

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:
Компютерийн ухааны магистр Г.Дашзэвэг
Гүйцэтгэсэн:
Компютерийн 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

| | |
|--|-----------|
| 1 Оршил | 7 |
| 1.1 Удиртгал | 7 |
| 1.2 Зорилго | 8 |
| 1.3 Зорилт | 8 |
| 2 Онолын хэсэг | 9 |
| 2.0.1 Authentication гэж юу вэ ? | 9 |
| 2.0.2 Үйлдлийн систем гэж юу вэ ?? | 12 |
| 2.0.3 USB flash drive гэж юу вэ ? | 13 |
| 2.1 USB key authentication | 14 |
| 2.2 USB key-ээр үйлдлийн системд нэвтрэх заавар?? | 15 |
| 2.3 Аюулгүй нэвтрэлтийн төрлүүд | 16 |
| 2.3.1 USB key-ийн төрлүүд | 17 |
| 2.3.2 Сертикат ашиглан Windows адилтган танилтыг хийх нь | 17 |
| 2.3.3 Smart картны баталгаажуулалт | 18 |
| 2.3.4 Алсын болон wireless authentication | 18 |
| 2.3.5 Бусад | 18 |
| 3 Судалгааны хэсэг | 19 |
| 3.1 Windows-г түгжих болон нээх | 19 |
| 3.1.1 LockWorkStation функц | 20 |
| 3.2 USB түлхүүр ашиглан үйлдлийн системд нэвтрэх нь | 20 |
| 3.2.1 USB түлхүүрийн давуу болон сул талууд | 22 |
| 3.2.2 Эрсдэлээс сэргийлэх нь | 23 |
| 3.2.3 USB түлхүүртэй холбоотойгоор хийгдсэн ажилууд | 23 |
| 3.2.4 USB түлхүүрийн цаашдын хөгжүүлэлт | 24 |
| 3.3 Windows credential гэж юу вэ? | 24 |
| 3.3.1 Adding a Credential - Итгэмжлэлийг нэмэх | 26 |
| 3.3.2 Windows crediantial management | 26 |
| 3.3.3 Credential Guard | 29 |
| 3.4 Windows Registry гэж юу вэ ? | 29 |
| 3.4.1 Usb түлхүүрийг register-т бүртгүүлэх | 31 |

| | | |
|-----|--|----|
| 3.5 | USB түлхүүр ашиглан апплекэйшнд нэвтрэх нь | 32 |
|-----|--|----|

Зургийн жагсаалт

| | | |
|-----|--|----|
| 3.1 | Windows итгэмжлэлийг нэмсэн процесс | 27 |
| 3.2 | Итгэмжлэлийн баталгаажуулалтын зураг | 28 |
| 3.3 | Registry-д хандсан байдал | 30 |

Бүлэг 1

Оршил

1.1 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 технологийн төлөө тэмүүлсээр байгаа. Манай орны хувьд компьютерийн 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 шаардлагатай мэдээллийг илүү үр дүнтэйгээр давхар хяналттайгаар баталгаажуулснаар илүү эрсдэлгүй , хувийн мэдээллийг найдвартай хадглана гэсэн үг юм .Мөн нууц үгээ урт төвөгтэй байдалаар өгснөөр нууц үгийг мартах зэрэг эрсдэлч учирч болзошгүй . 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 . 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.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 . Мэдээллийн аюулгүй байдлыг хангасан ирээдүй

бидний хүсэл юм.

1.2 Зорилго

USB түлхүүрийг ашиглан үйлдлийн системд хандах эрхээ баталгаажуулж эрсдэлүүдээс зайлсхийх мөн үйлдлийн системд хялбар хандах боломжтой болгохыг зорилоо.

1.3 Зорилт

Цаашидийн зорилт нь USB :

- 11 сарын 15 - USB-гүйгээр компьютерийн дэлгэцийг түгжих болон нээх .
- 11 сарын 20 - USB кее-ийг ашиглах компьютерт нэвтрэх эрхийг баталгаажуулах
- 11 сарын 30 - График интерфэйстэй болгох
- 12 сарын 1 бусад тохиргоог хийх /үүнд : олон хэрэглэгчийн хандалт гэх мэт/

Бүлэг 2

Онолын хэсэг

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

2.0.1 Authentication гэж юу вэ ?

Authentication гэдэг нь итгэмжлэгдсэн хэрэглэгчдийн мэдээллийг локал үйлдлийн систем дээр эсвэл нэвтрэлт танилтын серверийн дотор өгөгдөлд байгаа файльтай харьцуулсан үйл явц юм. Өөрөөр хэлвэл баталгаажуулалт нь байгууллагаас буюу хувь хүнээс мэдэгдэж байгаа өгөгдөлийн үнэнийг баталгаажуулах үйлдэл 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. Өөрөөр хэлбэл нэвтрэгчийг , болон өгөгдлийн мөн исэхийг шинж чанараар нь тодорхойлох үйл явц гэж ойлгож болно. Жишээлбэл : Биднийг иргэний үнэмлэх , Оюутны үнэмлэх мөн бусад баримт бичгээр мөн исэхийг тодорхойлдог. Үүнтэй адилаар бидний иргэн тойронд баталгаажуулах үйл явц өдөр бүр өрнөсөөр байдаг.

Нэвтрэлт танилтын үйл процессыг ерөнхийд нь явагдаж буй зарчмаас хамааран дараах шинж чанараар ангилж үздэг үүнд дээрх 3н шинж чанар орж болно :

- Тухайн биеийн жинхэнэ эсэхийг ямар нэгэн найдвартай эх сурвалж болон этгээдийн өгсөн баталгаажуулах нотлох баримтыг хүлээн авч үүний дагуу баталгаажуулан анхны удаа баталгаажуулах болно. Урлаг, физик гэх мэт салбарын хувьд объектын нотолгоо шаардагдах үед энэ баталгаа нь түүний бүтээлийн нотолгоог гэр-

чилж буй найз, гэр бүлийн гишүүн эсвэл хамт ажилж буй ажилтан байж болно, магадгүй бүтээгчийн эзэмшлийн эд зүйлсийг гэрчилсэн байж магадгүй. Эрх мэдэл бүхий төвлөрсөн итгэлцлийн харилцаа холбоо нь олон нийтийн сертификатын хамгийн найдвартай хүсэг юм.

