Информациска безбедност

Предавање 5:
Автентикација

Проф. д-р Весна Димитрова

Автентикација

- Автентикација е процес на при кој што се одредува дали на корисникот би требало да му се дозволи пристап од системот.
- Дали си тој кој што кажуваш дека си?

Методи на автентикација

- Методи кои што се најкористени за автентикација на корисници.
  - Нешто што поседуваш (Картица за банкомат, смарткарица)
  - Нешто што знаеш (Лозинка, ПИН)
  - Нешто што си (Скенирање на отпечатоци, глас, ирис)
  - Нешто што правиш (Овој метод најчесто се користи кога корисникот има физички пристап до системот на пример WPS – Wi-Fi Protected Setup каде од корисникот се бара да стисне одредено копче за да може да биде автентициран)

Лозинки

- Најчесто употребуван метод за автентикација е со употребата на лозинки.
- Лозинки (кодови за идентификација, безбедносни шифри) се користат во речиси секоја интеракција помеѓу корисниците и информациските системи.

Лозинки

- Компромитирана лозинка
  - можност да се влезе и искористи системот и се тоа да изгледа дека е незабележано.
- Во овој случај напаѓачот би имал
  - целосен пристап до сите ресурси кои се достапни на корисникот
  - би бил многу блиску до сите кориснички сметки и
  - до административните привилегии.

Лозинки

- Корисниците со лоши лозинки
  - често изложени на секакви напади.
- Организации со добри и детални упатства со совети за креирање и управување со добри лозинки
  - многу ретки.

Лозинки

- Идеална лозинка
  - нешто што вие го знаете,
  - нешто што компјутерот може да потврди дека вие го знаете и
  - нешто што никој друг не може да го погоди, дури и со пристап до некои неограничени компјутерски ресурси.
- Решение:
  - Математички случајни генерирани криптографски клучеви,
  - Проблем
    - човекот треба да ја запомни таа лозинка.

Лозинки

- Битен факт во врска со лозинките е дека многу работи дејствуваат како лозинки.
  - На пример, PIN број за картичка за банкомат е еквивалентна на лозинка.
  - И ако сте ја заборавиле "вистинската" лозинка, веб-сајтот може да ве идентификува врз основа на вашиот број на социјално осигурување, вашиот презиме, или вашиот датум на раѓање, во кој случај, овие "работи кои ги знаете" дејствуваат како лозинки.
  - Очигледен проблем е што овие работи не се тајна.

Лозинки

- Кога корисниците избираат лозинки, тие имаат тенденција да избераат лоши лозинки, со што пробивањето на лозинките е многу лесно.

Лозинки

- Едно решение за проблемот со лозинките е да се користи случајно генерираниот криптографски клуч на местото на лозинките.
- Потоа пробивањето на лозинка ќе биде еквивалентно на работата на brute force клучните пребарувања.
- Проблемот со таквиот пристап е дека луѓето мора да се сеќаваат на нивните лозинки.

Лозинки

- Како прво, треба да разбереме зошто лозинки се толку популарни.
  - Тоа е, затоа што е "нешто што знаете" повеќе популарно од "нешто што имате "и" нешто што сте ", последните две се, веројатно, посигурни.
  - Лозинките се бесплатни, додека паметните картички и биометриски средства чинат пари.
  - Лозинките се погодни за употреба и лесно прилагодливи и често можеме да ги менуваме.

Лозинки

- Во денешно време сите користиме голем број на сервиси (е-маилови, блогови, форуми и др.) кои од нас бараат користење на корисничко име и лозинка.
- Просечен интернет корисник може да има и над 5 кориснички имиња и лозинки кои секојдневно ги користи.

Лозинки

- Со цел да ја заштитите вашата приватност и да бидете барем малку сигурни дека вашите лозинки нема да бидат откриени на лесен начин од хакерите придржувајте се до следниве неколку совети:
- Лозинка е Вашата прва и последната линија на одбраната во компјутерска безбедност.

