Шинжлэх Ухаан Технологийн Их Сургууль
Мэдээлэл, Холбооны Технологийн Сургууль

Гомбожав Пүрэвсүрэн

Толь бичгийн халдлагын програм бүтээх нь

Систем хамгааллын төсөл

Улаанбаатар хот

Шинжлэх Ухаан Технологийн Их Сургууль
Мэдээлэл, Холбооны Технологийн Сургууль

Мэдээллийн сүлжээ, Аюулгүй байдал

Толь бичгийн халдлагын програм бүтээх нь

Мэргэжил: Системийн аюулгүй байдал

Удирдагч: Магистр Г.Дашзэвэг
Зөвлөгч: Магистр Г.Дашзэвэг
Гүйцэтгэгч: Г.Пүрэвсүрэн

Улаанбаатар хот
2017 он 11 сар

Гарчиг

Зургийн жагсаалт

Хүснэгтийн жагсаалт

БҮЛЭГ 1

Зорилго

1.1 Удиртгал

21-р зууныг хүн төрөлхтөн техник технологийн зуун хэмээн нэрийдэж буй билээ. Харин техник технологи хөгжихийн хэрээр аюул занал мөн даган хөгжсөөр байна. Тухайн аюул заналууд дунд томоохон байр суурь эзэлдэг халдлагуудын нэгт толь бичгийн халдлага зүй ёсоор ордог байна. Энэ халдлагын тухай ярихын тулд бид юуны өмнө нууц үг гэж юу болох түүний оновчтой сонголт зэргийн талаар авч үзнэ. Толь бичгийн халдлага нь хувь хүн болон албан байгууллагад их хэмжээний хохирол учруулах боломжтой бөгөөд тухайн халдлага хэрхэн явагддаг түүнчлэн халдлагад өртөхөөс хэрхэн зайлсхийх талаар мэдээлэлийг өгөхөд оршино.

1.2 Зорилго

Энэхүү төслийн ажлын зорилго нь Мэдээллийн Аюулгүй Байдал, түүнийг хангах аргууд цаашлаад халдлага гэж юу болох мөн түүний нэгэн төрөл болох толь бичгийн халдлага зэргийг судлан тухайн халдлагыг хялбар аргаар гүйцэтгэх боломжтой веб хөтөчийн нэмэлт буюу extension бүтээх явдал юм.

1.3 Зорилт

- Мэдээллийн Аюулгүй Байдал гэж юу вэ?
- Халдлага гэж юу вэ?
- Халдлагын төрлүүд
- Толь бичгийн халдлага гэж юу вэ?
- Урьдчилан сэргийлэх
- Веб хөтөчийн нэмэлтийн тухай судлах

БҮЛЭГ 2

Онолын хэсэг

2.1 Мэдээллийн Аюулгүй Байдал гэж юу вэ?

Үндсэн ойлголт

Анх "Компьютерийн Аюулгүй Байдал", "Мэдээллийн Технологийн Аюулгүй Байдал" гэсэн ойлголтууд мөн технологитой холбоотой аюулгүй байдлыг илэрхийлж байв. Улмаар хүнээс хамааралтай аюул, удирдлага, зохион байгуулалттай холбоотой эрсдэлүүд нэмэгдсэн учир утга нь өргөсөж "Мэдээллийн Аюулгүй Байдал" (МАБ) хэмээн нэрлэж байна. МАБ-ыг хангах үндэс суурь нь эрсдэлийн үнэлгээ, эрсдэлийн удирдлага байна. Эрсдэл гэдэг ойлголт нь аюул, эмзэг байдлын хослолоос үүсдэг.

2.1.1 Аюулууд

Аюул – МАБ-ыг ямар нэг байдлаар зөрчиж болох боломжуудыг хэлнэ. Аюул заналхийллийг хэрэгжүүлэх оролдлогыг халдлага гэнэ. Аюул заналхийлэл нь МАБ-ын удирдлага, зохион байгуулалт, Мэдээллийн Систем, сүлжээний эмзэг байдал, цоорхойг ашиглан хэрэгждэг. Цоорхойг хаах, арилгах хүртэл түүнийг ашиглах боломж оршсоор байна. Цоорхой, эмзэг байдал, түүнийг ашиглах хэрэгсэл, арга цаг минут тутамд шинээр үүсэж, бий болж байдаг тул аюул заналын эрсдэл байнга оршин байдаг, тиймээс эдгээр цоорхойг хянан шалгаж, шуурхай бөглөж байх ёстой.

Зарим аюул хэд хэдэн эд хөрөнгөд хор хохирол учруулж болно. Ямар эд хөрөнгөөсөө хамаараад үйлчлэл нь өөр өөр байж болно. Жишээ нь: нэг компьютер дээр суусан програмын вирус аюул багатай байхад сүлжээний сервер дээр энэ вирус суувал илүү хортой үр дагавартай. Аюул, халдлагууд хэдэн зуун мянган хэлбэр, төрөлтэй болсон. Зарим нийтлэг аюулын жишээг дараах хэсгээс харна уу:

Хортой кодууд – Вирус, Өт, Трояны морь Хууль бусаар нэвтрэх – Эмзэг цоорхойг ашиглан зүй бусаар хандах "Social engineering" – Хууль бусаар хандахын тулд хэрэглэгчийг хууран мэхлэж түүний мэдээлэл, мөнгө, баялагийг авах Аюул хэрэгжсэний улмаас үүсэх хор хохирол

Зарим эд хөрөнгийг устгах, МС-ийг гэмтээх, нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдал, тасралтгүй ажиллагаа, сэргээгдэх шинж, бодит байдал, найдвартай шинжийг алдагдуулах хор уршиг учирч болно. Шууд бус хор хохирол нь санхүүгийн алдагдал, зах зээлээ алдах, нэр хүндээ алдах гэх мэт Хор хөнөөлийг үнэлэх нь эрсдэлийг үнэлэх, хамгаалалтын арга хэмжээг сонгоход их нөлөөтэй. Хор хөнөөлийг тоон болон чанарын талаас хэмжихэд дараах аргуудыг ашиглана: Санхүүгийн алдагдлыг тооцох, Ноцтой байдлыг

нь үнэлэх, Жишээ нь: 1-ээс 10 хүртэл оноогоор Урьдчилан гаргасан жагсаалтын тодорхойлолт, шинжүүдийг ашиглах, Жишээ нь: Их, дунд зэрэг, бага гэх мэт.

2.1.2 Тодорхойлолт

Мэдээллийн Аюулгүй Байдал (МАБ) гэдэг нь өргөн утгаараа "Нийгэм, институт, байгууллагын мэдээллийн орчны хамгаалагдсан байдал", эсхүл "Мэдээлэл, өгөгдөл, түүнийг дэмжих дэд бүтцийн хамгаалагдсан байдал" (байгууллагын аюулгүй байдалтай ижил болж байна) юм. Гэхдээ эдгээр ойлголт зарим талаар явцуу шинж чанартай.

"Мэдээллийн аюулгүй байдал" гэдэгт гадны болон дотоодын сөрөг нөлөөллөөс үл хамааран мэдээлэл, түүнийг дэмжих дэд бүтцийн Нууцлагдсан байдал (confidentiality), Бүрэн бүтэн байдал (Integrity) , Хүртээмжтэй байдал (Availability)-ийг хангаж, өөрийгөө хөгжүүлэх чадвараа хадгалж буй мэдээллийн орчны тогтвортой байдлыг ойлгож болохоор байна. Мэдээллийн орчин гэдэгт мэдээллийн харилцан ажиллагаанд оролцож буй субъектуудын нэгдэл, уг харилцан ажиллагааг хангаж буй технологи, төрөл бүрийн нөөцүүдийг ойлгоно.

2.1.3 Мэдээллийн аюулгүй байдлыг хангах 4 түвшин

Эрх зүйн түвшин: МАБ-ын талаар хууль, эрх зүйн актууд, үндэсний хэмжээний стандарт

Захиргаа удирдлагын түвшин: байгууллагын МАБ-ын үзэл баримтлал (стратеги), бодлого, хөтөлбөр, хяналт

Дэгийн түвшин: байгууллагад хэрэгжүүлсэн МАБ-ын дэг, журам, үйл ажиллагааны арга барил

Програм-техникийн түвшин: Мэдээллийн болон сүлжээ, системийн аюулгүй байдлыг хангах зориулалттай төрөл бүрийн тоног төхөөрөмж, програм хангамжууд

МАБ-ыг хангах үндсэн зарчим:

Эрсдэлийн удирдлага: Зохих арга хэмжээг хэрэгжүүлэх замаар байгууллагын эд хөрөнгийг (мэдээллийг) хамгаалсан байна. Эрсдэлийн удирдлагын зохистой аргачлал дээр суурилан аюулгүй байдлын арга хэмжээг сонгож, хэрэгжүүлнэ. Энэ аргачлалын дагуу эд хөрөнгө, аюул, эмзэг байдал, түүний нөлөөлөл зэргийг үнэлж эрсдэлийг бууруулж, хязгаарлана. Үзэл бодол, хандлага: МАБ болон эрсдэлийн удирдлагад хандах байгууллагын хандлагыг зөв тодорхойлох. Зөв хандлага бий болгохын тулд МАБ-ыг хэрэгжүүлсний

ашиг тусыг тодорхойлсон байна. Гүйцэтгэх болон хүлээх үүрэг: Эд хөрөнгийг аюулгүй байлгах үүргийг удирдлага хүлээнэ. МАБ-ын талаар гүйцэтгэх болон хүлээх үүргийг тодруулж бүгдэд мэдэгдсэн, хэвшүүлсэн байна. Зорилго, стратеги, бодлого: Байгууллагын зорилго, стратеги, бодлогын дагуу эрсдэлийг удирдана.