- Объектын гарал үүслийн жинхэнэ эсэхийг баталгаажуулахын тухайд өмнө нь мэдэгдэж байсан баталгаатай зүйлүүдтэй нь объектын шинж чанарыг харьцуулах явдал юм. жишээ нь : Хэрвээ археологич нь олдворын насыг баталгаажуулахын тулд карбоны болзоо ашиглах, ашигласан материалын хими, спектроскопийн шинжилгээг хийдэг, эсвэл ижил төстэй гарал үүсэлтэй бусад барилга байгууламж, чимэглэлийг харьцуулах боломжтой. Энэ нь таны бүтээгдхүүн өмхөн баталгаажсан бүтээгдхүүнтэй ижил шинж чанар олонтой байвал таны бүтээгдхүүн ч бас баталгаажих боломжтой гэсэн үг юм.
- Энэ нь баримт бичиг болон бусад гадаад баталгаан дээр тулгуурладаг.Энэ нь нотлох баримт бичгийн бүртгэлээр дамжуулан , эсвэл түүнийг шийдэх цагдаагын мөрдөн байцаагч болон хууль зүйн ажилтнууд гэрчлэл хийж болно. Зарим эртний эрсдэл зэргийг баталгаажуулсан гэрчилгээ дагалдана. Спортын зэрэг цол хэргэм заасан байвал ихэвчлэн гэрчилгээ дагалдсан байдаг.Мөн эрүүгийн шүүхэд нотлох баримтын дүрмүүд нь нотлох баримтыг хадгалах сүлжээг бий болгохыг шаарддаг. Үүнийг бичмэл нотлох баримтаар, эсхүл түүнийг хариуцсан цагдаагийн ажилтнууд болон шүүх ажилтнуудаас мэдүүлгээр гүйцэтгэж болно.

Баталгаажуулах арга зам нь нэвтрэлт танилтын хүчин зүйлс гэж юу болох, хэрэглэгчийн ямар нэг зүйл, хэрэглэгчийн ямар нэг зүйл байгааг мэдэх гэсэн гурван төрөлд хуваадаг гэж үздэг боловч баталгаажуулах хүчин зүйл бүр нь хандалт хийх хүсэлтийг баталгаажуулах, баталгаажуулах, баримт бичиг, ажлын бусад баримт бичгийг гарын үсэг зурах, бусдад эрх мэдэл олгох, эрх мэдлийн гинжийг үүсгэхийн тулд тухайн этгээдийн хэн болохыг тодорхойлоход ашиглагддаг төрөл бүрийн элементүүдийг хамарна.

Аюулгүй байдлын судалгаанаас харахад эерэг нотолгоо, хоёроос доошгүй элементүүд, мөн эдгээр гурван хүчин зүйлүүдийг шалгаж үзэх шаардлагатай болохыг тогтоосон. Үүнд :

- Мэдлэгийн хүчин зүйлс: Хэрэглэгч ямар нэг зүйл мэдэж байх (Жишээ нь, нууц үг, хэсэгчилсэн нууц үг, өгүүлбэрийн дамжуулалт эс-

вэл хувийн дугаар (PIN), асуултуудад хариулах (хэрэглэгч асуулт эсвэл загвар хариулах ёстой)

- Өмчлөлийн хүчин зүйл: Хэрэглэгч ямар нэг зүйлтэй байх (ж.нь: бугуйн карт, үнэмлэх, гар утасны техник хангамж токен бүхий гар утас, програм хангамжийн токен, эсвэл програм хангамжийн токен)
- Уугуулын хүчин зүйлс: Хэрэглэгчийн аль нэг зүйл (жишээ нь: хурууны хээ, нурууны загвар, ДНХ-ийн дараалал (гарын авлагууд, гарын үсэг, нүүр, дуу, өвөрмөц био-цахилгаан дохио гэх мэт).

1 хүчин зүйлт баталгаажуулалт :

Баталгаажуулалтын хамгийн сул түвшин бол дээрх гурван хүчин зүйлээс зөвхөн нэг бүрэлдэхүүн хэсэгийг ашиглаж баталгаажуулалт хийх арга юм. Үүнийг нэг хүчин зүйлт баталгаажуулалт гэдэг. Зөвхөн нэг хүчин зүйлийг ашиглах нь буруу юм. Хорлон сүйтгэх болон халдлагаас бүрэн хэмжээнд хамгаалж чаддаггүй. Энэ төрлийн нотолгоог аюулгүй байдлын дээд түвшинг баталгаажуулах санхүүгийн буюу бие даасан үйл ажиллагааны хувьд зөвлөдөггүй.

2 хүчин зүйлт баталгаажуулалт :

Баталгаажуулалт хийхэд хоёр хүчин зүйлийг төлөөлөх элемент шаардлагатай үед хоёр хүчин зүйлийн баталгаажуулалтыг хэрэглэнэ өөрөөр хэлбэл: банкны карт (хэрэглэгчийн ямар нэг зүйл) болон ПИН (хэрэглэгч мэддэг зүйл). Бизнесийн сүлжээ нь хэрэглэгчдэд нууц үг (мэдлэгийн хүчин зүйл) болон аюулгүй байдлын жетон (пропорционал) дугаарыг эзэмшихийг шаарддаг. Өндөр аюулгүй байдлын системд хандах нь өндөр, жин, нүүрний болон хурууны хээг шалгах (хэд хэдэн өвөрмөц байдлын элементүүд) дээр нэмэх нь PIN болон өдрийн код (мэдлэгийн хүчин зүйл элементүүд) хүчин зүйл танин баталгаажуулдаг.

Олон хүчин зүйлийн баталгаажилт :

2FA-д хэрэглэгддэг хоёр хүчин зүйлийг ашиглахын оронд олон удаагийн нэвтрэлт танилтын хүчин зүйлсийг ашигладаг энэ нь 2FA баталгаажуулалтын үйл явцтай харьцуулахад гүйлгээний аюулгүй байдлыг сайжруулахад ашиглагддаг.

Strong authentication :

АНУ-ын Засгийн газрын Үндэсний мэдээллийн баталгаажуулалтын нэр томъёоны тайлбар нь Strong authentication -г тодорхойлдог. Өгөгдөл

гаргагч буюу хүлээн авагчийн хэн болохыг тодорхойлохын тулд хоёр буюу түүнээс дээш таниулагчдад тулгуурласан нэвтрэлт танилтын арга.

2.0.2 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 Гейтс 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.

2.0.3 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.

