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

0.1 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 ярихад нууц үг буюу password-ын тухай асуудал их яригдах бөгөөд нууц үгийг эвддэг олон төрлийн халдлага болон хэрэгсэлүүд байдаг тухай онолын хэсгээр өгүүлэх болно.

0.2 Зорилго

Энэхүү төслийн ажлаар тухайн толь бичгийн халдлагыг хялбар аргаар хийж гүйцэтгэх програм хангамж бүхий extension бүтээхийг зорилоо.

0.3 Зорилт

Толь бичгийн халдлага нь хувь хүн болон албан байгууллагад их хэмжээний хохирол учруулах боломжтой бөгөөд тухайн халдлага хэрхэн явагддаг түүнчлэн халдлагад өртөхөөс хэрхэн зайлс хийх талаар мэдээлэл өгөхөд оршино.

Гарчиг

Удиртгал **i**
0.1 Удиртгал i
0.2 Зорилго i
0.3 Зорилт i

1 Онолын хэсэг **1**
1.1 Толь бичгийн халдлага гэж юу вэ ? 1
1.1.1 Аргачлал 1
1.1.2 Нууц үг гэж юу вэ? 2
Үйлдлийн систем дэх нууц үг 2
Unix/Linux MD5 нууц үгний схем 4
1.1.3 Судалгаа 5
1.2 Толь бичгийн халдлагын ерөнхий 5 төрөл 6
1.2.1 Brute-force халдлага гэж юу вэ? 6
1.2.2 Hybrid халдлага гэж юу вэ? 6
1.2.3 Syllable халдлага гэж юу вэ? 6
1.2.4 Rule-Based халдлага гэж юу вэ? 6
1.2.5 Rainbow table халдлага гэж юу вэ? 7
1.3 Халдлага хийх боломжтой програмууд 7
Cain and Abel 7
Crack 7
Aircrack-ng 8
John the Ripper 8
L0phtCrack 8
Ophcrack 9
1.4 Толь бичгийн халдлагаас сэргийлэх нь 9
1.4.1 Сэргийлэх арга хэмжээнүүдийн сул тал 9
Account locking-ын эрсдэл 10
1.4.2 Tools-Reverse Turing Tests 10

Зургийн жагсаалт

1.1 Нууц үг хашлаж,тулгах 3
1.2 MD5 нууц үгний хаш 4
1.3 Нууц үгийн урт 5
1.4 Нууц үгийн төрөл 5
1.5 Captcha 11

Хүснэгтийн жагсаалт

1.1 The MCF 4

БҮЛЭГ 1

Онолын хэсэг

1.1 Толь бичгийн халдлага гэж юу вэ ?

Толь бичгийн халдлага буюу Dictionary Attack нь урьдчилан бэлтгэсэн бүх тэмдэгт мөрүүдийн жагсаалтыг шалгаж үзсэнээр нууц үгийг тааж олох халдлага юм. Энэ халдлагыг ихэвлчэн encrypt хийсэн алгоритм нь тайлагдахаргүй эсвэл decrypt хийгдэх 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, найзынх нь нэр, төрсөн өдөр, төрсөн газар гэх мэтчилэн хэрэглэгч нууц үг дээрээ тохируулсан байх магадлалтай гэх бусад чухал мэдээлэлүүд багтана.

1.1.1 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. Хэдийгээр урьдчилан боловсруулалтыг бэлтгэх хугацаа их шаарддаг ч халдлага хийх хугацааг бага болгож өгдөг. Урьдчилан боловсруусан толь бичгийг нэг л удаа үүсгэнэ, ингээд бэлтгэгдсэн нууц үгийн хашуудаар хэдийд ч тохирсон нууц үгийг олох боломжтой. Харин 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.

1.1.2 Нууц үг гэж юу вэ?