2.1.4 Эрсдэлийн удирдлага

"Эрсдэл" – энэ бол аюулгүй байдал хэмээх зүйлийн суурийг бүрдүүлж буй үндсэн үзэл баримтлал. Эрсдэл – энэ бол хамгаалалт шаардаж буй хор хохирол учрах магадлал. Эрсдэл байхгүй бол хамгаалалт хэрэггүй. Эрсдэл бол аюулгүй байдлын салбарт ажиллагсдын заавал ойлгох зүйл.

Аюул болон эмзэг байдлын хослол. Эмзэг сул байдал болон аюул заналхийлэл нь эрсдэлийн үндсийг бүрдүүлнэ. Эмзэг байдал гэдэг нь довтолгоон үйлдэж болох боломжит суваг, зам. Систем, сүлжээ болон захиргааны дэг жаягт байдаг. Аюул заналхийлэл гэдэг нь мэдээллийн систем, сүлжээний аюулгүй байдлыг зөрчиж, эвдэж чадах үйлдэл, үйл явдал. Эрсдэлийг үнэлнэ гэдэг нь урьдчилан таах аргагүй үйл явдал бий болох магадлалыг тодорхойлох үйл явц. Эрсдэлийг үнэлсний үндсэн дээр эрсдэлийн түвшинг тодорхойлон гаргаж, дараалалд оруулж хамгийн ноцтой эрсдлүүдээс эхлэн бууруулах арга хэмжээг төлөвлөн хэрэгжүүлнэ. Эрсдэлийн үнэлгээг ихэвчлэн гэрчилгээжсэн аудиторууд гүйцэтгэдэг. Мөн байгууллагын мэргэшсэн ажилтан, мэргэжлийн байгууллагууд гүйцэтгэж болно.

Эрсдэлийн үнэлгээ хийж, түүний дагуу эрсдэлийг бууруулах цогц арга хэмжээг эрсдэлийн удирдлага гэнэ.

2.1.5 Аюулгүй байдлын хяналтууд

Эрсдэлийн үнэлгээн дээр тулгуурлан шаардлагатай зохих хяналтыг сонгох, хэрэгжүүлэх нь эрсдэлийг бууруулах үндсэн арга хэмжээ байдаг. Хяналтууд мөн чанараараа янз бүрийн байж болох ч эцсийн дүндээ мэдээлэл, мэдээллийг дэмжих дэд бүтцийн нууцлагдсан, бүрэн бүтэн болон хүртээмжтэй байдлыг хангахад чиглэгддэг.

2.2 Халдлага гэж юу вэ?

Компьютерийн эмзэг байдлыг ашиглан Мэдээллийн аюулгүй байдлын эсрэг чиглэсэн аливаа үйлдлийг халдлага гэж хэлж болно. Мөн халдлагийн маш олон төрөл байдаг. Халдлагийн хамгийн түгээмэл хоёр хэлбэр байдаг энэ нь бусниулах буюу ажиллагаагүй болгох мөн дундаас нь мэдээллийг бариж аван өгөгдлийг өөрчилж дахин дамжуулах гэсэн хоёр төрөл юм. Халдлага хийх үе шат нь дараахи хэлбэртэй байна. Үүнд:

- Байг судлах буюу мэдээлэл цуглуулах
- Эмзэг байдлийг илрүүлэх
- Хандалтийг нээх
- Халдлага хийх
- Ул мөрөө цэвэрлэх

2.3 Толь бичгийн халдлага гэж юу вэ?

Толь бичгийн халдлага (Dictionary attack) нь урьдчилан бэлтгэсэн бүх тэмдэгт мөрүүдийн жагсаалтыг шалгаж үзсэнээр нууц үгийг тааж олох халдлага юм. Энэ халдлагыг ихэвчлэн encrypt хийсэн алгоритм нь тайлагдахааргүй эсвэл decrypt хийх боломжгүй нууц үгийг эвдэхэд ашиглана. Урьдчилан бэлтгэсэн толь бичиг дотроос зөв нууц үг гарч ирэх хүртэл бүх үгийг шалгаж үзнэ. Тухайн толь бичгийг бэлдэхдээ тухайн хэрэглэгчийн хувийн мэдээлэл эсвэл сошиал инженерчлэл ашиглах нь зүйтэй. Хувийн мэдээлэл гэдэг нь дуртай өнгө, найзых нь нэр, төрсөн өдөр, төрсөн газар гэх мэтчилэн хэрэглэгч нууц дээрээ тохируулсан байх магадлалтай гэх бусад бүх чухал мэдээлэлүүд багтана.

2.3.1 Аргачлал

Ихэвчлэн толь бичиг дэх үгүүдээр жагсаалт үүсгэдэг үүсгэх учир толь бичгийн халдлага гэж нэрлэдэг. Том хэмжээтэй түлхүүрийн сангаас системтэйгээр хайх brute-force халдлагаас толь бичгийн халдлага нь амжилттай хэрэгжинэ гэж үзсэн цөөн боломжуудыг шалгаж үздэгээрээ ялгаатай. Хүмүүс ихэвчлэн нийтлэг нууц үг эсвэл энгийн үгүүд тээр таамаглаж болохуйц хэдэн тоо эсвэл цэг, таслал гэх мэт тэмдэгт нэмсэн нууц үг сонгох хандлагатай байдгаас шалтгаалж толь бичгийн халдлага ихэвчлэн амжилттай болдог. Их хэмжээний нууц үг тайлагдахад урьдчилан боловсруулсан толь бичгийн халдлага их үр дүнтэй. Урьдчилан боловсруусан толь бичгийг нэг л удаа

үүсгэнэ, ингээд бэлтгэгдсэн нууц үгийн хашуудаар хэдийд ч тохирсон нууц үгийг олх боломжтой. Rainbow table халдлага гэдэг нь урьдчилан боловсруулсан толь бичгийн халдлагыг бодвол илүү нарын аргачлалаар хадгалах багтаамжын хэрэгцээг багасгаж нууц үг таах цагийг бага зэрэг багасгасан халдлага юм.

2.4 Нууц үг гэж юу вэ?

Бүх л системд өөрийн хэрэглэгч болон түүний хувийн мэдээлэлүүдийг таних шаардлагатай байдаг. Хэрэглэгчийг таних олон процесс байж болох ба нууц үг нь хамгийн түгээмэл ашиглагддаг төрөл юм. Системд нэвтрэхэд тухайн хэрэглэгчийн өмнө нь оруулсан нууц үг, тоо эсвэл тэмдэгтийг шаардах процесс юм. Нууц үг нь тэдгээрийн хэрэглэгчийн нэртэй зохицож байх шаардлагатай бөгөөд маш олон төрлийн зүйлүүд нууц үгээр хамгаалагдсан байдаг. Үүнд:

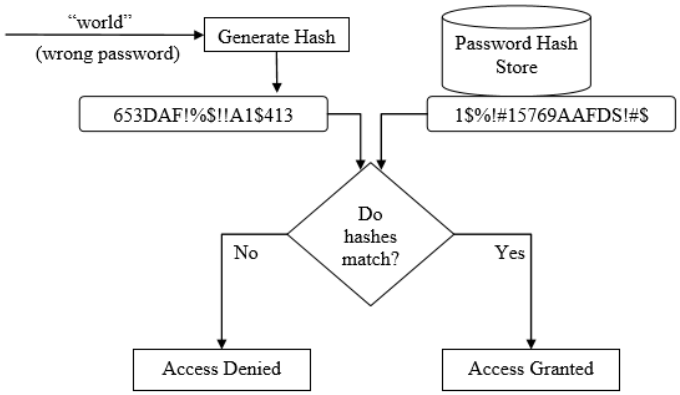
- Үйлдлийн систем
- CMOS
- Document файл
- Програмууд
- Шахсан файл гэх мэт

Эдгээр нь бүгд өөр өөр нууц үгний схем ашигладаг. Үйлдлийн систем дундаас Unix үйлдлийн систем нь чухал байр суурь эзэлдэг.