2.1 USB key authentication

Үйлдлийн системд хүмүүс ихэвчлэн Username , Password гэсэн үндсэн 2 баталгаажуулалтыг хийж нэвтрэдэг. Харин өдгөө хурууны хээ , нүдний бүрхүүл гэсэн хүний давтагдашгүй шинжээр адилтган танилт хийж нэвтрэдэг 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 баталгаажуулалт 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 key -ийг алдах , гэмтээх эрсдэл байж болох ч алдсан usb-ний нууц үгийг оруулах боломжтой . Харин системийн админууд 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 зайлсхийх 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) стандартыг ашиглан USB нэвтрэлтийг дэмждэг.U2F стандарт нь баталгаажсан данс эсвэл үйлчилгээнд хандах эрхийг баталгаажуулахын тулд нэвтрэлтийн аюулгүй байдлын хоёр хүчин зүйлийг 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.

2.2 USB key-ээр үйлдлийн системд нэвтрэх заавар??

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 |

2.3 Аюулгүй нэвтрэлтийн төрлүүд

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

2.3.1 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 хугацааны 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 .

2.3.2 Сертификат 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 certificate-ийг солилцох замаар итгэлцлийг тогтоодог.

Тоон сертификат гэдэг нь харьяалагдсан 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 эсвэл SAM дээр хадгласан байх ба нэвтрэлт хийх үед хувийн мэдээллийг ашиглан үүсгэсэн certificat-аар тулгат хийх нэвтрэх эрхийг баталгаажуулалтыг хийдэг энэ нь үйлдийн системд илүү амар найдвартай нэвтрэх аргуудын нэг юм.

2.3.3 Smart картны баталгаажуулалт

Смарт картын технологи нь гэрчилгээнд үндэслэсэн баталгаажуулалтын жишээ юм. Ухаалаг карттай нь сүлжээнд нэвтэрч хэрэглэгчийг домейнд 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.

2.3.4 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 сертикатаа үүсгэж адилтган танилт хийх технологи юм. Таны төхөөрөмжийн Mac хаягаар сертикат үүсгэж сүлжээнд холбогдох үед нь баталгаажуул боломжтой.

2.3.5 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.

Бүлэг 3

Судалгааны хэсэг

3.1 Windows-г түгжих болон нээх

Хэрвээ та өөрийн зөөврийн болон суурин компьютерийг түр хугцаанд орхих шаардлагтай ба компьютераа унтраахыг хүсэхгүй байгаа бол WINDOWS screen лок/lock/ болон ан лок/unlock/ үйлдлийг хийх хэрэгтэй болно. Лок үйлдэл нь таны компьютерийн дэлгэцийг хаах ба хэрэв нээхийг оролдвол нууц үг , нэр зэргийг нэхдэг . Харин authentication хийж системд буцаж нэврэхийг ан лок үйлдэл гэдэг. Өөрөөр бол түгжих үйлдэл нь янз бүрийн үйлдлийн системд хэрэглэгддэг компьютерийн хэрэглэгчийн интерфэйстэй элемент юм.

- Өөрийн компьютерийг түгжихийн тулд та POWER хэсгийн Sleep модонд тавих боломжтой . Өөрөөр бол та Windows -ийн лого бүхий цонх товчлуур нэмэх нь L товчлуурийг дархад л таны компьютер түгжигдэх бөгөөд Windows-ийн нэвтрэх дэлгэц гарч ирнэ.
- Компьютерийн түгжээг онгойлгохдоо Windows -ийн нэвтрэх дэлгэц дээрээс Ctrl + Alt + Delete дарахад нууц үг нэхэгдэг болно . Уг цонх дээр нууц үгээ хийгээд нэвтрэх боломжтой . Хэрвээ таны компьютер 1ээс олон хэрэглэгчтэй бол таны түгжихээс өмнө нэвтэрсэн байсан хэрэглэгчийн нууц үгийг нэхэх юм.

Windows 10 нь FIDO Холбооноос боловсруулсан стандартуудын дагуу олон хүчин зүйлийн баталгаажуулалт хийх технологийг агуулдаг. Үйлдлийн систем нь Windows Hello платформоор дамжуулан биометрийн баталгаажуулалтыг сайжруулахад орно. Туслах камертай төхөөрөмжүүд (хэт улаан туяаны гэрэлтүүлэг шаарддаг, тухайлбал Intel RealSense гэх мэт) хэрэглэгчид Kinect-тай адилхан хүний хувийн мэдээлэл эсвэл нүүрний таних тэмдгээр нэвтрэхийг зөвшөөрдөг. Мөн уншигчидтай боловсронгуй төхөөрөмжүүд нь хэрэглэгчид хурууны хээ таних тэмдгээр нэвтрэхийг зөвшөөрдөг. Итгэмжлэл нь Windows -доо хадгалагдаж, тэгш хэмт бус шифр ашиглан хамгаалагдсан байдаг.

```
import time
import ctypes
ctypes.windll.user32.LockWorkStation()
```

Зураг 3.1: LockWorkStation функцыг ашиглаж буй нь

3.1.1 LockWorkStation функц

BOOL WINAPI LockWorkStation(void)

LockWorkStation функц нь интерактив компьютер дээр ажиллаж байгаа процессоор дуудагддаг. Уг процессийг дуудаснаар компьютер түгжигддэг. Хэрэв функц амжилттай бол буцах утга нь тэг биш байна асинхроноор гүйцэтгэгддэг учраас буцах утга нь үйл ажиллагааг харуулаж байдаг. Хэрвээ бүрэн ажилж дуусвал windows дэлгэц түгжигддэг.

Хэрэв функц ажиллахгүй бол буцах утга тэг байна. Өргөтгөсөн алдааны мэдээллийг авахын тулд GetLastError руу хандах хэрэгтэй.

Шаардлага :

- Дэмжигдэх хамгын бага хувилбар нь - Windows XP desktop apps only
- Дэмжигдэх хамгын бага server хувилбар нь - Windows Server 2003 desktop apps only
- Header - Winuser.h (Windows.h оруулна)
- Library - User32.lib
- DLL - User32.dll

3.2 USB түлхүүр ашиглан үйлдлийн системд нэвтрэх нь

USB хадгалалтын төхөөрөмжүүд нь нэг компьютероос нөгөөд өгөгдлийг шилжүүлэх олон нийтэд дамжуулах үндсэн шийдэл болж ирсэн. Үүнээс гадна тэдгээрийг clone хөтөчүүдэд ашиглаж болно мөн үйлдлийн системийг суулгах боломжтой boot-лэсэн төхөөрөмжүүдийг үүсгэх боломжтой. Өөр нэгэн боломж нь дээр дурьдсанчлан зарим функцүүдийг ашиглан USB флаш драйверуудын тусламжтайгаар физик түлхүүрүүдийг орлуулахын тулд Personal Computers эсвэл Laptops түгжигч/нээгч

болгож болно. Ердийн нэр нууц үг ашиглан өөрийн төхөөрөмжөө хамгаалдаг хэрэглэгчдийн **35н хувь нь** нууц үгээ хэзээч сольдоггүй нь Global Password Usage Survey болон PC World Piracy Survey зэрэг хэд хэдэн албан байгууллагын судалгаагаар батлагдсан байдаг.