Бүх л системд өөрийн хэрэглэгч болон түүний хувийн мэдээллүүдийг таних шаардлагатай байдаг. Хэрэглэгчдийг таних олон процесс байж болох ба нууц үг нь хамгийн түгээмэл ашиглагддаг төрөл бөгөөд 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.

Үйлдлийн систем дэх нууц үг

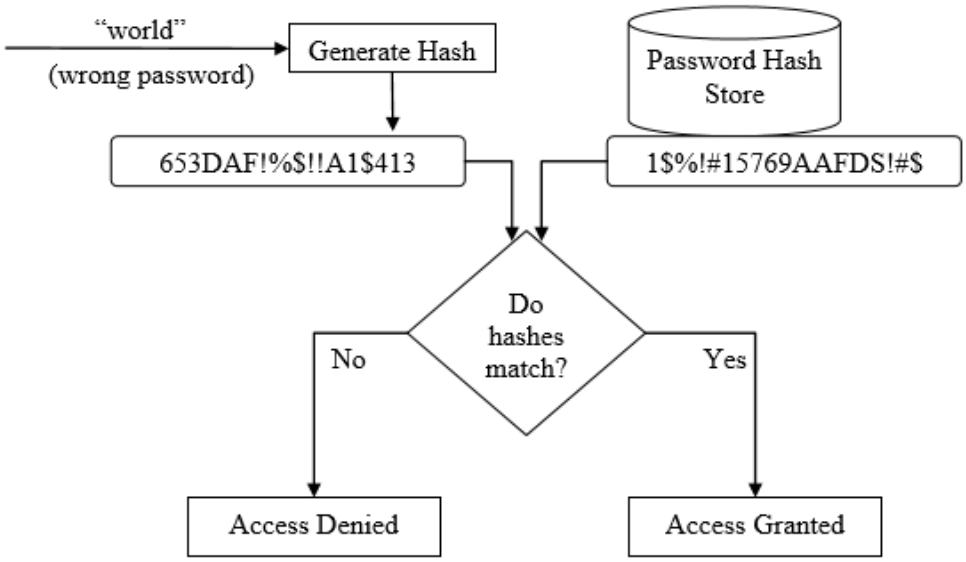
Хамгийн түгээмэл үйлдлийн системүүд дээр хэрэглэгчийг адилтган танилт хийхдээ нууц үгийг ашигладаг. Гэсэн хэдий ч үйлдлийн систем бүр хэрэгжүүлэлтийн хувьд өөр өөр механизмыг ашигладаг.

Харин хувь хүний хувьд тухайн үйлдлийн систем рүү нэвтрэх эрх авахын тулд тэрээр өөрийн итгэмжлэлээ оруулах шаардлагатай. Энэ итгэмжлэл нь Хэрэглэгчийн нэр болон нууц үгээс 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 олгож буруу бол үгүйсгэнэ.

Үйлдлийн системийн хувьд эдгээр итгэмжлэлүүдийг санах ойд хадгалагдсан эсэхийг шалгах ба үйлдлийн систем хадгалагдсан утгыг оруулсан утгатай харьцуулна. Хэрвээ хадгалагдсан нууц үг нь хоосон текст хэлбэрээр байвал энэ нь аюулгүй байдлын чухал асуудал бөгөөд ямар ч хэрэглэгч бусад хэрэглэгчийн итгэмжлэлүүдийг харах боломжтой. Тиймээс үйлдлийн систем нь нууц үг бүрийг хаш хэлбэрээр шифрлэдэг. Нууц үгний хаш нь тогтмол урттай бөгөөд ямар ч 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.