2.4.1 Үйлдлийн систем дэх нууц үг

Хамгийн түгээмэл үйлдлийн системүүд дээр хэрэглэгчийг адилтган танилт хийхдээ нууц үгийг ашигладаг. Гэсэн хэдий ч үйлдлийн систем бүр хэрэгжүүлэлтийн хувьд өөр өөр механизмыг ашигладаг. Харин хувь хүнд тухайн үйлдлийн систем рүү нэвтрэх эрх авахын тулд итгэмжлэлээ оруулах шаардлагатай. Энэ итгэмжлэл нь хэрэглэгчийн нэр болон нууц үгнээс бүрдэнэ. Хэрэглэгчийн нэр нь аль хэрэглэгч нэвтэрч буйг тодорхойлно. Харин нууц үг нь зөвхөн хэрэглэгч мэддэг бөгөөд үргэлж нууц байх шаардлагатай бөгөөд өөрийгөө мөн гэдгийг баталгаажуулахад хэрэглэнэ. Хэрэглэгчийн нэр болон нууц үгийг оруулсны дараа үйлдлийн систем нь тэдгээрийг зөв эсэхийг шалгаж хэрэв зөв бол нэвтрэх эрхийг хэрэглэгчид олгоно. Үйлдлийн системийн хувьд эдгээр итгэмжлэлүүдийг санах ойд хадгалагдсан эсэхийг шалгах ба үйлдлийн систем хадгалагдсан утгыг оруулсан утгатай харьцуулна. Хэрвээ

хадгалсан нууц үг нь хоосон текст хэлбэртэй байвал энэ нь аюулгүй байдлын чухал асуудал бөгөөд ямарч хэрэглэгч бусад хэрэглэгчийн итгэмжлэлүүдийг харах боломжтой. Тиймээс үйлдлийн систем нь нууц үг бүрийг хаш хэлбэрээр шифрлэдэг. Нууц үгний хаш нь тогтмол урттай бөгөөд ямарч утгагүй юм. Нэг талаар хаш функц нь нууц үгний хаш утгыг нууц үгнийхээ утгаас гаргаж авдаг. Гэсэн хэдий ч хаш нь тооцоологдсоны дараа хаш утгаасаа буцааж нууц үгээ гаргаж авах нь боломжгүй хэрэг юм. Зарим үйлдлийн системд нууц үгний хашийг үүсгэхдээ 'salt' гэх нэмэлт утгыг ашиглаж хаш функцээ илүү санамсаргүй болгодог. Тиймээс 'salt' гэдэг нь нэмэлтээр нууц үгнийхээ аюулгүй байдлыг ихэсгэх зорилгоор ашиглаж байгаа санамсаргүй богино хэмжээний string юм.

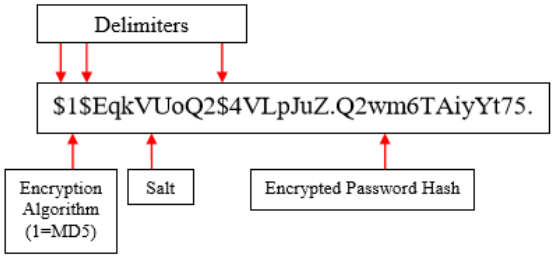


Зураг 2.1: Hash

2.4.2 Unix/Linux MD5 нууц үгний схем

Unix/Linux төрлийн үйлдлийн систем нь олон төрлийн хашлах схемтэй. Сонгодог Unix/Linux үйлдлийн систем нь нууц үгээ хашлахдаа DES алгоритмыг ашигладаг бол түүний шинэ хувилбарууд нь MD5 алгоритмыг ашигласан тохиолдолд Unix/Linux нь хязгааргүй урттай нууц үгийг дэмжиж ажиллах чадамжтай. Unix-ын зарим төрөл нь хамгийн ихдээ 256 тэмдэгтийн урттай нууц үгийг дэмжиж ажилладаг. MD5 алгоритм нь DES алгоритмыг бодвол тооцоолохдоо илүү нарийн тооцдог ба илүү аюулгүй алгоритм юм. Unix/Linux үйлдлийн систем нь нууц үгийг encrypt-лэхдээ 'crypt()' гэх хаш функцыг дуудаж ажиллуулдаг. Энэ функц нь Modular Crypt Format(MCF) encode-г ашиглаж нууц үгээ MD5 эсвэл DES-рүү encrypt хийдэг. Тухайн функцыг

ашиглан нууц үгийг хашлаж дууссаны дараа тухайн хашыг /etc/shadow эсвэл /etc/passwd файл дотор хадгалдаг. Доорхи зурганд MFC-г ашиглан Linux дээр нууц үгээ хэрхэн encrypt хийж буйг харууллаа.



Зураг 2.2: MD5

Дээрхи зурагт харагдаж байгаагаар MCF дэхь MD5 нууц үгний хаш утга нь 3 талбараас бүрдэнэ. Хаш утга дотор харагдаж буй долларын тэмдэгт нь талбар доторхи 3 утгыг хооронд нь ангилж буй зааглагч юм. MFC-ын тус тусын талбарууд болон тэдгээрийн зорилгыг дараахи хүснэгтэнд харуулав.

Field	Purpose	Notes
1	Specifies encryption algorithm	1 specifies MD5, 2 specifies Blowfish
2	Salt	Limited to 16 characters
3	Encrypted password hash	Hash value without salt

Хүснэгт 2.1: MFC

2.5 Толь бичгийн халдлагын төрлийн ерөнхий төрлүүд

- Dictionary attack
- Brute-force attack
- Hybrid attack
- Syllable attack
- Rule-based attack
- Rainbow-table attack

2.5.1 Brute-force attack

Brute-force халдлага гэдэг нь криптографт ямарч шифрлэгдсэн мэдээллийг таахад хэрэглэгддэг нууц бичээсийг тайлж унших халдалага юм. Энэ төрлийн халдлага нь шифрлэлтийн системд ямарч сул тал олдохгүй байх тохиолдолд ихэвчлэн хэрэглэгддэг. Энэ халдлагын гол санаа нь зөв нууц үгийг олтол боломжит бүх түлхүүр юмуу нууц үгийг системтэйгээр шалгах юм. Хамгийн муу тохиолдолд боломжит бүх нөхцөлийг туршиж үзэж болно. Нууц үг таах явцад богино хэмжээтэй нууц үгийн хувьд brute-force-ыг ашиглахад хугацаа их шаарддагүй, харин урт хэмжээтэй нууц үг таахад Dictionary attack гэх мэт илүү нарийн ажиллагаатай хугацаа бага шаардах халдлагыг ашигладаг. Орчин үеийн криптосистемд нууц үгийг таахад түлхүүрийн урт нь brute-force хийгдэх практик боломжийг тодорхойлдог.

2.5.2 Hybrid халдлага гэж юу вэ?

Энэ халдлага нь хосолсон байдлаар ажилладаг бөгөөд яг толь бичгийн халдлагатай ижил ажиллагаатай ба ялгаа нь гэвэл зарим нэг тоо болон тэмдэгтүүдийг толь бичигтээ нэмсэн байдаг.

2.5.3 Syllable халдлага гэж юу вэ?

Энэ халдлага нь brute-force болон толь бичгийн халдлагыг хослуулсан байдлаар ажилладаг. Мөн Hybrid халдлагатай төстэй бөгөөд ялгаа нь маш нарийн байдлаар оршдог. Hybrid нь толь бичиг дээр суурилсан бол энэ нь үгүй юм.

2.5.4 Rule-based халдлага гэж юу вэ?

Энэ халдлага нь тухайн хэрэглэгч нууц үгийг тохируулахдаа ямар дүрмийг баримталж буйг халдагч мэдсэний дараа нууц үгийг олох арга дээрээ анхаарлаа хандуулж ажилладаг төрлийн халдлага юм.

2.5.5 Rainbow-table халдлага гэж юу вэ?

Нууц үгийг мөн таах зарчмаар ажилладаг халдлага бөгөөд таах оролдлого хийсэн нууц үг бүхэн нь нууц үгийг хашлахад ашигласан алгоритмтай яг ижил алгоритмаар encrypt-лэгдсэн байдаг. Дараа нь тэр хаш утгаа жинхэнэ нууц үгийн хаштай харьцуулж тулгалт хийж ижил утга гарч ирэх хүртэл шалгах зарчмаар ажиллана. Rainbow-table нь халдлагын үйл явц болон хурдыг сайжруулсан халдлага бөгөөд өөрийн үүсгэсэн хүснэгт дээрээ тэрбум

орчим нууц үгийн хашын урьдчилан тооцоолж хадгалсан байдаг. Энэ хүснэгтийг үүсгэхэд их хугацаа ордог боловч нэг удаа үүсгэчихээд дараа нь дахин ашиглах боломжтой юм. Ингэснээр тухайн хүснэгт дундаас хаш утгыг хайх нь жинхэнэ хаш утгыг тус бүрд нь тооцоолхоос илүү хурдан, цаг хэмнэх юм.

2.6 Халдлага хийх боломжтой програм хангамжууд

Энэхүү халдлагуудыг хийх боломжтой програм хангамжуудаас дурьдвал:

- Cain and Abel
- Crack
- Aircrack-ng
- John the Ripper
- L0pthCrack
- Metasploit Project
- Ophcrack

2.6.1 Cain and Abel

Cain and Abel нь Microsoft Windows-д зориулсан нууц үг сэргээх хэрэгсэл м. Сүлжээний пакетыг шинжлэх замаар олон төрлийн нууц үгийг сэргээх мөн толь бичгийн халдлага, brute-force, болон cryptoanalysis зэрэг халдлагыг хийж янз бүрийн нууц үгийн хашийг эвдэх боломжтой хэрэгсэл юм. Cryptoanalysis халдлага нь Cain and Abel-ээс хамааралтай winrtgen.exe гэх програмаас rainbow table-ээ үүсгэж халддаг.