Лозинки

- **прво и основно, никогаш не ја давајте вашата лозинка на секој.**
- **направете ја вашата лозинка така што никој нема да може да ја запамти.**
- **направете ја вашата лозинка тешко да може некој друг да ја погоди.**
- **Избегнувајте бесплатен безжичен интернет.**

Лозинки

- **Какви лозинки не треба да користите**
  - Еве некои од видовите на лозинки кои лесно можат да се погодат и кои не треба да ги употребувате:
    - избегнувајте лозинки од вашите лични информации: име, презиме, датум на раѓање, име на миленичe, град, телефониски број, регистарски број на автомобил итн.
    - Не користете лозинки врз основа на работите кои се наоѓаат во ваша близина. Лозинките како "компјутер", "монитор", "тастатура", "телефон", "печатач", итн, се бескорисни.

Лозинки

- Не користете од оние лозинки кои се лесни за запамтување но кои не нудат никаква безбедност како "password", "letmein".
- зборови кои можат да се најдат во било каков речник
- вашето корисничко име, името на компјутерот или емаил адресата
- името на некој ваш близок
- зборови кои се лесни за погодување, лозинки лесни за пробивање. Еве неколку такви примери: кратенки, астероиди, имиња од цртани, кратки фрази, презимиња, места, спортови, филмови...

Лозинки

- никогаш не додавајте број до некој збор на пример "apple1"
- не го дуплирајте зборот на пример "appleapple". Зборовите кои постојат во речникот на кој било јазик во светот, напишани од лево кон десно или од десно кон лево, не треба да се користат како лозинки, бидејќи лесно можат да бидат „уловени“од страна на сајбер-криминалците.
- не го пишувајте зборот кој го користите како лозинка во обратен редослед на буквите пример "elppa”

Лозинки

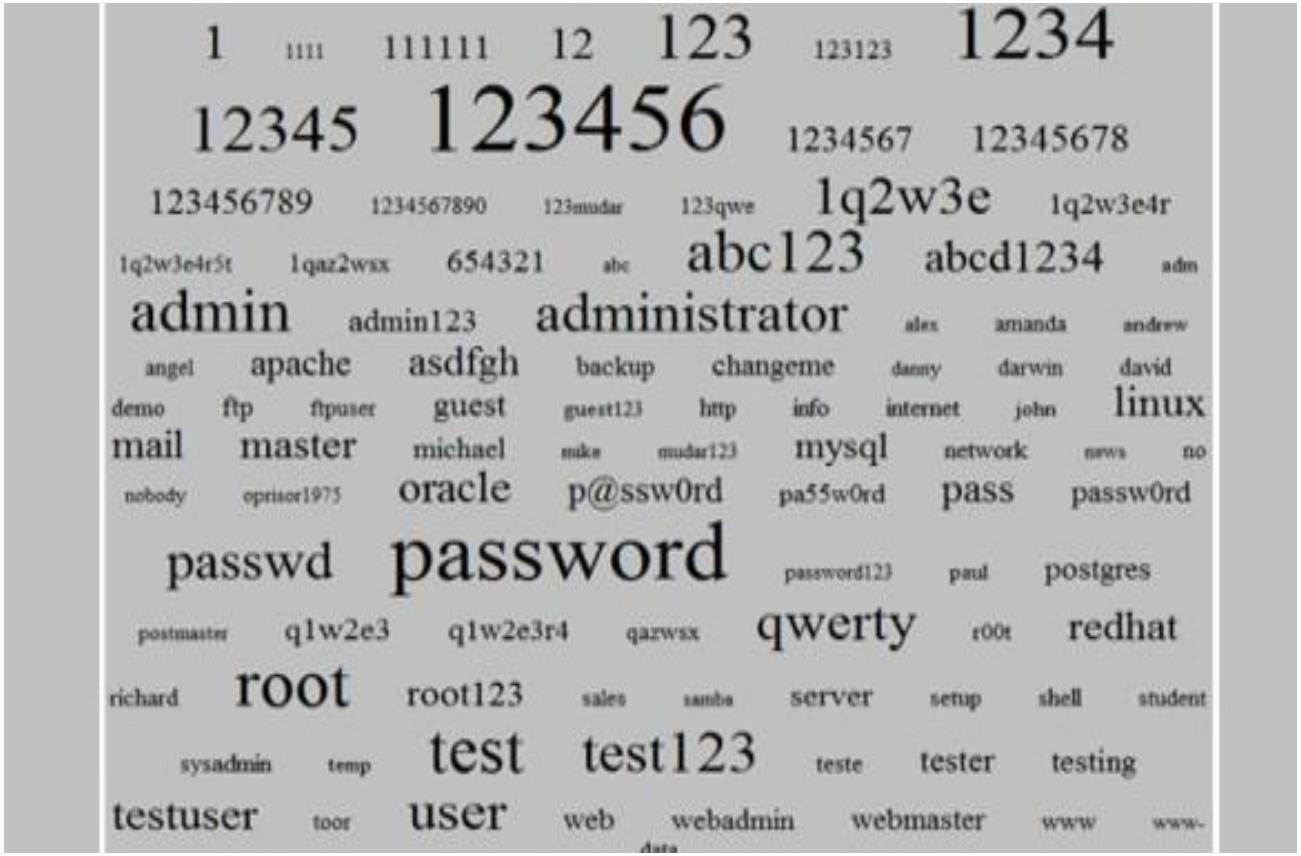
- не ги отстранувајте само самогласките пример "ppl"
- Клучни секвенци кои лесно може да се повторат,. на пример, "QWERTY", "asdf" итн
- Зборови како што се `` foobar", `` xyzzy" и `` QWERTY" се уште се едноставни зборови. Тие исто така се често употребувани лозинки, и програмите за пробивање лозинки лесно ги наоѓаат. Избегнувајте ги нив.