Хэрэглэгч үйлдлийн системд нэвтрэхдээ Флаш драйв-ийг залгаснаар 2 давхар баталгаажуулалт шаардах болно. Хэрэглэгчийн нэвтрэлт танилт буруу үед хэрэгжүүлэхэд шаардлагатай буруу оролдлогын тоог мөн тохируулах боломжтой юм. Байгууллагууд болон аюулгүй байдалын инженерүүд таныг нууц үгээ солихыг байнга шаардаж байдаг. Та хүчтэй нууц үг ашиглахыг хүсч байсан ч нууц үг өөрчлөгдөх бүрт үнэхээр хүчтэй, санамсаргүй нууц үгийг санаж байх нь бараг л боломжгүй юм. Мөн та олон төрлийн бүртгэлтэй бол (Жишээ нь : Instagram , Facebook , Gmail гэх мэт) тэднийг нэг бүрчлэн нууц үгээр хамгаалах түүнийгээ байнга санаж байх нь бүр ч илүү төвөгтэй. Та бүх бүртгэлдээ нэг төрлийн нууц үг үүсгэвэл энэ нь нэг нууц үгээ алдсан тохиолдолд та бүх бүртгэлийн нууц үгээ ахин солих шаардлагатай тулгарна гэсэн үг юм. Түүний шийдэл нь USB флашыг өөрийн физик түлхүүр болгох явдал юм. Түлхүүрэй ашигласнаар та нууц үгээ санаж байх шаардлаггүй юм.

Та өөрийн флаш драйв дээрээ нууц үг болон хэрэглэгчийн нэр гэсэн мэдээллүүдийг хадгалсан байх шаардлагатай ба уг мэдээллийг мөн шифрлэх боломжтой юм. Windows credential дээр үүсгэгдсэн байгаа итгэмжлэлийн мэдээллийг нэг урсгалт шифрлэлтээр шифрлснээр жишээ нь : MD5 адилхан шифрлэгдсэн 2 өгөгдлийг харьцуулж тулгалт хийн нэвтрэх эрхийг баталгаажуулах боломж бий.

Нэвтрэлт хийгдсэний дараа флаш диск залгагдаж байх нөхцөлд л өөрийн компьютерийг ашиглах боломжтой ба салгасан үед автоматаар түгжигдэнэ.

Та флаш диск дээрээ үүсгэсэн итгэмжлэлээ хадгалах шаардлагатай болно. Тиймээс таны флаш диск бага хэмжээний зай агуулах ёстой. Энэ зайнд text файл хадгалах учир 200 mB байхад л хангалттай юм. Харин үлдсэн зайнд та флаш дискний үндсэн ашиглалтыг хийж болно. Мөн хэд хэд итгэмжлэлийн мэдээлэл хадгалж нэг компьютер дээр байгаа олон хэрэглэгч эсвэл олон компьютер дээр байгаа тус тусын хэрэглэгчдийн мэдээллийг ашиглан authentication хийн нэвтрэх боломжтой юм. USB flash drive -аа давхар шалгалт болгох гэж байгаа бол MAC хаягаа мөн бүртгүүлэх шаардлагатай болно. Хэрвээ Mac хаягаараа тулгат хийн нэг флашаар нэг компьютерт нэвтрэхийг хүсвэл дээрх олон нэвтрэлтийн арга нь боломжгүй болох юм.

Хэрэв USB Key залгагдаагүй л бол ажилгааг хориглосон байгаа эсэхийг шалгана. Энэ нь боломжтой бөгөөд таны хатуу диск / HARD /

эсвэл компьютер хулгайлсан тохиолдолд таны өгөгдлийг хамгаалахад тохиромжтой арга юм . Мэдээж таны өгөгдөл байгууллагын нууц мэдээлэл зэрэг байвал ямагт хамгаалах шаардлагтай юм. Гэхдээ хэрэв таны компьютерт хэн нэгэн алсаас хандсан байвал USB түлхүүр нь ямар ч үр дүнгүй гэдгийг мэдэх хэрэгтэй . Та алсын хандалтыг хэрэглэгдэхгүй болгох мөн ямар нэгэн нөхцөл биелэгдсний дараа /USB залгагдах гэх мэт / алсаас хандах эрхтэй болгох гэх мэт асуудлыг мөн шийдэж болно .

3.2.1 USB түлхүүрийн давуу болон сул талууд

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, Жоккоб 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 вирусын эсрэг програм зэргээр дайралт хийхэд нэвтрэх, эсвэл дамжин өнгөрөх үеэр эмзэг нууцлалын нэвтрэх эрхийг хулгайлж чадна.

3.2.2 Эрсдэлээс сэргийлэх нь

Та windows -д нэвтрэхдээ USB флаш драйв ашигладал байсан гэж бодъё . Харин таний USB flash дискийг хэн нэг нууцаар авсан аль эсвэл гэмтсэн бол та нууц үгээ хийн нэвтрэч болох юм . Флаш драйв -ийн давуу талыг ашиглаж нууц үгээ урт төвөгтэй хийснээр та нууц үгээ санахгүй байгаа бол дараах аргаар сэргээж болно. Та Windows уруу нэвтрэч чадахгүй учраас сэргээх дискээр дамжуулан System Restore руу хандах хэрэгтэй болно. Энэхүү энгийн процессыг Windows 10 компьютер дээр хийж болох бөгөөд нэг төрлийн 32-бит эсвэл 64-битийн Windows 10 компьютерт ашигладаг. Энэ боломжийг олох хамгийн хялбар арга бол taskbar дахь хайлтын самбарт сэргээх хөтчийг бичих явдал юм.