2.6.2 Crack

Crack нь систем администраторуудад зориулж загварчлагдсан хэрэгсэл бөгөөд аль хэрэглэгч толь бичгийн халдлагад өртөх магадлалтай сул нууц үгийг ашиглаж буйг илрүүлэх зорилготой хэрэгсэл юм. Мөн Unix системийн хамгийн анхны бие даасан байдалтай нууц үг эвдэгч бөгөөд мөн анхны програмчлагдсан толь бичиг үүсгэгч юм. Энэ хэрэгсэл нь анх 1990 онд Wales Aberystwyth-ын их сургуулийн Unix систем администратор Alec Muffett-ээс гаралтай.

2.6.3 Aircrack-ng

Aircrack гэдэг нь өөртөө Detector буюу илрүүлэгчийн цуглуулга агуулсан сүлжээний програм хангамж мөн пакет шинжлэгч юм. WEP болон WPA(1,2) тайлах мөн 802.11 утасгүй сүлжээний анализ хийдэг хэрэгсэл юм. Энэ хэрэгслээр утасгүй сүлжээний нууц үгийг олох боломжтой бөгөөд ингэхдээ ихэвчлэн толь бичгийн халдлагыг ашигладаг.

2.6.4 John the Ripper

John the Ripper нь хуучны бөгөөд хамгийн алдартай нууц үг эвддэг хэрэгслүүдийн нэг юм. Хоёр өөр хувилбартай бөгөөд эхнийх нь Үнэгүй open-source дараагийх нь pro хувилбар байдаг. Энэ хэрэгсэл нь командын горимд суурилсан бөгөөд ямар GUI(Graphic User Interface) байхгүй. Open-source хувилбар дээр маш олон шинэчлэлт, нөхөлт хийгдэж байсан бөгөөд олон төрлийн шинж чанар ба encrypt хийх алгоритмуудыг оруулж өгсөн. Мөн олон янзын эвдэх төлөв(mode)-үүдийг нэмсэн. Үүнд:

- Wordlist mode
- Single crack mode
- Incremental mode
- External mode

John the Ripper нь секундэд дунджаар 800,000 нууц үгийг дамжуулах боломжтой бөгөөд энэ нь CPU-ны маш жижиг хэсэгт л ажилладаг.

2.6.5 L0phtCrack

Энэ хэрэгсэл нь Peiter C.Zatko-ын зохиосон нууц үг шалгаж мөн сэргээдэг application юм. Энэ нь нууц үгний чадлыг шалгадаг мөн зарим тохиолдолд Microsoft Windows-ын мартсан нууц үгийг толь бичиг, brute-force, hybrid болон rainbow-table халдлагуудыг ашиглан сэргээх боломжтой. Хүртээмжтэй байдал нь өндөр харин үнийн хувьд хямд байдаг тул өргөнөөр ашиглагддаг. L0phtCrack нь 6 өөр төрлийн нууц үгийн хашыг дэмжиж ажилладаг. Үүнд:

- The LM Hash (for Windows)
- The NTLM Hash (for Windows)
- The LM Challange Response
- The NTKM Challange Response
- Unix MD5-encoded password files
- Unix DES-encoded password files

2.6.6 Ophcrack

Ophcrack нь үнэгүй open source бөгөөд rainbow table дээрхи LM хашыг ашиглан Windows-ын нэвтрэх нууц үгийг эвддэг програм юм. Энэ програм нь хаш утгын олон төрлийн форматыг оруулж ирэх чадварыг агуулсан бөгөөд Windows-ын SAM (Security Accounts Manager) файлуудаас шууд dumping хийх боломжтой.

2.7 Толь бичгийн халдлагаас сэргийлэх нь

Толь бичгийн халдлагаас сэргийлэх хамгийн хялбар арга бол нууц үгээ илүү хүчтэй журмаар тохируулах явдал юм. Толь бичгийн дотор ихэвчлэн сул нууц үгүүдийг оруулж ирсэн байдаг. Нууц үгний хэмжээ маш чухал: урт нууц үг оруулах нь хүчээр олоход хэцүү болгоно. Ингэхдээ:

- 7-оос бага тэмдэгтээр оруулахгүй байх
- Том жижиг үсэг хольсон байх
- Тоо оруулсан байх
- Тусгай тэмдэгт оруулах

Мөн энэхүү халдлагаас сэргийлэх 2 түгээмэл арга байдаг. **1. Delayed Response**
Нэвтрэх нэр болон нууц үгийг хослуулж ашиглаж серверээс ирэх хариуг бага зэргийн хоцрогдолтой ирүүлэх. (1 Секундэд нэгээс илүү хариу хүлээн авах боломжгүй гэх мэт) Энэ нь халдлагч этгээдийг тухайн нэг агшинд олон нууц үг оруулж шалгахаас урьдчилан сэргийлнэ. **Account locking**
Тухайн хэрэглэгчийн хаяг нь олон удаа амжилтгүй нэвтрэх оролдлого хийхэд түгжигддэг байх шаардлагатай. (Жишээлбэл хэрэглэгчийн хаяг 5 удаа амжилтгүй оролдлого хийвэл 1 цагийн турш ахин нэвтрэх оролдлого хийгддэгүй байхаар тохируулах) Энэ нь мөн л олон нууц үг шалгахаас сэргийлнэ. Дээрхи арга хэмжээнүүд нь нэг компьютерийн орчинд ба хэрэглэгч нэвтрэхдээ физик байдлаар холбогдсон гар ашигладаг байх нөхцөлд сайн ажиллагаатай байна. Эдгээр аргуудыг сүлжээний орчинд хэрэглэх нь маш чухал.

2.7.1 Delayed Response-ын сул тал

Нэвтрэх систем нь маш олон хэрэглэгчийн бүртгэлийн хаягтай байдаг бөгөөд сүлжээн дээр нэвтрэх оролдлого хийх нь халдагчид том боломжийг олгоно. (Халдагч сүлжээн дээрхи урсгалыг чагнах тухай биш, харин тэд сүлжээнд

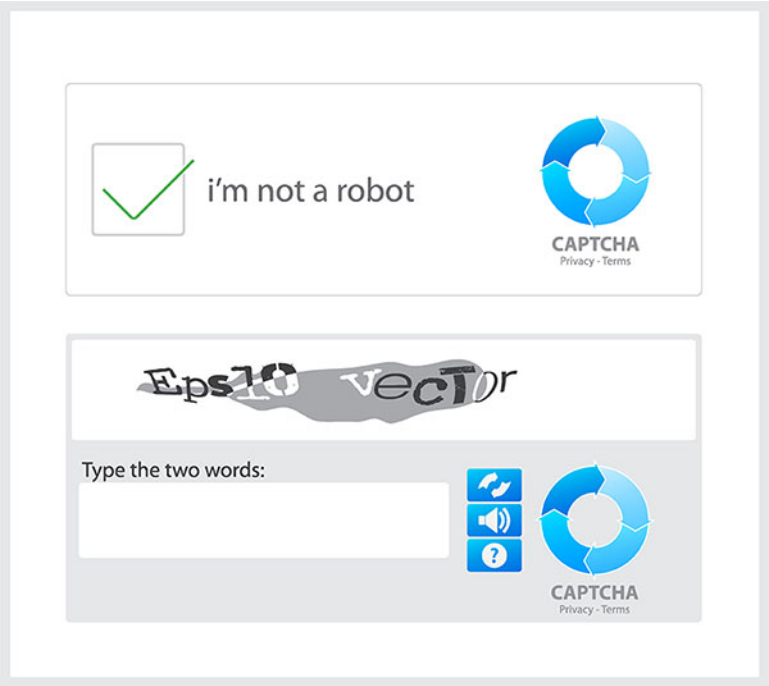
холбогдож сервер рүү зөвшөөрөлтэй хэрэглэгч мэт нэвтрэхийг оролдох болно.) Халдагч этгээд нь ямар зөвхөн нэг хүний хаягыг онилохоос илүүтэй системд байгаа ямарч хамаагүй бүртгэлийн хаягыг эвдэх сонирхолтой байдаг ба маш олон оролдлогыг нэгэн зэрэг гүйцэтгэх боломжтой байдаг. Хэрэглэгчийн нэвтрэх үйл явц нь системээр удирдагддаг тул энэ нь мөн л параллелиар нэгэн зэрэг нэвтрэх оролдлогыг ч удирдах боломжтой. Жишээлбэл халдагч нь 10 мСек тутамд нэвтрэх оролдлоыг илгээх ба сервер нэвтрэх оролдлогод хэр удаан хариу өгөхөөс үл хамааран секунд тутамд 100 хүртэлх оролдлогыг нэвтрүүлэх боломжтой.

