд байж болно.
- USB дискийн серийн дугаарыг шалгах
- Систем бүрийн өвөрмөц түлхүүр

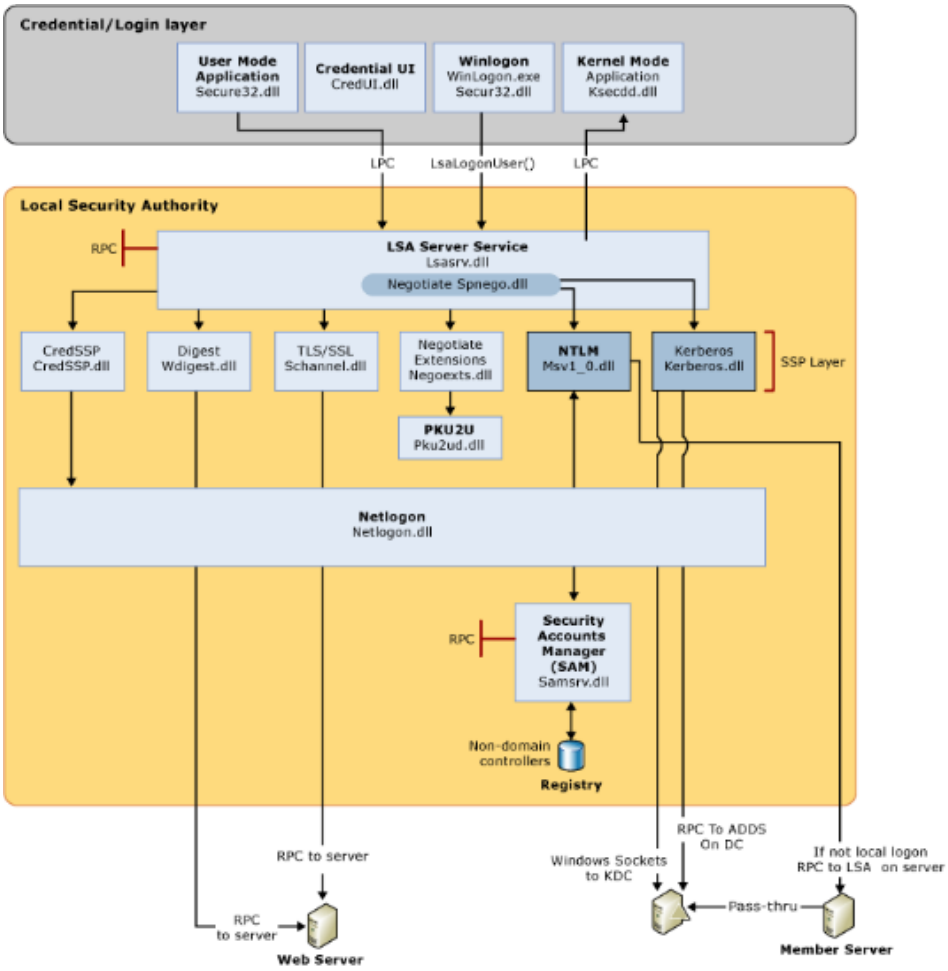
гэх мэт ажилыг та гүйцэтгэж болно.

USB түлхүүр нь үнэтэй болон үнэгүй хувилбар нь дараах ялгаатай болно .

Хийгдэх ажилууд	үнэтэй	үнэгүй
USB түлхүүрээр үйлдлийн системрүү автоматаар нэвтэрч орно	чадна	чадна
Санах шаардлагагүйгээр урт, хүчирхэг нууц үг ашигладаг	чадна	чадна
Нууц үгт суурилсан нэвтрэлтийн сул талыг USB түлхүүрээр солих	чадна	чадна
2 хүчин зүйлийн нэвтрэх нууц үг: Таны USB товчлуур + Пин код	чадна	чадахгүй
USB Түлхүүр дээр тулгуурлан компьютерт хандах хандалтыг хязгаарлах	чадна	чадахгүй
Онцгой байдлын бүртгэл нь алдагдсан USB флашаа хаясан Pin кодоо мартсан бол системд нэвтрэх боломжийг олгодог	чадна	чадахгүй
Түлхүүр баталгаажуулах USB флаш	чадна	чадна
Нэг удаагын нууц үг , Смарт карт зэрэг	чадна	чадахгүй