- Никогаш не ја користете истата лозинка двапати.

Лозинки

- **Совети**
  - Изберете лозинка на која може да се сеќавате, така што не треба да ја запишувате или барате, ова ја намалува веројатноста некој да ја најде и открие.
  - Изберете лозинка која брзо ќе можете да ја напишете, ова ја намалува веројатноста некој да ја запамти со гледање.
  - Вашата лозинка третирајте ја како една од најголемите тајни во вашиот живот.

Лозинки


1 1111 111111 12 123 123123 1234
12345 123456 1234567 12345678
123456789 1234567890 123mudar 123qwe 1q2w3e 1q2w3e4r
1q2w3e4r5t 1qaz2wsx 654321 abc abc123 abcd1234 adm
admin admin123 administrator alex amanda andrew
angel apache asdfgh backup changeme danny darwin david
demo ftp ftpuser guest guest123 http info internet john linux
mail master michael mike mudar123 mysql network news no
nobody oprisor1975 oracle p@ssw0rd pa55w0rd pass passw0rd
passwd password password123 paul postgres
postmaster q1w2e3 q1w2e3r4 qazwsx qwerty r00t redhat
richard root root123 sales samba server setup shell student
sysadmin temp test test123 teste tester testing
testuser toor user web webadmin webmaster www www-
data

Лозинки

- **Избор на лозинка**
  - Корисниците се поделени во три групи и им се даваат следниве совети во врска со изборот на лозинки:
    - Група А: Изберете лозинки кои се состојат од најмалку шест карактери, и со најмалку еден карактер што не е буква. Ова е типичен совет за избор на лозинка.
    - Група В: Изберете лозинки врз основа на фрази.
    - Група С: Изберете лозинка која се состои од осум случајно избрани карактери.
  - Со експерименти е пробано да се пробијат лозинки на корисниците во секоја од трите групи.