2.7.2 Account locking-ын сул тал

Энэ хамгаалах арга нь мөн өөр төрлийн эрсдэлийг дагуулдаг. Хэрэглэгчдийн эсрэг DOS буюу Denail of Service халдлагыг хэрэгжүүлэх боломжийг нээж өгдөг. Энэ халдлага нь хэрэглэгчийн бүртгэлээр санаатай буруу нууц үгийг хэд хэдэн удаа оруулж тухайн хаягыг цоожлуулах боломжтой. Мөн DOS халдлагын төрөл буюу Distributed Denial of Service(dDoS)-ыг өөр нэгэн хэлбэрээр гүйцэтгэх боломжтой. Халдлагч этгээд нь вебийн орчинд нууцаар агент(agent)-уудыг байршуулах бөгөөд бүх агентууд тодорхой нэг агшинд тухайн сервер лүү санамсаргүй нууц үг ашиглан (эсвэл толь бичгийн халдлага ашиглан) нэвтрэхийг оролдох юм. Энэ халдлага нь халдсан серверийн хэрэглэгчийн хаягийн ихээхэн хэсгийг блок хийдэг байна. Энэ эрсдэлийг өөрөөр авч үзвэл хэрвээ хэрэглэгч өөрөө нууц үгээ буруу бичиж цоожлуулсан тохиолдолд үйлчилгээ үзүүлэгч байгуулагатай холбогдох шаардлага гарна. (Хэрвээ үйлчилгээ үзүүлэгч байгууллага нь автоматаар цоожийг тайлах эсвэл зөвхөн зөвшөөрөлтэй хэрэглэгч мэдэх хувийн асуулт зэрэг механизмыг суулгаж өгөөгүй бол) Энэ тохиолдолд санхүү болон цаг хугацааны хувьд хохиролтой байх болно.

2.7.3 Tools-Reverse Turing Tests

Толь бичгийн халдлагаас сэргийлэх өөр нэгэн арга нь хэрэгсэл ашиглах явдал байж болно. Энэ нь хэрэглэгч болон компьютерын програм 2-ыг хооронд нь ялгаж адилтган таних процесс юм. Энэ арга нь хэрэглэгч давахад амархан харин автоматжуулсан програмын хувьд хэцүү шалгалт байх ёстой. Энэ аргыг анх M. Noar гэх хүн санаачилсан бөгөөд Reverse Turing Tests(RTTs) хэмээн нэрлэсан байдаг ба өөрөөр энэ шалгах процессыг CAPTCHAs гэж нэрлэдэг.



Зураг 2.3: Captcha

RTTs нь дараах шаардлагыг хангасан байх шаардлагатай.

- **Автоматжуулсан үүсгэх процесс:** Энэ нь автоматжуулсан аргаар маш олон тохиолдлыг үүсгэхэд хялбар байх шаардлагатай.
- **Хүний хувьд хялбар:** Үүсгэсэн тест нь хүмүүс тэнцэхэд хялбар байх шаардлагатай.
- **Машины хувьд хүнд:** Автоматжуулсан тухайн програм нь гараас утга орж ирсэний дараа хэрэглэгчтэй шууд харьцаж чадахгүй. Тэр програм нь оруулах боломж нь 2 төрлийх байж болно.

  1 Энэ нь RTTs-ыг үүсгэх боломжтой алгоритмыг оруулж өгсөн байх боломжтой. Ингэснээр RTTs-г өөр дээрээ үүсгэж шийдэлийг олох

  2 Аюулгүй байдлын талаархи муу ойлголттой бол бол RTT-ын тухайн үеийн тохиолдлуудын шийдэлүүдийг агуулсан m жишээг хүлээн авна.

- **Хариултыг зөв таах магадлал бага:** Бид тестын хариуг зөв таах магадлалыг маш бага байхаар тооцоолох шаардлагатай. Жишээлбэл тестээр нэг хүний зургыг өгөх бөгөөд энэ хүнийг эрэгтэй эсвэл эмэгтэй эсэхийг заах ба зөв таах магадлал дор хаяж 50 хувь байна. Өөр нэг шаардлагатай зүйл бол санамсаргүйгээр 6 ширхэг string өгөгдөх ба энийг OCR (Optical Character Recognitions) програмуудаар decode хийхэд хэцүү бөгөөд хэрэглэгчээс string-ын төрлийг асууна.

2.8 Веб хөтчийн тухай

Вэб хуудсыг үзэхэд зориулагдсан програмыг Вэб Хөтөч хэмээн нэрлэдэг. Цахим хөтөч буюу Вэб хөтөч(Web browser) нь интернет болон дотоод сүлжээний орчинд цахим хуудсан дахь бичиг, зураг, дуу, дүрс болон бусад мэдээлэлийг үзүүлэхэд хэрэглэгддэг програм хангамж юм. Вэб хуудсан дахь текст болон зураг нь өөртөө бусад вэб хуудасруу дамжих зориулалт бүхий гипер холбоосыг (hyperlink) агуулах боломжтой, ингэснээр богино хугацаанд олон олон вэб хуудас руу хандах боломжийг олгодог. Мэдээллийн эх үүсвэр нь uniform resource identier (URI)-р ялгагдах вэб хуудас, зураг, дуу, видео зэрэг ямар ч хэлбэртэй байж бол Hyperlink-үүд нь вэб хөтчөөр мэдээллийг хялбархан олох боломж олгодог. Хэдийгээр вэб хөтчийн гол үүрэг нь world wide web-д хандах боловч үүнийг ашиглан хувийн сүлжээ, төхөөрөмж, файл системрүү хандаж болдог. Хамгийн их хэрэглэгддэг вэб хөтчүүд нь Firefox, Google Chrome, Internet explorer, Opera, болон Safari.

Анхны вэб хөтөчийг 1990 онд Тим Баннэрс Лий (Tim Banners-Lee) бүтээсэн. Баннэрс Лий нь вэбийн хөгжүүлэлтийг хянадаг World Wide Web Consortium (W3C) – ийн захирал, мөн World Wide Web байгууллагын үүсгэн байгуулагч юм. World Wide Web гэх түүний хөтөч хожим Nexus гэсэн нэртэй болсон. Анхны график хэрэглэгчийн интерфэйстэй вэб хөтөч нь Erwise байв. Erwise-ийн хөгжүүлэлтийг эхлүүлсэн хүн нь Робэрт Кэллио (Robert Cailliau).

1993 онд Марк Андэрсэн (Marc Andreessen) -ы Mosaic дэлхийн анхний алдартай хөтөч нээлтээ хийснээр хөтчийн програмууд шинэ шатанд гарсан. Mosaic нь World Wide Web системийг энгийн хэрэглэгчидэд ашиглахад маш амар болгосон. Андэрсэний хөтөч 1990 - д онд тэсрэлт болсон. Харин Microsoft 1995 онд Internet Explorer – ийг танилцуулсанч Mosaic – д хүчтэй шахуулсанаар анхны вэб хөтчийн дайныг эхлүүлсэн. Windows – н иж бүрдэлд орсноор Internet Explorer вэб хөтчийн худалдаан дахь давуу талыг авч, 2002 он гэхэд хэрэглэгчидийн 95 хувь нь Internet Explorer – ийг хэргэлдэг болсон. 1996онд Opera гарсанч хэзээч олон нийтэд тархсан хэрэглээнд хүрч байгаагүй. 2012 оны 2-р сарын байдлаар нийт вэб хөтөч хэрэглэгчидийн 2-с доош хувьд л хүрсэн. 1998 онд Netscape (хожим Mozilla Foundation болсон) байгуулагдаж нээлттэй эхийн вэб програмыг бүтээж эхэлсэн. Энэ хөтөч эцэст нь Firefox болж хөгжсөн. 2011 оны 8 р сарын байдлаар хэрэглэгчидийн 28 хувь нь Firefox -ийг хэрэглэж байна. Apple – ийн Safari анх 2003 оны 1 - р сард анхны туршилтын хувилбараа гаргасан. 2008 оны 9-р сард вэб хөтчийн зах зээлд шинэ оролцогч нээлтээ хийсэн нь Chrome хөтөч.

2.8.1 Google Chrome

Google Chrome нь Google - ийн хөгжүүлсэн үнэгүй програм бүхий вэб хөтөч юм. Энэ хөтөч iOS - д гаргасан хувилбараас бусад хувилбар 27 хүртлээ WebKit бүтцэт механизмийг ашигладаг байсан бол хувилбар 28 - с эхлэн WebKit болон салаалсан Blink механизмийг ашиглаж эхэлсэн. Анхны Microsoft Windows -д зориулсан бэта хувилбар нь 2008 оны 9 - р сарын 2 - нд гарсан бол, нээлттэй хувилбар нь 2008 оны 12 - р сарын 11 - нд гарсан. 2015 оны 12 - р сарын байдлаар дэлхийн нийт суурин компютэр дэх вэб хөтчийн 58 хувь нь Google Chrome байгааг StatCounter(вэб урсгалын шинжилгээ хийдэг хэрэгсэл) - ийн тооцоогоор гаргасан. Мөн Chrome хөтөч ухаалаг утасуудад маш алдартай бөгөөд бүх платформуудыг нэгтгэсэн байдлаар 45 хувьд нь хэрэглэгдэж байна. Chrome хөтөч дэмжих платформуудын жагсаалт :

- Windows: XP Service Pack 2 болон 3 / Server 2003 Service Pack 1 эсвэл түүнээс дээш / Vista / Server 2008 / 7 / 8 / Server 2012 / 8.1 / 10 / Server 2016
    1. Windows XP болон Vista дахь хөгжүүлэлт 2016 оны 4 -р сард дууссан.
- OS X: 10.6 эсвэл түүнээс дээш
    1. 32 битийн Mac дахь хөгжүүлэлт 2014 оны 10 -р сард дууссан.
    2. OS X 10.6, 10.7 болон 10.8 дахь хөгжүүлэлт 2016 оны 4 -р сард дууссан.
    3. 32-bit Intel processors дахь хөгжүүлэлт 2016 оны 3 - р сард дууссан.
- Android 4.1 эсвэл түүнээс дээш
- iOS 9.0 эсвэл түүнээс дээш

2.8.2 Internet Explorer

Анх 1995 оны 8 сарын 16-нд Thomas Reardon (Microsoft-н хөгжүүлэгч) Windowsийн үйлдлийн системд зориулан зохион бүтээсэн. C++ хэл дээр бичигдсэн. Trident (layout engine), Chakra (JScript engine), EdgeHTML (Зөвхөн Windows 10 үйлдлийн системд) гэсэн системүүдтэй. Энэхүү хөтчийг зөвхөн Windows үйлдлийн систем л дэмждэг. Windows 8.1 шинэчлэлт хийснээр Internet Explorer 11 онцлог болсон. Зөвхөн үүнд л Media Source Extensions, Encrypted Media Extentions, WebCrypto нэмэгдсэн.