3.2.3 USB түлхүүртэй холбоотойгоор хийгдсэн ажилууд

USB төхөөрөмжийг ашиглах олон тооны арга хэрэгслүүд өдрөөс өдөрт шинчлэгдэн гарсаар байгаа юм. Жишээ дурьдвал :

- Zhihui Liu гэх иргэн итгэмжлэгдсэн холболттой USB Key дээр үндэслэн таниулалтыг баталгаажуулах схемийг байгуулсан. Тэрбээр төхөөрөмжийн нэвтрэлт танилт нь хэрэглэгчийн нэвтрэлт танихтай адилхан байгаагүй бөгөөд ингэснээр хэрэглэгчийн нэвтрэлт танилтын үүрэг гүйцэтгэдэг давтагдашгүй USB системийг ашигласан бөгөөд ингэснээр програмын серверт хандах боломжийг олгодог.

- Мэдээллийг батламжлан найдвартай болгох өөр нэг аргыг Ю Жин-Вэй гэх эрхэм санал болгосон бөгөөд энэ нь USB түлхүүр дээр суурилсан логик системийг санал болгож нэвтрүүлэх процессыг мөн сайжруулсан .
- Тао Yizheng уламжлалт болон ганц нэвтрэлт танилтын найдваргүй сул талыг шинжилж, ХХЗБ-ыг таньж баталгаажуулах , олон хүчин зүйл таних систем болон USB Key тоон гэрчилгээг боловсруулсан болно.

3.2.4 USB түлхүүрийн цаашдын хөгжүүлэлт

USB түлхүүрийг ашиглан үйлдлийн системд нэвтрэхийг хөгжүүлэх боломж нь :

- Өвөрмөц түлхүүр үүсгэх , нэвтрэлт танилтыг түүгээрэй дамжуулан баталгаажуулах
- Лог файлтай харьцах, үйл явдлыг бүртгэх
- Сэргээх систем

Usb drive -ийг залгах үед үйлдлийн систем дээр өвөрмөц түлхүүр үүсгэх боломжтой юм . Та үүсгэсэн итгэмжлэлээ шифрлэж , аль эсвэл итгэмжлэлтэй хамаатай ямар нэгэн өгөгдөл өгсөн үед түүнтэй адилхан үүсгэгдэн түлхүүрээр адилтган таниулалт хийгдэнэ гэсэн үг юм. Ийм боломжийг үүсгэвэл нууц үгийг ашиглах шаардлаггүй болох ба нууц үгийг илрүүлэх төрөл бүрийн халдлагуудаас сэргийлэх болмжтой . Энгийн USB түлхүүрийг ашиглах үед нууц үг нь хэвийн байдаг ба флаш диск салгагдсан үед Broute Force зэргийг хийх боломжтой юм . Үүнээс ч мөн адил сэргийлж болно .

Лог файл үүсгэснээр та флаш драйваа залгах үед үйлдлийн систем дээр таны хийгдэн ажилуудыг тэмдэглэх болно. Хэрвээ таны компьютерийн нууц үгийг хэн нэгэн таах гэх оролдох , мөн таны флаш диск дээрх мэдээллийг нууцаар хуулан өөрөөр флаш драйв дээр суулгаад таны компьютерт нэвтрэсэн бол та үүнийг мэдэх боломжтой юм . Мөн цаашдын хөгжүүлэлтийн түвшинд таны флашаас өөр флаш залгагдвал нээгдэхгүй байх нөхцөл үүсгэх MAC хаягын мэдээлэл зэрэгийг бүртгэх мөн боломжтой юм.

Flash disk ашиглан нэвтрэлт хийж байгаа үед хамгын том эрсдэл бол та флаш дискээ алдах мөн гэмтээх явдал юм. Флаш дискээ алдасны дараа нууц үгээ хийн нэвтэрч болох ч өөрийн мэдээллийг дахин сэргээх шаардлагтай .

3.3 Windows credential гэж юу вэ?

Windows итгэмжлэл буюу Credential хэмээх ойлголт нь сүлжээнд ямар нэгэн веб сайт болон бусад компьютеррүү нэвтрэхэд ашиглан хэрэглэгчийн нэр болон нууц үг гэх мэт итгэмжлэгдсэн мэдээллийг хадгалж итгэмжлэл үүсгэж мөн үүсгэсэн итгэмжлэлээрэй нэвтрэх эрхийг олгодог. Өөрөөр бол үйлдлийн систем хэрэглэгчийн итгэмжлэлийг хүлээн авч баталгаажуулалт хийхийн тулд мэдээллийг хадгалах процесс юм. Нэвтрэх хэсэгт нь биометрийн хэмжигдэхүүн ашиглан хурууны хээ ,ухаалаг карт , USB дискээр нэвтрэх зэрэг нэмэлт баталгаажуулах механизмийг итгэмжлэл үүсгэх замаар хэрэгжүүлэх боломжийг олгодог . Winlogon нь интерактив logon хийдэг Windows модуль юм. Winlogon төлвийг итгэмжлэл ханган нийлүүлэгчийг хэрэгжүүлэх болон бүртгэх замаар өөрчилж болно.Итгэмжлэлүүдийг хангагч нь :

- Windows vista
- Windows 7 ,8,10
- Windows server 2008 , 2008 R2 гэх мэт үйлдлийн системүүд багтана.

Доорх хүснэгтэд одоогоор интерактив logon архитектурт багтах бүрэлдэхүүнийг жагсаасан болно.

| Бүрэлдхийн хэсэг | Тодорхойлолт |
|---|---|
| Winlogon | Интерактив нэвтрэлтийг дэд бүтцийг хангадаг. |
| Logon UI | Интерактив хэрэглэгчийг интерфэйсээр хангадаг. |
| Итгэмжлэлийн үйлчилгээ үзүүлэгч(Нууц үг , Ухаалаг карт) | Итгэмжлэлүүдийн мэдээллийг эрэмбэлж итгэмжлэлүүдийг тайлбарладаг. |
| LSA | Логон итгэмжлэлүүдийг боловсруулдаг |
| Authentication багц | NTLM болон Kerberos орно. Хэрэглэгчдийг таниулахын тулд серверийн нэвтрэлт танилт багцуудыг хангадаг. |

Хэрэглэгч CTRL + ALT + DELETE дарахад Windows интерактив logons эхэлнэ. CTRL + ALT + DELETE товчлуурын хослолыг аюулгүй анхааралын дараалал (SAS) гэж нэрлэдэг.