0.7 Windows credential гэж юу вэ?

Windows credential гэдэг нь үйлдлийн систем хэрэглэгчийн итгэмжлэлийг хүлээн авч баталгаажуулалт хийхийн тулд мэдээллийг хадгалах процесс юм. Компьютер нь аль нэг домайнд холбогдсон тохиолдолд баталгаажуулах үйлдэл нь мөн домайн дээр явагддаг. Баталгаажуулхад ашигласан итгэмжлэлүүд нь хэрэглэгчийг таних хэлбэрийн нууц үг , нэр , сертипкат гэсэн дижитал бичиг баримт байдаг. Default-аар Windows итгэмжлэл нь Security Accounts Manager (SAM) өгөгдлийн сан эсвэл WinLogon үйлчилгээгээр дамжуулан компьютерт холбогдсон домайн дээр Active Directory-ийн эсрэг хамгаалагдсан байдаг. Credential нь хэрэглэгчийн User interface дээр логин хийсэн оролтыг API гаар бүртгэж аван шифрлэсэн байдаг. Local аюулгүй байдлын мэдээлэл нь HKEY LOCAL MACHINE/SECURITY дээр бүртгэгдэн хадгалагдана. Мэдээлэл хадгалалтад нь аюулгүй байдалын default утгууд , кэшийн нэвтрэх эрхийн тухай гэх мэт мэдээллүүд багтсан байдаг. Security Account Manager -ийн хуулбар мэдээлэл нь мөн энд хадгалагдана.



Зураг 1: Итгэмжлэлийн баталгаажуулалтын зураг

Дараахь диаграмм-д бүрэлдэхүүн хэсгүүдийг харуулж, амжилттай нэвтрэн орохын тулд хэрэглэгчийг баталгаажуулах итгэмжлэлийг харуулж байна .

Тухайн зурагт харуулсан бүрэлдхийн хэсгүүдийг харуулвал .

- User Logon -Winlogon.exe нь хэрэглэгчийн харилцан үйлдлийг удирдах үүрэгтэй файл юм. Winlogon үйлчилгээ хэрэглэгчийн (Logon UI)итгэмжлэлүүдийг Windows Secure32.dll-ээр дамжуулан Local Security Authority (LSA) руу шилжүүлэх замаар Windows үйлдлийн системийг бүртгэх үйл явцыг эхлүүлдэг.
- Application logon - Application буюу service нэвтрэлтүүд нь интерактив бүртгэлийн шаардлагагүй. Хэрэглэгч эхлүүлсэн ихэнх процессууд нь user mode-д ажилладаг бөгөөд Secur32.dll-ийг ашиглан процессыг эхлүүлэхэд процессууд нь Ksecdd.sys-ийг ашиглан цөмийн горимд ажилладаг.
- Secur32.dll-Баталгаажуулах үйл явцын суурийг бүрдүүлдэг олон танилт шалгалтын үйлчилгээ үзүүлэгч юм.
- Lsasrv.dll- LSA серверийн үйлчилгээ нь аюулгүй байдлын бодлогыг шаарддаг бөгөөд LSA-ийн аюулгүй байдлын багцийн дагуу ажилладаг. LSA нь ямар протокол амжилттай болохыг тодорхойлох NTLM эсвэл Kerberos протоколыг сонгосноор тохиролцох функцийг агуулдаг.
- Security Support Providers-Нэг буюу хэд хэдэн танилтын протоколыг дангаар нь нэг удаа үүсгэж болох үйлчилгээ үзүүлэгчдийн багц. default тохируулгууд нь Windows-ийн хувилбар бүрээр өөрчлөгдсөн байдаг, мөн тохируулан бичиж боломжтой .
- Samsrv.dll - Security Accounts Manager (SAM) нь Local Account-ийн мэдээллийг хадгалдаг. APIs -ийг дэмждэг үйлчилгээ юм.

0.8 USB түлхүүр ашиглан апплекэйшнд нэвтрэх нь

USB түлхүүрийг ашигласнаар та апплекэйшнд нэвтрэх боломжтой юм. Жишээ дурдвал Facebook, Google's Gmail, Google Cloud and G Suite, GitHub, Dropbox зэрэг томоохон апплекэйшнүүд орж байгаа юм. Энэ нь FIDO U2F-г дэмждэг . Таны бүртгэлтэй account-ууд Пишинг болон Brute Force зэрэг халдлагуудаас сэргийлэх боломжтой юм.

0.9 Аюулгүй нэвтрэлтийн төрлүүд

Хэрвээ аюулгүйгээр баталгаажуулалтыг хийж үйлдийн системдээ нэвтэрийг хүсвэл дээрх аргуудыг ашиглаж болно.