2.8.3 Mozilla Firefox

Firefox нь Mozilla Corporation-ий гаргасан free and open source үнэгүй нээлттэй эхийн вэб хөтөч юм. Mozilla Foundation хөгжүүлдэг. Windows, OS X мөн Linux, гар утасны Android, Firefox OS-д дэмжиж ажиллах чадвартай. 2002 оны 9 сард анх олон нийтэд зарлагдсан. Firefox-ийн стандартуудад HTML4, HMTL5, XML, XHTML, MathML, SVG 1.1, CSS (extensions), ECMAScript(JavaScript), DOM, XSLT, XPath мөн зургийн APNG багтдаг.

2.8.4 Microsoft Edge

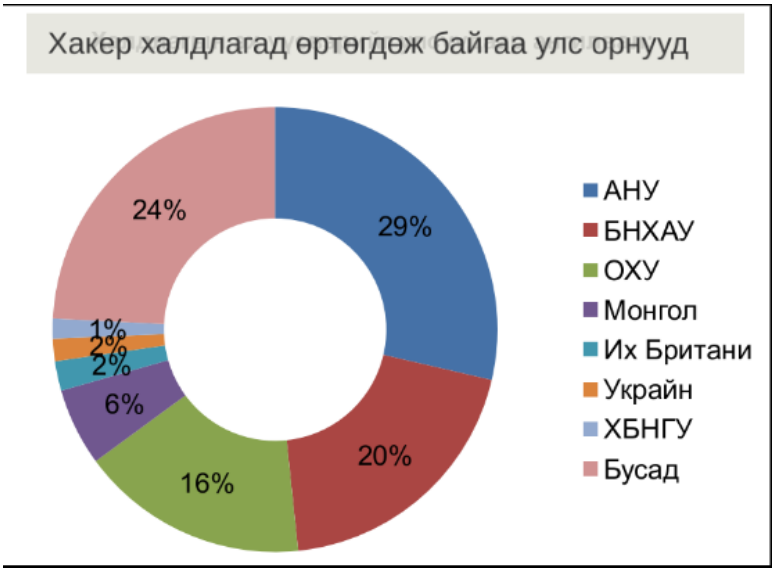
Microsoft Edge нь хамгийн залуу хөтөч бөгөөд Windows 10 үйлдлийн системийг суух үед цуг суудаг. Internet Explorer-ийн хамгийн сүүлийн хувилбар гэхэд ч болно.

БҮЛЭГ 3

Судалгааны хэсэг

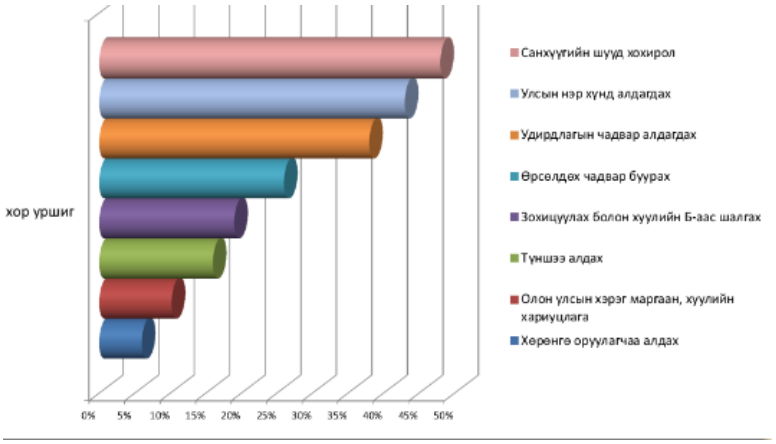
3.1 Халдлага

Халдлага гэдэг нь ерөнхийдөө өөрийн мэдлэгийг ашиглан интернет сүлжээгээр бусдын компьютер руу хууль бусаар нэвтэрч мэдээллийг устгах, өөрчлөх, хулгайлах үйл ажиллагаа юм. 2013 оны байдлаар халдлагад өртөж буй улс орнуудын графикыг гаргавал:



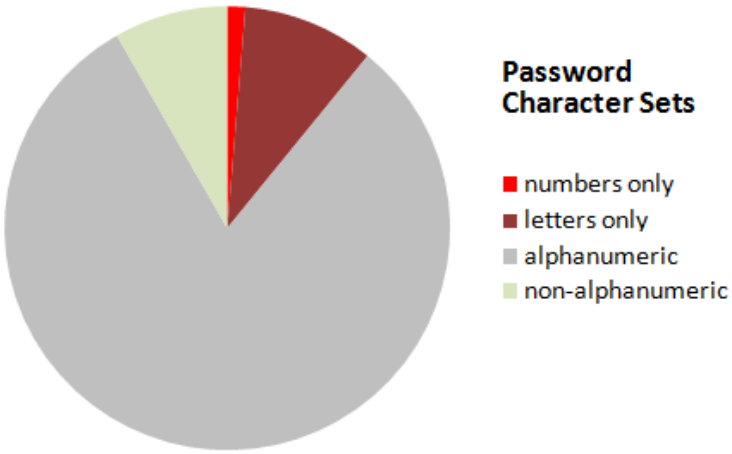
Зураг 3.1: Country Chart

Мөн Монгол улсын интернэт хэрэглэгчидийн тоо 650 мянга, үүн дээр нэмэгдээд 3G ашигладаг 350 мянган хүн байдаг байна. Тохиолдож буй нийт халдлагын 30-40 хувь нь төрийн байгууллага руу хандсан байдаг ба нэг өдөрт төрийн байгууллага руу хандсан халдлагын хэмжээ нь хамгийн багадаа 50-60 удаа, хамгийн ихдээ 2000 удаа гэж тогтоогдсон байна. Халдлагад өртсөнөөр улс оронд учрах эрсдэл:



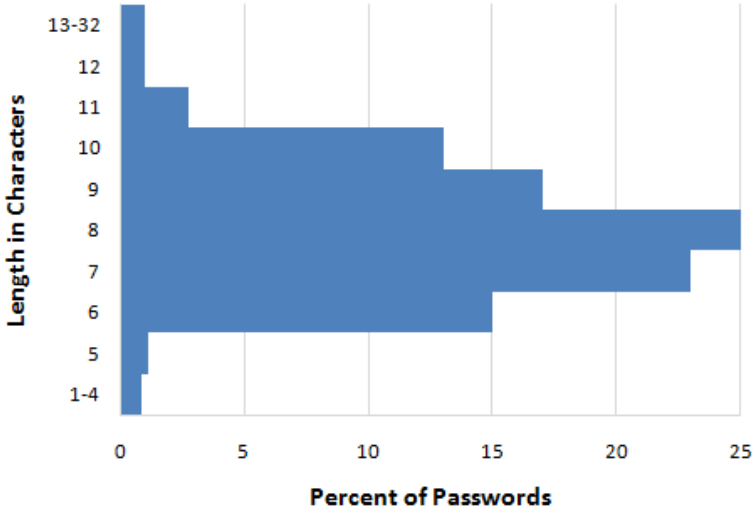
Зураг 3.2: Учрах эрсдэл

3.2 Нууц үгний сонголт



Зураг 3.3: Password Characters

2006 онд авсан судалгаагаар нийт хэрэглэгчдийн дийлэнхи хувь нь нууц үгээ дан үсгээр ашигладаг нь тогтоогдсон харин дан тоогоор нууц үгээ оруулсан хэрэглэгчид хамгийн бага хувийг эзэлдэг болохыг дээрхи зурагнаас харж болно.



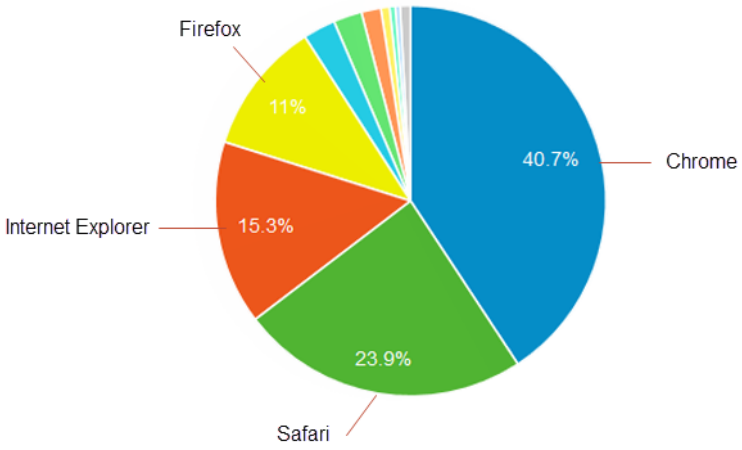
Зураг 3.4: Password Length

Харин нууц үгийн нийт уртын хувьд хамгийн их хувийг 8 тэмдэгт эзэлдэг ба дараагаар нь 7 тэмдэгт байдгыг харуулсан байна.