Windows Итгэмжлэл нь гурван ангилалд хуваагдана:

- Windows Credentials - зөвхөн Windows болон түүний үйлчилгээнд ашиглагдана. Жишээлбэл: Windows танай сүлжээнд өөр компьютерын хуваалцсан фолдерууд буюу Shared Folder- руу автоматаар нэвтрэхийн тулд энэ мэдээллийг ашиглаж болно. Эсвэл, бүлгийн нууц үгийг хадгалахын тулд та холбогдож , хуваалцсан зүйлсэд /файлд / хандах бүрдээ автоматаар үүнийг ашигладаг. Хэрэв та буруу нэвтрэлтийн Credentials хэрэглэж байгаа бол, Windows үүнийг санаж байх боловч таны access хийх эрхийг баталгаажуулах болно.
- Сертификатанд суурилсан итгэмжлэл (Certificate-Based Credentials) - Эдгээр нь ухаалаг картын хамт хэрэглэгддэг, ихэвчлэн илүү төвөгтэй бизнесийн сүлжээний орчинд ашиглагддаг. Энэ нэвтрэлтийг компьютерийн хэрэглэгчид ихэвчлэн ашигах шаардлаггүй байдаг бөгөөд ашигласан тохиолдолд таны Windows дээр ийм танилт байхгүй учир хоосон байхыг анхаарах хэрэгтэй.
- Ерөнхий итгэмжлэл (Generic Credentials) - Generic итгэмжлэлүүд нь таны суулгах зарим програмуудаар тодорхойлогддог бөгөөд тэдгээр нь тодорхой нөөцүүдийг ашиглах эрх олгодог. Ерөнхий итгэмжлэлийн түгээмэл нэг жишээ нь Windows Live Security Essentials-д орсон хэрэгслүүдийг ашиглан хадгалж , ашиглаж байгаа Windows Live ID юм.

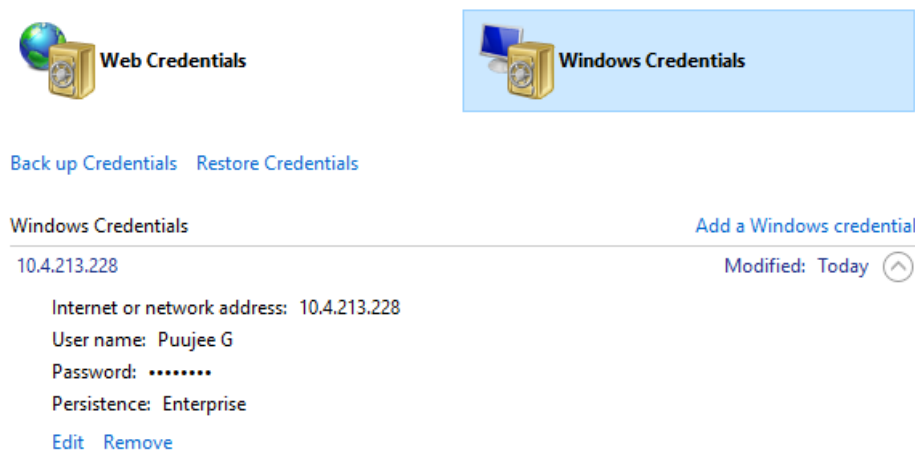
Эдгээр итгэмжлэлийг Windows болон таны ашиглаж буй програмууд автоматаар хадгалж, удирдаж болно. Хэрэв та компьютер дээр ямар итгэмжлэлүүд хадгалагдаж байгаагаа мэдэхийг хүсэхгүй эсвэл устгах , засварлах хэрэгтэй бол та credential management ашиглах шаардлагатай болно.

3.3.1 Adding a Credential - Итгэмжлэлийг нэмэх

Windows credential -ийг нэмсэнээр хэрэглэгч нэмэгдсэн хэрэглэгчийн хуваалцсан мэдээллийг автоматаар харах боломжтой болно . Хэрэглэгчийг нэмэхдээ Credential management -ийн windows credential хэсэгт орж нэмнэ. Нэмэхдээ хэрэглэгчийн нэр , нууц үг , IP хаяг зэргийг мэдэж байх шаардлагатай . Мөн windows итгэмжлэлийг хасах боломжтой бөгөөд дээрх зурагт харуулсан болно .

3.3.2 Windows credential management

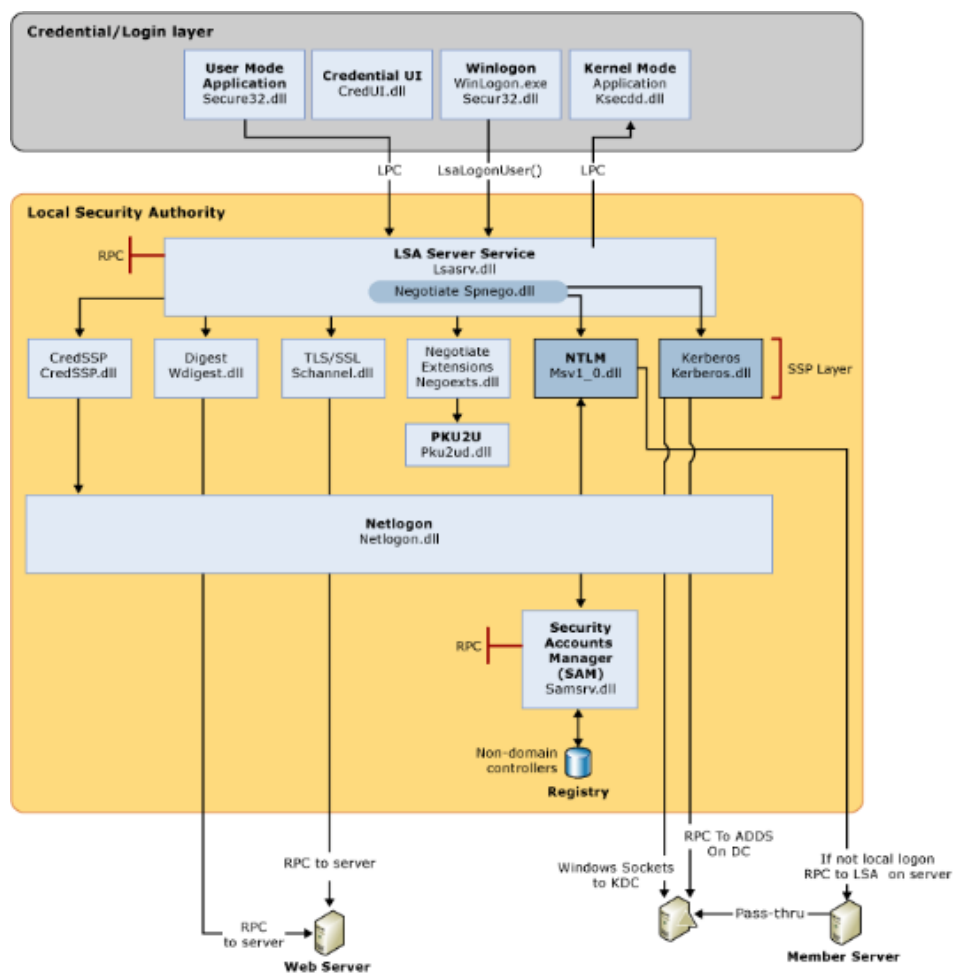
Итгэмжлэлийн менежмент удирдлагын API нь Windows хэрэглэгчийн нэр нууц үг гэм мэт эдгээрийг удирдан зохион байгуулахтай холбогдсон чиг үүргийн итгэмжлэгдсэн мэдээллийг удирдах бөгөөд итгэмжлэлийн