Лозинки

- Група А: Околу 30% од лозинките се пробиени. Корисниците од оваа група лесно ги паметат своите лозинки.
- Група В: 10% од лозинките биле пробиени, како и на корисниците во групата А, на корисниците од оваа група лесно можат да ги паметат своите лозинки.
- Група С: Околу 10% од лозинките биле пробиени. Но корисниците од оваа група тешко можат да ги запаменат своите лозники.

- Овие резултати укажуваат на тоа дека лозинките базирани на фрази претставуваат најдобра опција за лозинка, бидејќи лозинките од оваа група тешко можат да се пробијат, а лесно да се запаметат од страна на корисниците.

Лозинки

- Според резултатите од експериментот, речиси 10% од лозинките најверојатно ќе бидат пробиени, без разлика на дадениот совет.
- Значи најдобар начин за избирање на лозинки е според вториот совет, група 2.
- Покрај тоа, администраторот треба да користи алатка за пробивање на лозинки со што ќе се тестираат слабите лозинки на корисниците, пред напаѓачите да ги пробијат.

Лозинки

- **Промена на лозинка**
  - Треба да се менува лозинката барем еднаш месечно.
  - Исто така треба да ја смените лозинката секогаш кога ќе се сомневате дека некој ја знае, или дека некој ќе може да ја погоди.
  - Никогаш не употребувајте некоја стара лозинка повеќе пати.

Лозинки

- **Заштитете ја вашата лозинка**
  - Никогаш не чувајте ја вашата лозинка на вашиот компјутер освен во шифрирана форма.
  - Не кажувајте ја лозинката на никој, дури и на вашиот систем администратор
  - Никогаш не ја испраќајте вашата лозинка преку е-маил или некој друг необезбеден канал.
  - Бидете внимателни кога ја пишувате вашата лозинка, кога сте во иста просторија со некој друг.

Лозинки

- **Памтете ја вашата лозинка**

  Памтењето на лозинки секогаш е тешко и поради тоа многу луѓе се во искушение да ги запишуваат на парчиња хартија. Ова е многу лоша идеја. Така што можете да направите?

  - Користете безбедносен пасворд менаџер
  - Користете текстуална датотека шифрирана со силна енкрипција
  - Изберете лозинки кои полесно ќе ги запаметите.
  - Многу е важно да запомните дека во никој случај не треба да ја споделувате вашата лозинка со никого, дури ако се работи и за вашиот шеф или пак ИТ администратор. Доколку тоа се случи, веднаш сменете ја лозинката во прва прилика.

Лозинки

- Постојат повеќе програми и алатки со кои можете да се чуствувате повеќе безбедни и сигурни такви се:
  - Password Safe, KeePass Password Safe, Password Safe Pro, LSN Password Safe, Password Safe and Repository Personal Edition, Enterprise Password Safe, My Password Manager, Atory Password Generator 1.2, Sticky Password.

Лозинки

- **Пробивање на вашата лозинка**
  - Постојат четири основни техники кои хакери можат да ги користат за да ги прибијат вашите лозинки:

Лозинки

- Украдена. Тоа значи дека вашата лозинка може да се пробие кога некој гледа додека вие ја пишувате, или ја пронајдат хартијата на која сте ја запишале лозинката. Ова е најверојатно најчестиот начин на компромитирање на лозинки, со што е многу важно ако ја пишувате лозинка на хартија таа да биде колку што може на најбезбедно место. Исто така не ја пишувајте вашата лозинка кога некој може да ве гледа.

Лозинки

- Погодена. Ова се случува бидејќи многу луѓе ги користат своите лични информации како лозинка. Психолозите велат дека повеќето луѓе ги користат имињата на своите љубовници, мажи, жени или деца како лозинки

Лозинки

- Brute force напад. При овој напад се користи секоја можна комбинација од букви, бројки и симболи, во обид да се погоди лозинката. Иако ова е многу тешка задача, со модерните брзи процесори и софтверски алатки овој метод не треба да се потценува. Пентиум 100 компјутери обично може да биде во можност да се обиде со 200.000 комбинации во секунда тоа би значело дека на лозинка од 6 карактери која содржи само мали и големи букви може да се открие само за 27 ½ часа.