3.3 Веб хөтөчийн тухай судалгаа

Вэб хөтөч (web browser) нь интернэтээр аялах боломжийг бидэнд олгодог. URL дээр өөрийн үзэхийг хүссэн вэбийн хаягийг бичихэд браузер серверт үзэх хүсэлт тавина. Хэрэв тухайн хуудас байвал вэб сервер түүнийг браузер лүү илгээдэг. Үүнд IP хаяг, Вэб браузерын дэлгэрэнгүй мэдээлэл, өмнө нь орсон эсэх мэдээллүүд (cookie) гэх мэт.

2015 оны 3 сард гаргасан судалгаагаар хүмүүсийн аль веб хөтөчийг илүү ашигладаг болохыг тогтоожээ.



Зураг 3.5: Browser

3.4 Нэмэлт буюу Extension гэж юу вэ?

Хамгийн анх Internet Explorer нь нэмэлтүүдийг 1999 онд гарсан 5-р хувилбараасаа эхлэн дэмжиж эхэлжээ. Түүний дараагаар Firefox нь 2004 оноос хойшоо, Opera нь 10-р хувилбараасаа буюу 2009 оноос хойшоо, Google Chrome нь 2010 онд гарсан 4-р хувилбараасаа хойшоо, Safari нь 2010 онд гарсан 5-р хувилбараасаа, хамгийн сүүлд Microsoft Edge нь 2016 оны 3 сараас эхлэн нэмэлтүүдийг тус тус дэмждэг болжээ. Вэб хөтчийн нэмэлт гэдэг нь ямар нэг байдлаар вэб хөтчийн үйл ажиллагааг өргөжүүлэх зорилготой залгаас програм (plug-in) юм. Зарим нэмэлт нь HTML, JavaScript, CSS гэх мэт вэб технологиудыг ашигладаг. Хөтөчийн нэмэлтүүд нь вэб хуудас дахь контентүүдад шууд нөлөө үзүүлэхгүйгээр хэрэглэгчийн интерфэйст өөрчлөлт хийдэг.

1999 онд Internet Explorer – ийн version 5-с эхлэн нэмэлтүүдийг дэмжиж эхэлсэн. Firefox анх 2004 онд гарснаасаа хойш нэмэлтүүдийг дэмжиж байгаа. Google Chrome ийн хувьд 2010 онд version4–өөсөө эхлэн нэмэлтүүдийг дэмжиж байгаа. Нэмэлтүүдийн синтаксууд хөтчөөс хөтчийн хооронд маш ялгаатай байдаг. Нэг хөтөч дээр ажиллах нэмэлт нөгөө хөтчид ихэнхидээ ажилдаггүй. Харин нэмэлтийг хөтөчид суулгахын хувьд ихэнхи хөтчүүд өөрийн онлайн нэмэлт татах дэлгүүртэй (store) байдаг.

Үйл ажиллагааны хувьд маш олон төрлийн зорилготой нэмэлтүүд байдаг. Ерөнхийд нь ангилж үзвэл:

- Тоноглолын зурвас (Toolbars): Ихэнхи томоохон хөтчүүд граффик хэрэглэгчийн интерфэйс (GUI) болон үйл ажиллагаагаа өргөтгөхийн тулд хөтчийн toolbar – г эрхлэн хөгжүүлдэг.
- Бусад залгаас програм (plug-in): Програм програмчлах интерфэйс (APIs) – ийг ажигласнаар гуравдагч тал хөтчид нэмэлт бүтээх боломжтой болдог.
- Хувийн нууц: Ихэнхи хөтчүүдэд байдаг хувийн үзэлтийн боломжуудаас илүү цаадахь хувийн нууцыг хамгаалах хөтчийн нэмэлт. Хувийн нууцтай холбоотой ихэнхи хөтчийн нэмэлтүүд дараах төрөлд хамаарагддаг. Үүнд гуравдагч этгээд таний үйлдэл бүрийг мөшгихөөс сэргийлэх нэмэлт, сурталчилгаа болон скрипт хориглох нэмэлт мөн хүчин чадал бага шаардах хамгаалалтын хэрэгсэлүүд.

Хөтчийн нэмэлтийн хөгжүүлэлт нь тухайлсан хөтчид зориулагдаж бүтээгддэг. Хөтөч бүр өөрийн гэсэн нэмэлт бүтээх архитектур болон APIs – тай байдаг бөгөөд энэ нь нэмэлт бүрт өөр өөр код болон чадвар шаарддаг. Одоо үед хөгжүүлэлтийн ерөнхий бүтэц (development framework) гэж байдаг болсон. Энэ нь хөгжүүлэгч зөвхөн ганц код болон ганц API ашиглан олон хөтчид ажиллах нэмэлт бүтээх боломж олгосон. Нэмэлт бүтээгч (Extension Maker) гэдэг нь олон хөтчийн нэмэлт хөгжүүлэх бас нэг сонирхолтой багаж юм. Үүнийг ашиглахад ямарч код бичих шаардлагагүй бэлэн блокуудыг угсран нэмэлт хийх боломжтой.

3.4.1 Нэмэлт юу хийдэг вэ?

Хөтөчийн нэмэлт нь ихэвчлэн дараахи зориулалтуудаар бүтээгдсэн байдаг. Үүнд:

- Хэрэглэгчийн интерфейсыг сайжруулах
- Хүртээмжтэй байдалыг сайжруулах

- Аюулгүй байдлыг сайжруулах
- Зар сурталчилгааг блоклох
- Интернетэд холбогдоход илүү хялбар болгох

Үүнээс гадна өөр олон төрлийн нэмэлтүүд байдаг ба хамгийн түгээмэл нь хэрэглэгчийн интерфейс загварыг өөрчилдөг түүлбар(toolbar) юм.

3.5 Ашиглагдах хэлнүүдийн судалгаа

Бид энэхүү нэмэлтийг бүтээхийн тулд веб бүтээхэд ашиглагддаг хэлүүд болох HTML,CSS болон Javascript гэх хэлүүдийг ашиглах бөгөөд энэхүү програмчлалын хэлүүдийн тухай товч танилцуулгыг орууллаа.

3.5.1 HTML

HTML гэдэг нь Hyper Text Markup Language гэсэн үгийн товчлол. Энэ нь вэб хуудас харуулах заавар бичдэг кодчлол юм. HTML файлыг энгийн текст боловсруулах програм ашиглан үүсгэж болох бөгөөд htm эсвэл html гэсэн өргөтгөлтэй байна. Уг хэлийг Tim Berners-Lee 1991 онд шинжлэх ухааны бичиг баримтыг зохион байгуулах, өөр өөр платформруу дамжуулах зорилгоор үүсгэжээ. HTML хэл нь script хэл бөгөөд ямар нэг хөрвүүлэлт шаарддаггүй, дурын текст боловсруулах програм дээр бичиж болдог бөгөөд Hypertext Transfer Protocol (HTTP) –г ашигладаг. HTML - н комманд болгон нь их багын хос тэмдэгтийн хооронд байдгаараа бусад хэлээс онцлогтой.

Файлын эхний кодчлол нь <html> байна. Энэ кодчлол Вэб хуудас харуулах заавар эхэлж байгааг заана. Файлын хамгийн сүүлийн кодчлол нь </html> байна. Энэ нь хуудас харуулах заавар дуусч байгааг илэрхийлнэ. <head> </head> гэсэн кодчлолын хооронд бичигдсэн мэдээлэл нь хуудасны толгойн хэсгийн мэдээллийг агуулах ба энэ нь Вэб хуудас харуулах хэрэгслээр харагдахгүй. <title> хэсэгт хуудасны гарчгийг бичнэ. Энэ гарчиг цонхны гарчгийн хэсэгт гарна. <body> кодчлолын хооронд бичигдсэн мэдээлэл Вэб хуудас харуулагч хэрэгслээр харагдана. ба кодчлолын хооронд бичигдсэн текст тодоор бичигдэнэ.