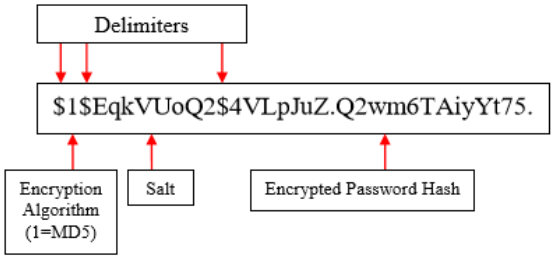


Зураг 1.1: Нууц үг хашлаж,тулгах

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 хаш алгоритмыг ашигладаг байна. Хэрвээ 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 1.2: MD5 нууц үгний хаш

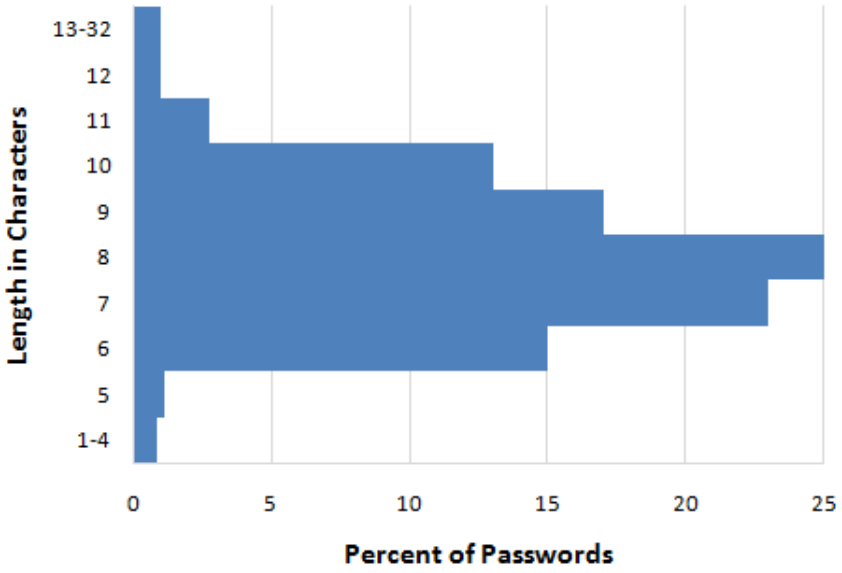
Дээрхи зурагт харагдаж байгаагаар MCF дэхь MD5 нууц үгний хаш утга нь 3 талбараас бүрдэнэ. Хаш утга дотор харагдаж буй долларын тэмдэгт нь талбар доторхи 3 утгыг хооронд нь ангилж буй зааглагч юм. MFC-ын тус тусын талбарууд болон тэдгээрийн зорилгыг дараахи хүснэгтэнд харуулав.

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.

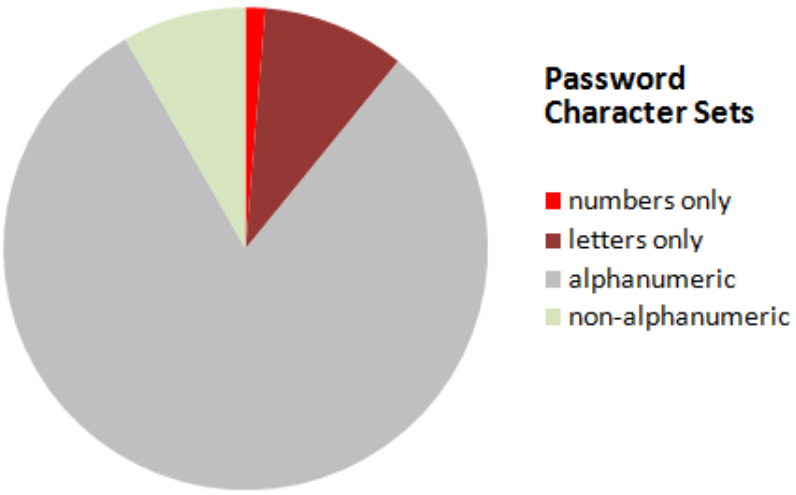
Хүснэгт 1.1: The MCF

1.1.3 Судалгаа

2006 оны судалгаагаар доорх графикийг байгуулсан бөгөөд нийт хэрэглэгчдийн дийлэнхи хувь нь 8 оронтой нууц үгийг ашигладаг мөн дийлэнхи хувь нь нууц үгээ хийхдээ үсэг ашигладаг бол үлдсэн хувь нь дан тоо болон тэмдэгт зэргийг ашигладаг нь тогтоогдсон байна.