Лозинки

- Dictionary attack (речник напад). Овој метод е поинтелегентен од Brute force нападот кој е опишан погоре. Тука комбинациите се добиваат според првиот слободен збор во речникот. Со помош на многуте софтверски алатки кои се достапни може да се проба секој збор во речник или зборот, или и двете се додека вашата лозинка не се понајде. Достапни се речници со стотици и илјади зборови, како и специјални, технички и речници со странски јазик, листи на илјадници зборови кои често се користат како лозинки како "qwerty", "ABCDEF" итн

Прифаќање на лозинка

- За еден компјутер да ја утврди валидноста на внесена лозинка мора да има пристап до соодветната лозинка.
- Поради поголема безбедност наместо да ја сочуваме лозинката директно во датотека, ќе ја сочуваме:

  $$y=h(password)$$

  во датотека, каде што h е безбедна хаш функција.
- Внесената лозинка се хашира и се споредува со y, ако се исти тогаш корисникот е успешно логиран на системот.

Биометрика

- Постојат повеќе видови на автентикација кои се користат денес меѓу кои е вклучена и автентикацијата со помош на биометрика.
- Биометриката може да се разбере на начин на кој што тоа го кажал Schneier, односно “you are your key”.
- Биометриката како автентикација вклучува повеќе методи за автентицирање, а некои од нив се: отпечатоци од прсти, своерачни потписи, распознавање на ликови, отпечатоци од дланка, говор, па како нешто најсовремено од оваа област, распознавање на мирис.
- Една од главните цели на биометриката е замената на лозинките кои ги користиме секојдневно, но постојат мали ограничувања за тоа зашто биометриката сеуште не се користи масовно, а тоа е поради нејзината цена и безбедност.

Карактеристики

- Тие се побезбедна замена за лозинките
- Карактеристики на идеалниот систем за биометрика:
  - Универзален
    - Треба да биде подобен за секого. На пример постојат луѓе чии отисоци од прстите не се читливи
  - Прецизност
    - Способност за распознавање со голема прецизност. Во реалност не може да се надеваме на 100% прецизност меѓутоа постојат системи кои што имаат многу мала рата на грешка
  - Постојан
    - Идеално би било физичките карактеристики на системот да останат исти за подолг временски период
  - Доверлив, робусен и лесен за интеракција со корисниците

Фази во биометриката

- Постојат две фази во биометриката и тоа се:
  - Првата фаза се нарекува “enrollment phase” и е фаза во која што системот “учи” податоци, односно во системот се внесуваат биометриски податоци за автентикацијата.
  - Втората фаза се нарекува “recognition phase” односно фаза во која системот ги врши распознавањата на податоците. Во оваа фаза корисниците се автентицираат на системот.

Типови на грешки

- Постојат два типа на грешки, ќе дадеме примери:
  - Првиот пример е кога Боб пробува да се претстави како Алис и системот по грешка го автентицира Боб како Алис. Ратата на оваа грешна автентикација се нарекува “fraud rate”.
  - Вториот пример е кога Алис сака да се автентицира самата себе си, но сега системот паѓа на нејзината автентикација. Ратата на оваа грешна автентикација се нарекува “insult rate”.
- Ратата на грешки може да варира, односно да се променува, но промената на едната рата на грешки е за сметка на другата. Тоа значи дека доколку ние ја зголемиме insult ратата, fraud ратата ќе се намали и обратно.
- Најкорисно е кога ратите на грешки се на исто ниво.

Биометрика - Проблеми

- Веројатноста за грешка може да доведе до злоупотреба или до неуспех при автентикација на правилен корисник.
- Ако се намали границата за совпаѓање ќе се зголеми процентот на злоупотреба.
- Ако се зголеми границата за совпаѓање ќе се зголеми незадоволството на правилните корисници заради неуспех на автентикацијата.