0.9.1 USB key-ийн төрлүүд

- KeyLock - KeyLock бол USB Flash Drive ашиглан компьютерээ түгжих програм юм. Гол ялгаатай нь түгжээг дэлгэцэн дээрээ бүрэн тохируулах боломжийг олгоно .
- USB Raptor - Энэ нь USB flash drive ашиглан компьютерээ түгжээд онгойлгох бас нэг хэлбэр юм. Онцлог нь USB компьютераас салснаас хэсэг хугцааны дараа онгойлгох боломжтой.
- Predator - Predator-ийн давуу тал нь таныг хол байсанч түгжигдэх боломжтой юм.
- Rohos logon key- Ямар ч USB флаш эсвэл Bluetooth ухаалаг төхөөрөмжийг таны компьютерийн аюулгүй байдлын токен руу хөрвүүлдэг . Хоёр хүчин зүйл таних шийдэл бөгөөд Windows-д хандалт хийх боломжийг олгодог .

0.9.2 Сертипкат ашиглан Windows адилтган танилтыг хийх нь

Нийтийн түлхүүр (PKI) нь харилцаа холбоо, бизнесийн ажил үйлчилгээг баталгаажуулах боломжийг олгодог шифрлэлтийн технологийн үйлчилгээ юм. Ажил үйлчилгээг баталгаажуулахын тулд PKI-ийн баталгаажуулсан хэрэглэгчид болон итгэмжлэгдсэн нөөцүүдийн хоорондох certifcate-ийг солилцох замаар итгэлцлийг тогтоодог.
Тоон сертификат гэдэг нь харъяалагдсан этгээдийн тухай мэдээллийг агуулсан цахим баримт бичиг юм. Үүнд олгосон байгууллага , серийн дугаар эсвэл өөр өвөрмөц тодорхойлолт , олгосон хугацаа ба дуусах хугацаа , мөн хурууны хээ гэх мэт мэдээллүүд багтаж болно .

Баталгаажуулалтын хувьд certification authority(CA) -аас гэрчилгээ авах замаар алсын зайнаас найдвартай байдлыг бий болгодог. CA нь ахлах дээд байгууллагаас гэрчилгээтэй авсан байж болох бөгөөд гэхдээ итгэлцлийн сүлжээ бий болох юм . Гэрчилгээ нь найдвартай эсэхийг тодорхойлохын тулд CA-ын жинхэнэ нэрийг тодорхойлж, найдвартай эсэхийг тодорхойлох ёстой.

Тийм учраас Windows дээр үүсгэсэн certificat-ыг алдсын сервер эсвэс SAM дээр хадгласан байх ба нэвтрэлт хийх үед хувийн мэдээллийг ашиглан үүсгэсэн certificat-аар тулглат хийх нэвтрэх эрхийг баталгаажуулалтыг хийдэг энэ нь үйлдийн системд илүү амар найдвартай нэвтрэх аргуудын нэг юм.

0.9.3 Smart картны баталгаажуулалт

Смарт картын технологи нь гэрчилгээнд үндэслэсэн баталгаажуулалтын жишээ юм. Ухаалаг карттай нь сүлжээнд нэвтэрч хэрэглэгчийг домэйнд таниулахдаа криптограф дээр тулгуурласан таних болон эзэмшлийн баталгааг тулгадаг учир танин баталгаажуулах хүчтэй хэлбэрийн нэг юм. Active Directory Certificate Services нь ухаалаг карт бүрийн бүртгэлийн гэрчилгээ олгох замаар криптограф дээр тулгуурласан таних боломжийг олгодог.

0.9.4 Алсын болон wireless authentication

Алсын болон утасгүй сүлжээний нэвтрэлт танилт нь баталгаажуулах гэрчилгээг ашигладаг өөр нэг технологи юм.Microsoft Internet Authentication Service (IAS) болон виртуал хувийн сүлжээний сервер нь Extensible Authentication Protocol-Transport Level Security (EAP-TLS),(VPN) болон утасгүй холболтууд зэрэг сүлжээний хандалтын төрлүүдтэй байдаг. Энэ нь wireless-аар дамжуулан сертипкатаа үүсгэж адилтган танилт хийх технилөги юм. Таны төхөөрөмжийн Mac хаягаар сертипкат үүсгэж сүлжээнд холбогдох үед нь баталгаажуул боломжтой.

0.9.5 Бусад

Хэрэглэгчийн өөрийн таних тэмдэгээр баталгаажуулалт үүсгэх боломжтой . Энд хурууны хээ , нүүрний төрх , нүдний бүрхээл зэрэг хэсгүүд байж болно . Хэрвээ энэ шинж тэмдгүүдээр баталгаажуулсан бол хамгын найдвартай юм . Мөн даралт мэдрэн баталгаажуулалт хийдэг төхөөрөмжүүд бас бий. Давхар шалгалт хийх мөн бүрэн боломж бий.