Зураг 1.3: Нууц үгийн урт



Зураг 1.4: Нууц үгийн төрөл

1.2 Толь бичгийн халдлагын ерөнхий 5 төрөл

- 1. Dictionary attack
- 2. Brute-force attack
- 3. Hybrid attack
- 4. Syllable attack
- 5. Rule-Based attack

1.2.1 Brute-force халдлага гэж юу вэ?

Brute-force халдлага гэдэг нь криптографт ямарч шифрлэгдсэн мэдээллийг таахад хэрэглэгддэг нууц бичээсийг тайлж унших халдлага 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 - г 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.

1.2.2 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.

1.2.3 Syllable халдлага гэж юу вэ?

Энэ халдлага нь brute-force болон толь бичгийн халдлагыг хослуулсан байдлаар ажилладаг. Энэ халдлага нь Hybrid халдлагатай төстэй бөгөөд ялгаа нь маш нарийн. Hybrid нь толь бичиг дээр суурилсан байдаг.

1.2.4 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 хандуулдаг төрлийн халдлага юм.

1.2.5 Rainbow table халдлага гэж юу вэ?

Нууц үгийг мөн л таах зарчимаар ажилладаг халдлага. Таах оролдлого хийсэн нууц үг бүхэн нь нууц үгийг хашлахад ашигласан алгоритмтай яг ижил алгоритмаар encrypt-лэгддэг. 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 улам сайжруулсан халдлага бөгөөд өөрийн үүсгэсэн хүснэгт дээрээ тэрбум орчим нууц үгийн хашыг урьдчилан тооцоолж хадгалсан байдаг. Энэ хүснэгтийг үүсгэхэд их хугацаа ордог боловч нэг удаа үүсгэчихээд дараа нь дахин ашиглах боломжтой. Ингэснээр тухайн хүснэгтэн дундаас хаш утгыг хайх нь жинхэнэ нууц үгийн хаш утгыг тус бүрд нь тооцоолхоос илүү хурдан, цаг хэмнэх юм.

1.3 Халдлага хийх боломжтой програмууд

Энэхүү халдлагуудыг хийх боломжтой програм хангамжуудыг дурьдвал:

- Cain and Abel
- Crack
- Aircrack-ng
- John the Ripper
- L0phtCrack
- Metasploit Project
- Ophcrack

Cain and Abel

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

Crack

Crack нь систем администраторуудад 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.

Aircrack-ng

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

John the Ripper

John the Ripper нь хуучны бөгөөд хамгийн алдартай нууц үг эвддэг хэрэгсэлүүдийн нэг юм. Хоёр өөр хувилбартай бөгөөд 1. Үнэгүй, open-source болон 2. pro хувилбар байдаг. Энэ хэрэгсэл нь коммандын горимд суурилсан бөгөөд ямар ч GUI (Graphic User Interface) байхгүй. Open-source хувилбар дээр маш олон шинэчлэлт, нөхөлт гарч ирсэн. Энэ нөхөлт нь нэмэлтээр олон төрлийн шинж чанарыг нэмсэн ба өөр олон encrypt хийх алгоритмуудыг оруулж өгсөн. Мөн олон янзын эвдэх төлөвүүд бий болсон. Үүнд: wordlist төлөв, single crack төлөв, incremental төлөв болон external төлөв зэргийг агуулсан байдаг. John the Ripper нь секундэд дунджаар 800,000 нууц үгийг дамжуулах боломжтой. Энэ нь CPU-ны маш жижиг хэсгийг л ачааллагдаг.