Биометриски техники

- Отпечатоци на прсти
- Геометрија на рака
- Скенирање на ирисот

Отпечатоци на прсти

- Прва подетална анализа е направена во 1798 год кога е претпоставено дека се уникатни.
- Во 1892 год е развиен систем на класификација според шема на отпечатоците.
- Со помош на класификацијата се вршело ефикасно пребарување дури и пред добата на компјутерите.

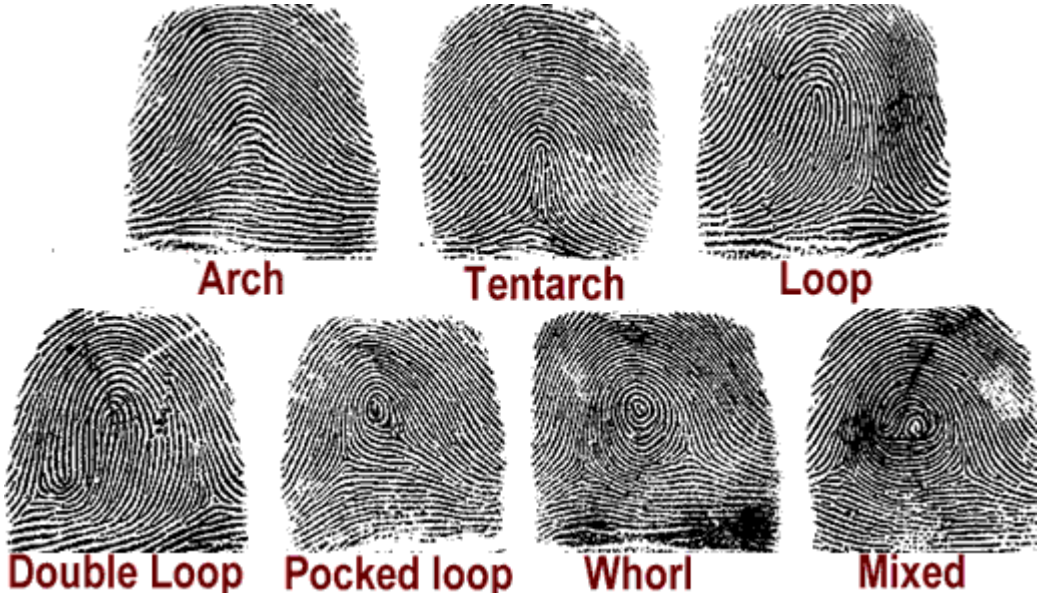
Отпечатоци на прсти

- Употреба на отпечатоци

- Се зема слика од отпечатокот, којашто потоа се подобрува и анализира со алатки за процесирање на слики.
- Се откриваат точки за лесно препознавање, коишто потоа се сместуваат во база.
- Кога се прави некоја споредба системот враќа процент на совпаѓање на тие точки.