3.5.2 CSS

CSS гэдэг нь Cascading Style Sheets гэдэг үгийн товчлол бөгөөд хэлбэр, дизайн гэж ойлгож болох юм. CSS нь HTML кодчлолын элэмент тагуудийг хэрхэн үзүүлэх форматлахыг тодорхойлдог. Өөрөөр хэлбэл таны вэбийн өнгө

үзэмжийн, харагдах байдлыг сайжруулдаг. CSS нь .css гэсэн өргөтгөлтэйгээр хадгалагддаг. CSS ашиглахад давуу тал нь гэвэл: Та нэг элемэнтийн өнгийг, эсвэл форматыг солихын тулд бүх хэсэгтээ өөрчлөлт хийх шаардалагагүй, харин CSS бичсэн хэсэгтээ солиход л бүх элэмэнтүүд хэвжүүлэгддэг. Энэ нь вэб мастеруудын ажлыг маш их хөнгөвчилдөг. HTML нь зөвхөн энэ элемент гэдгийг тодорхойлдог . ж.нь : <p> гэх мэт. Энэ нь зөвхөн элемэнтийг үүсгэдэг болохоос ямар хэмжээтэй, яаж харагдах гэх зэргийг тодорхойлж чаддаггүй. Үүнийг CSS ашиглан шийдэж чадна. CSS-ийг харуулж чадах web browser - ууд нь төрөл бүр байдаг. Өргөн хэрэглэгддэг Internet Explorer, Netscape Navigator, программууд нь зарим тохиолдолд хэлбэрийн хуудсуудыг харуулж чадахгүй. IE 4.0 дээших хувилбарууд NN 4.0 дээшхи хувилбарууд нь хэлбэрийг харуулж чадах болсон. Хэлбэрүүд нь ихэвчлэн вэб хуудасны гадна өөр файлд хадгалагддаг. Эсвэл вэб хуудасандаа хийсэн ч болно. Гадаад хэлбэрийн хуудасны ашигтай тал нь нэг хэлбэрийг өөрчлөхийн тулд нэг л файлд өөрчлөлт оруулахад бүх хуудсанд хэвжүүлэгдэнэ гэсэн үг.

3.5.3 Javascript

JavaScript бол интернет дэх хамгийн түгээмэл тархсан скрипт хэл бөгөөд Internet Explorer, Firefox, Opera гэх мэт ихэнх вэб хөтөчүүд дэмжин ажилладаг. Вэб дизайн хийх, сайжруулах, бөглэх форм зохиох, хөтөч ялгах, cookie үүсгэх, төрөл бүрийн чимэглэл хийх, анимаци дээр ажиллах гэх мэт олон давуу талтай. Java болон JavaScript хоёр нь концепци болон дизайнаар огт өөр програмын хэлнүүд юм. Netscape хөтөч дээр 1995 оны 9 сард LiveScript beta гэсэн нэрээр анх гарч ирсэн билээ. Энэ нь HTML дотор бяцхан хэмжээний script код шигтгэж хэрэглэгчрүү явуулснаар хэрэглэгчийн хөтөч HTML-ээ өрж байхдаа зэрэг тэр script-ийг копайлдаж ажиллуулах юм. HTML хуудсын элемент бүрийг унших, шинэ элемент үүсгэх, хүссэн элементийнхээ агуулгыг өөрчлөхөөс гадна устгах хүртэл боломжоор бүрэн хангахын тулд анхнаасаа асинхрон ажиллагааг шаардаж байжээ. Netscape нь LiveScript-н нэрийг програм хангамжийн ертөнцөд дуулиан дэгдээж байсан Java хэлний нэрийг маркетингийн хэрэгсэл болгон JavaScript гэдэг нэрийг өгсөн. Энэ нэрээр одоог хүртэл байгаа билээ.

Бичиглэл ба syntax

Анх харахад бичиглэл буюу syntax-аараа C, Java-гаас ялгараад байх зүйлгүй харагддаг нь Java-гийн script хувилбар гэж андуурахад хүргэдэг биз, нэр нь

хүртэл. C, Java програм дээр бичдэг шиг жижигхэн арифметикийн үйлдлүүдийг ажиллах болвол JavaScript дээр яг адилхан бичиглэлээр бичигдэнэ, үүн дээр төөрөөд байх зүйл байдаггүй.

Давуу талууд

Түгээмэл хэрэглэгддэг хэлүүдэд байдаггүй хамгийн том давуу талуудынх нь нэг нь nonblock буюу асинхрон ажиллагаатай. Синхрон, асинхрон гэх мэт үгнүүдийг бид мэддэг ч яг програмчлал дээр яаж тусдагийг мэдэх нь маш чухал.

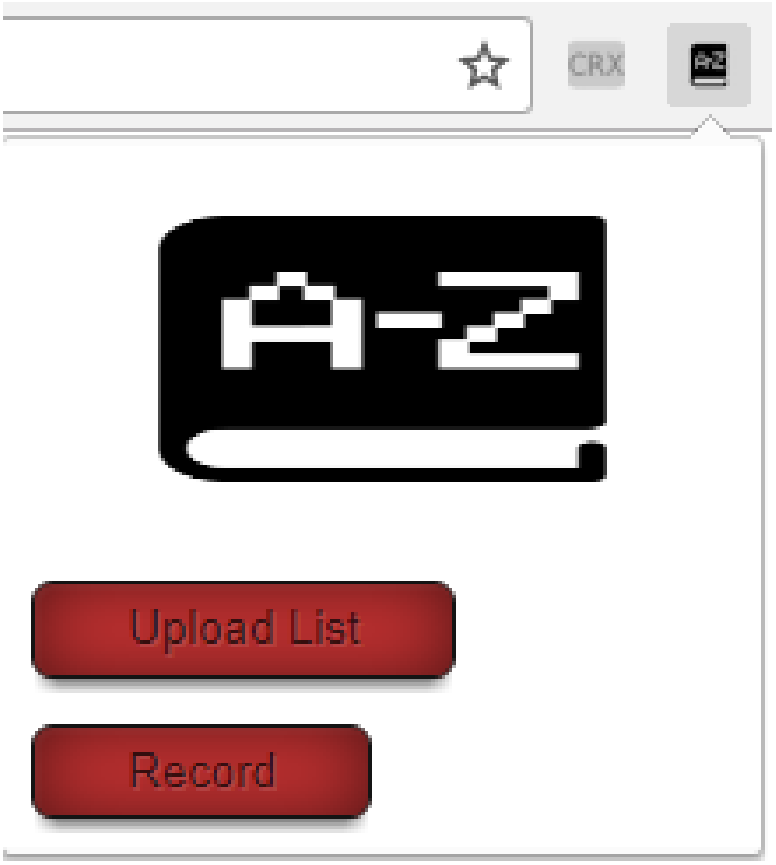
- Синхрон - Та үйлдэл хийхийн тулд яг одоо хийгдэж байгаа өөр нэг үйлдлийг дуусахын хүлээх шаардлагатай.
- Асинхрон - Синхроны эсрэг буюу та үйлдэл хийхдээ заавал яг одоо хийгдэж байгаа өөр нэг үйдлийн дуусахыг хүлээх шаардлагагүйгээр хажуугаар нь шургаж ороод зэрэг үйлдэх боломжтой.

БҮЛЭГ 4

Төслийн хэсэг

Энэ хэсэгт тухайн нэмэлтийн ерөнхий харагдах байдал, ажиллах ажиллагааг харуулна.

4.1 Програмын дэлгэцийн зохиомж

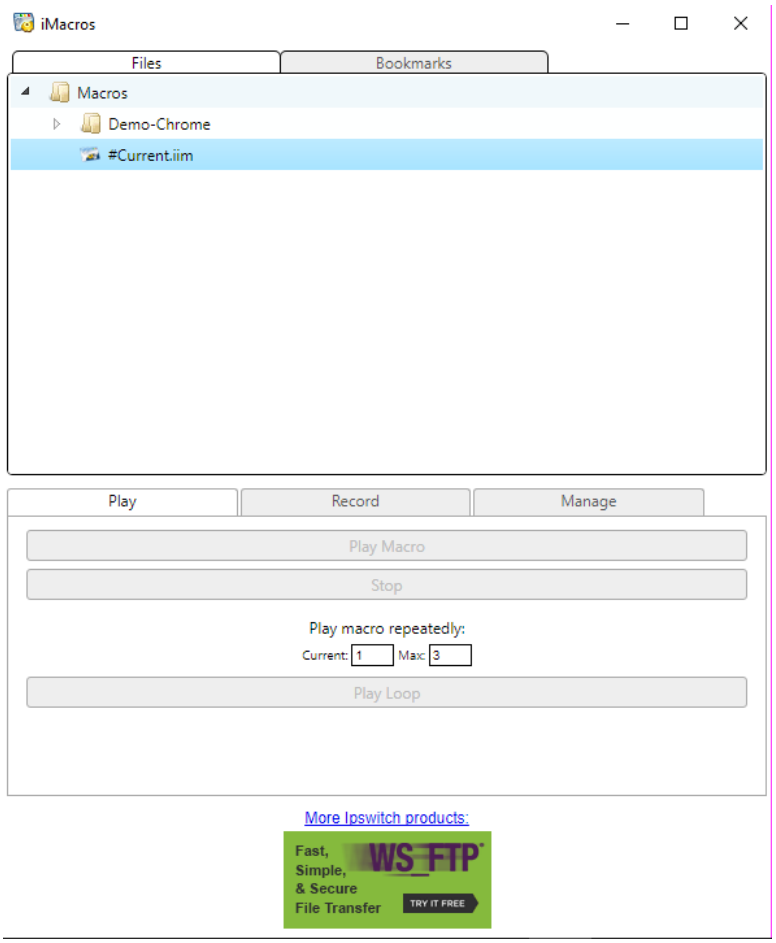


Зураг 4.1: Extension

Энэ хэсэгт ижил төстэй програмуудын ажиллагаа, туршилт болон өөрийн програмын харьцуулалтыг харуулна.

4.1.1 Ижил програм ажиллуулсан хэсэг

- iMacro



Зураг 4.2: iMacro