L0phtCrack

Энэ хэрэгсэл нь Peiter C. Zatko-ын зохиосон нууц үг шалгаж мөн сэргээдэг application юм. Энэ нь нууц үгний чадалыг шалгадаг мөн зарим тохиолдолд Microsoft Windows-ын мартсан нууц үгийг толь бичиг. brute-force, hybrid болон rainbow table гэх зэрэг халдлагуудыг ашиглан сэргээдэг. Хүртээмжтэй байдал нь өндөр харин үнийн хувьд хямд байдаг тул өргөн хэрэглэгддэг. 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 NTLM Challange Response
- Unix MD5-encoded password files
- Unix DES-encoded password files

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.

1.4 Толь бичгийн халдлагаас сэргийлэх нь

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

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

Мөн энэ халдлагаас сэргийлэх түгээмэл 2 төрлийн арга байдаг.

1. Delayed response Нэвтрэх нэр болон нууц үгийг хослуулж ашиглаж серверээс ирэх хариуг бага зэргийн хойшлуулах. (1 секундэд нэгээс илүү хариу хүлээн авах боломжгүй гэх мэт) Энэ нь халдагч этгээдийг тухайн нэг агшинд олон нууц үгийг оруулж шалгахаас урьдчилан сэргийлнэ.

2. 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 түгжигддэг байхаар) Энэ нь мөн л олон нууц үгийг шалгахаас сэргийлнэ.

Дээрхи эсрэг арга хэмжээнүүд нь нэг компьютерийн орчинд ба хэрэглэгч нэвтрэхдээ физик байдлаар холбогдсон гар ашигладаг байх нөхцөлд сайн ажиллагаатай. Эдгээр аргууд нь мөн сүлжээний орчинд хэрэгжүүлэх нь маш чухал.

1.4.1 Сэргийлэх арга хэмжээнүүдийн 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 систем байгаа ямарч хамаагүй бүртгэлийн хаягыг эвдэх сонирхолтой байдаг ба маш олон оролдлогыг параллелиар гүйцэтгэх боломжтой байдаг. Хэрэглэгчийн нэвтрэлт нь серверээр удирдагддаг учир энэ нь мөн параллелиар олон тооны нэвтрэлтийг ч удирдах боломжтой байдаг ба үүнийг ашиглан хугацаа хэмжих арга барилаас зайлсхийдэг байна. Жишээлбэл халдагч нь 10 милсекунд тутамд нэвтрэх оролдлогыг илгээх ба сервер нэвтрэх оролдлогод хэр удаан хугацаанд хариу өгөхөөс үл хамааран секунд тутамд 100 хүртэлх оролдлогыг нэвтрүүлэх боломжтой.

Account locking-ын эрсдэл

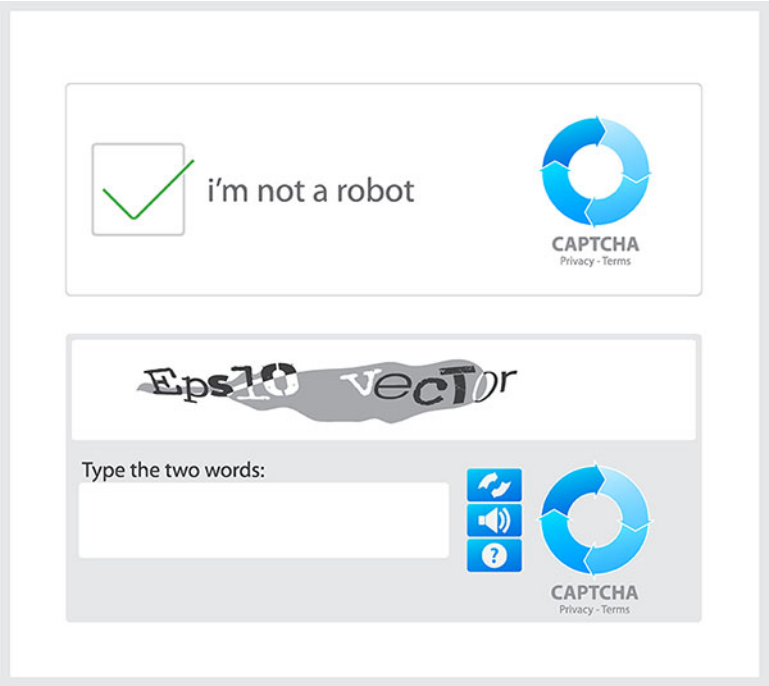
Энэ хамгаалах арга нь мөн өөр төрлийн эрсдэлийг дагуулдаг. Хэрэглэгчдийн эсрэг DOS буюу Denial of Service халдлагыг хэрэгжүүлэх боломжийг олгодог. Энэ халдлага нь хэрэглэгчийн бүртгэлээр санаатай буруу нууц үгийг хэд хэдэн удаа оруулж тухайн хаягыг цоожлуулах боломжтой.