Зураг 3.2: Windows итгэмжлэлийг нэмсэн процесс

менежмент нь хэрэглэгчийн удирдлагын интерфэйсийг ашиглаж болно. Итгэмжлэлүүдийн менежер нь та сүлжээний веб сайт болон бусад компьютеррүү нэвтэрхэд ашиглах хэрэглэгчийн нэр болон нууц үг гэх мэт итгэмжлэлүүдийг хадгалах боломжийг олгодог. Таны итгэмжлэлийг хадгласан тохиолдолд үйлдлийн систем автоматаар веб сервер болон бусад компьютерт нэвтэрч болно.

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



Зураг 3.3: Итгэмжлэлийн баталгаажуулалтын зураг

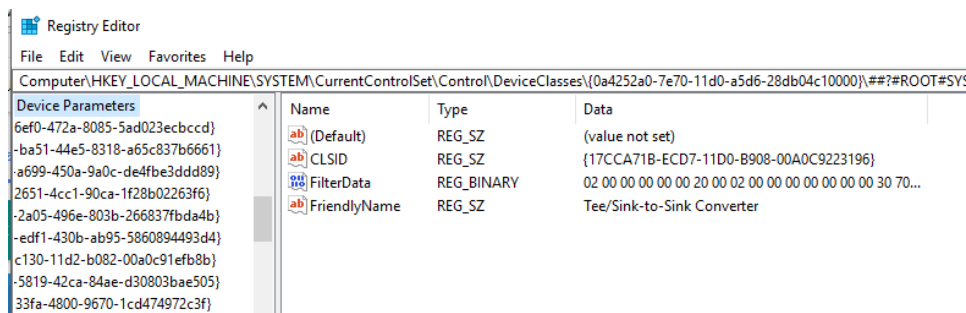
Тухайн зурагт харуулсан бүрэлдхийн хэсгүүдийг харуулвал .

- 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.

3.3.3 Credential Guard

Хэрэв та pass-the-hash халдлагын талаар санаа зовж байгаа бол Windows 10-ийн итгэмжлэгдсэн хамгаалагчийг хэрэгжүүлээрэй. Энэ нь Windows нэвтрэлт танилтыг зохицуулдаг (LSA) болон VBS-д хэрэглэгчийн үүсгэсэн итгэмжлэлүүдийг (NTLM хэш гэх мэт) хамгаалдаг. Баталгаажуулах үйлчилгээ болон NTLM итгэмжлэлийн өгөгдлийг хамгаалахын тулд VBS нь сүлжээнд суурилсан PtH халдлагаас хамгаалдаг.

Сул тал дээр Гишүүний хамгаалалт нь орон нутгийн итгэмжлэлүүдийг (дискэнд эсвэл бүртгэлийн системд байрладаггүй) хамгаалахгүй бөгөөд одоогоор Remote Desktop Protocol logons-тай ажилладаггүй. Гэхдээ хэрэв та орон нутгийн захиргааны нууц үгүүд нь компьютеруудын хооронд өвөрмөц байдгийг эс тооцвол энгийн нууц үгийн hash халдагч таны сүлжээг ашиглах гэж оролдоход зогсохгүй бол удааших болно.



Зураг 3.4: Registry-д хандсан байдал

3.4 Windows Registry гэж юу вэ ?

Registry нь нь Microsoft Windows үйлдлийн систем ашиглагддаг програмуудад зориулсан доод түвшний тохиргоонуудыг хадгалах шаталсан мэдээллийн сан юм. Цөм, төхөөрөмжийн драйвер, үйлчилгээ, Security Accounts Manager (SAM), болон хэрэглэгчийн интерфэйс бүгд Registry-ийг ашигладаг. Windows Registry-г өөрөөр компьютер дэхь бүх мэдээллийн нэгдсэн төв гэж хэлж болно. Энд үйлдлийн систем, хардвер, инсталл гээд бүхий л компьютерийн хэсгүүдийн мэдээлэл агуулагдаж байдаг бөгөөд ямарваа нэг өөрчлөлтийг компьютерт хийхэд энэ нь Windows Registry-д тэмдэглэгдэж байдаг. Windows үйлдлийн системийн бүх хувилбарт суулгасан програмууд болон тоног төхөөрөмжүүдэд зориулсан мэдээлэл, тохиргоо, сонголтууд болон бусад утгуудыг агуулдаг. Жишээлбэл, програм суулгах үед програмын байршил, хувилбар, хэрхэн програмыг эхлүүлэх зэрэг шинэ програмыг Windows бүртгэлд нэмдэг. Windows Registry -аас өмнө .INI файлууд нь олон хэрэглэгчийн хувилбарт тохиргоог хангахгүй байсан ба мөн заасан байршилд програмын тохируулга бүрийг текст файл болгон хадгалдаг байсан .

Microsoft-ийн мэдээлснээр registry нь хэд хэдэн давуу талтай:

- regedit.exe, built-in Windows Registry Editor програмыг ашиглан түлхүүрүүдийг засварлахад ашиг тустай .
- Нэгдсэн нэг удирдлага бүхий цогц системтэй .
- Хэрэглэгчид суурилсан бүртгэлийн тохиргоонууд нь зөвхөн үндсэн системийн байршлаас бусдаар хэрэглэгчийн өөрийн hard disk дээр заасан замаас дуудагддаг учраас Registry нь олон хэрэглэгчид ижил машиныг хуваалцах боломжийг олгодог, мөн давуу эрхтэй хэрэглэгчдэд зориулсан програмууд ажиллах боломжийг олгодог.

- Бүртгэлд алсын удирдлага /скриптүүдээс, стандарт API-уудыг ашиглан Remote Access / support-д сүлжээний холболтоор хандаж болно. Алсын Бүртгэлийн үйлчилгээ ажиллаж байгаа бөгөөд firewall дээр үүнийг хүлээн зөвшөөрдөг зөвшөөрдөг.

Жишээ дурьдвал :

- HKEY CLASSES ROOT -нь бүртгэгдсэн бүх програмын мэдээллийг агуулах буюу түүнтэй холбоотой файлууд
- HKEY CURRENT USER - Хэрэглэж буй хэрэглэгчийн тодорхойлсон тохируулгыг агуулдаг, хэрэв компьютер давхар хэрэглэгчтэй бол хэрэглэч тус бүрийн тохируулга байрлах газар юм.
- HKEY LOCAL MACHINE - Бүх хэрэглэгчдийн тохируулгыг агуулана.
- HKEY USERS - HKEY CURRENT USER-ийн нэг хэсэг болох хэрэглэгч бүрийн тухайлсан агуулах
- HKEY CURRENT CONFIG - Асаж унтрахтай холбоотой файлын агуулах. Энэ нь зөвхөн компьютер унтарч асахад хэрэглэгдэх бөгөөд хатуу дискэнд хадгалагдаггүй.

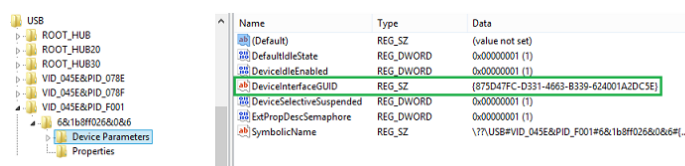
Windows Registry нь c:\windows\system32\config хавтас дотор байрлах хэд хэдэн тухайлбал SAM, SOFTWARE, SECURITY, болон SYSTEM файлуудаас тогтдог. Мөн NTUSER.DAT гэж нэрлэгдэх c:\Documents and Settings<your user name> байрладаг файл мөн агуулагддаг .

3.4.1 Usb түлхүүрийг register-т бүртгүүлэх

1. USB төхөөрөмж нь таны компьютерт холбогдсон үед HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\ -ийг олж DeviceInstance утгыг тэмдэглэнэ.

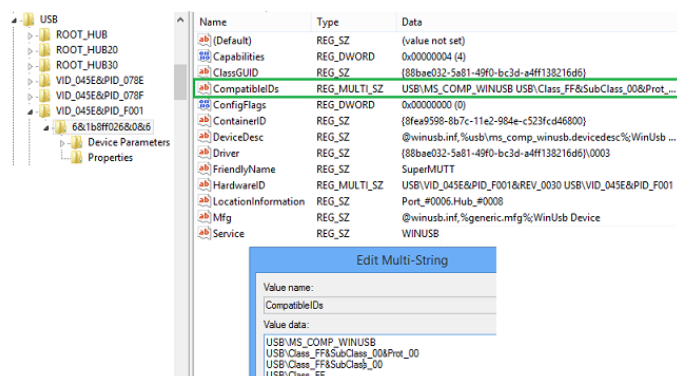
| Name | Type | Data |
|----------------|--------|--------------------------------------|
| (Default) | REG_SZ | (value not set) |
| DeviceInstance | REG_SZ | USB\VID_045E&PID_F001\681b8ff026&0&6 |

2. Төхөөрөмжийн түлхүүрийг олох ба төхөөрөмжийн интерфэйс GUID авах. HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Enum\USB/<hardware id>/<instance id>/Device Parameters дотор орно.



| Name | Type | Data |
|--------------------------|-----------|---|
| (Default) | REG_SZ | (value not set) |
| DefaultIdleState | REG_DWORD | 0x00000001 (1) |
| DeviceIdleEnabled | REG_DWORD | 0x00000001 (1) |
| DeviceInterfaceGUID | REG_SZ | {875D47FC-D331-4663-B339-624001A2DC5E} |
| DeviceSelectiveSuspended | REG_DWORD | 0x00000001 (1) |
| ExtPropDescSemaphore | REG_DWORD | 0x00000001 (1) |
| SymbolicName | REG_SZ | \\?\\USB#VID_045E&PID_F001#681b8ff026&0&6#... |

3. HKEY LOCAL MACHINE/SYSTEM/CurrentControlSet/Enum/USB руу орж Төхөөрөмжийн instance түлхүүр үгийн дагуу төхөөрөмжийн анги, дэд анги, протокол кодыг тэмдэглэнэ.



4. USB драйверийн стекийн тохиргоог тохируулах бүртгэлийн тохиргоо:

```
HKEY LOCAL MACHINE
SYSTEM
    CurrentControlSet
        Control
            usbflags
                VVVVPPPPRRRR
                    Device-specific registry entry
```

- vvvv нь борлуулагчийг тодорхойлдог 4 оронтой 16-тын тоо
- rrrr нь бүтээгдэхүүнийг таниулсан 4 оронтой 16-тын тоо
- gggg нь төхөөрөмжийн тоон утгыг агуулдаг 4 оронтой 16-тын тоо

3.5 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.

Жишээ нь: Клауд орчинд файл хадгалах үйлчилгээ үзүүлдэг “Dropbox” компани хэрэглэгчдийнхээ аюулгүй байдлыг сайжруулах томоохон алхам хийсэн. Интернэтээр үйлчилгээ авч байгаа хэрэглэгч аюулгүй байдалаа хангахын тулд хоёр алхамт нэвтрэх системийг ашиглаж байсан бол

энэ удаад “USB” оролттой түлхүүр ашиглан “Dropbox” дахь сан руугаа нэвтрэх боломжтой болсон байна. Ингэснээр хоёр алхамт нэвтрэх систем ашигладаг байсан хэрэглэгчид нууц үгээ оруулаад, гар утсанд мессежээр ирсэн 6 тэмдэгт бүхий кодыг оруулдаг байсан нь өөрчлөгдөж, нууц үг болон “USB” түлхүүрээрээ нэвтрэх юм. Ийм замаар нэвтрэх нь аюулгүй байдлыг улам бүр баталгаажуулна. Учир нь мессежээр авах код болон баталгаажуулах аппликейшнүүдийг ч хөндлөнгөөс хакердах боломжтой байдаг юм.