Мөн DOS халдлагын өөр төрөл буюу Distributed Denial of Service (DDos)-ыг өөр нэгэн хэлбэрээр гүйцэтгэх боломжтой. Халдагч этгээд нь вебийн орчинд нууцаар агент(agent)-уудыг байршуулах бөгөөд бүх агентууд тодорхой нэг агшинд тухайн сервер луу санамсаргүй нууц үг ашиглан (эсвэл толь бичиг 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 бүртгэлийн хаяг нь цоожлогдсон хэрэглэгч үйлчилгээ үзүүлэгч байгууллага руугаа залгах шаардлага гарна. (Хэрвээ үйлчилгээ үзүүлэгч байгууллага нь автоматаар цоожийг тайлах эсвэл зөвхөн зөвшөөрөлтэй хэрэглэгч мэдэх хувийн асуулт зэрэг механизмийг суулгаж өгөөгүй бол) Энэ тохиолдолд тухайн байгууллагатай ярих өртөг өндөр гарах асуудалтай байдаг.

1.4.2 Tools-Reverse Turing Tests

Толь бичгийн халдлагаас сэргийлэх өөр нэгэн арга нь багаж хэрэгсэл ашиглах явдал байж болох юм. Энэ нь хэрэглэгч болон компьютерийн програм 2-ыг хооронд нь ялгах хэдэн шалгах процесс юм. Энэ шалгах аргууд нь хэрэглэгч тэнцэхэд амар байх бөгөөд харин автоматжуулсан програмын хувьд хэцүү байх ёстой. Тэдгээрийг анх M. Noar гэх хүн санаачилсан бөгөөд Reverse Turing Tests(RTTs) хэмээн нэрлэгдсэн байдаг бөгөөд өөрөөр энэ шалгах процессийг CAPTCHAs гэж нэрлэдэг.



Зураг 1.5: Captcha

RTTs нь дараах шаардлагыг хангасан байх шаардлагатай.

- Автоматжуулсан үүсгэх процесс: Энэ нь автоматжуулсан аргаар маш олон тохиолдлыг үүсгэхэд хялбар байх хэрэгтэй.
- Хүний хувьд хялбар: Үүсгэсэн тест нь хүмүүс тэнцэхэд хялбар байх шаардлагатай
- Машины хувьд хүнд: Автоматжуулсан тухайн програм нь гараас утга орж ирсний дараа хэрэглэгчтэй шууд харьцаж чадахгүй. Тэр програм нь оруулах боломж нь 2 төрлийх байж магадлалтай: 1. Энэ нь RTTs-ыг үүсгэх боломжтой алгоритмыг оруулж өгсөн байх боломжтой. Ингэснээр RTTs-ыг өөр дээрээ үүсгэж шийдэлийг олох 2. Аюулгүй байдлын талаархи муу ойлголттой 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 тестын шаардлагатай зүйл бол санамсаргүйгээр 6 ширхэг string өгөгдөх ба энийг OCR (Optical Character Recognitions) програмуудаар decode хйихэд хэцүү бөгөөд хэрэглэгчээс string-ын төрлийг асууна.