Отпечатоци на прсти

Различни шеми



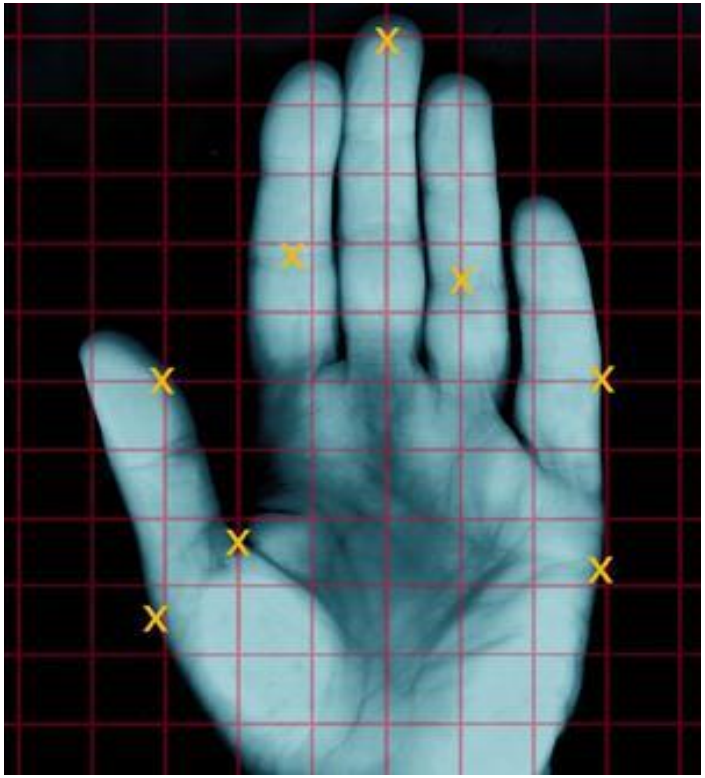
Геометрија на рака

- Принцип кој најчесто се користи за влез во згради со високо обезбедување.
- Форма на раката, должина и ширина на дланката и прстите.
- Рацете не се “уникатни” како отпечатоците.
- Не е препорачлива за идентификација поради голем број на лажни совпаѓања.
- Предности – брзи, симетричност на раце.
- Негативности – не се користи кај деца и стари лица.

Геометрија на рака

- Hand geometry measurements

- Hand geometry measurements



Скенирање на ирисот

- Релативно нова технологија, идејата – 1936, примена – 1986.
- Најдобар начин за вршење автентикација.
- Ирисот (обоениот дел од окото) е различен за секоја личност, разлика постои и помеѓу двете очи кај иста личност.
- d(x,y) = број на несовпаѓачки битови/вкупен број на споредени битови
- d(x,y) = 0,08 – ист ирис.
- d(x,y) = 0,50 – различен ирис.
- Вообичаената шема за точна потврда при споредба на ириси е дистанцата помала од 0.32, во спротивно се смета дека не се исти.

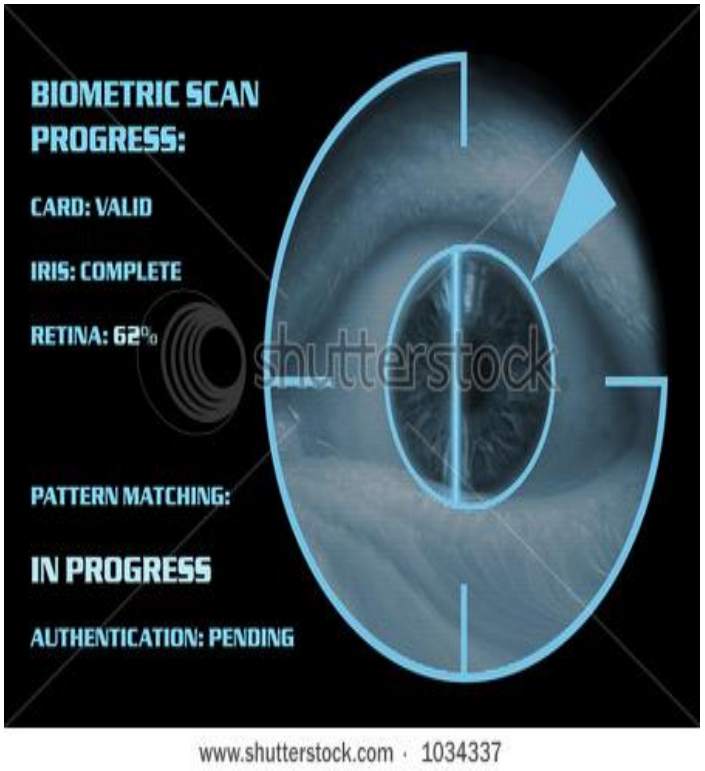
Скенирање на ирисот

- Напади на системот се возможни.
- Боб има слика од окото на Алиса и сака да се престави како неа.
- Слични случки во минатото.
- Со цел заштита од овој вид напади повеќето iris scan системи прво пуштаат сноп на светлина со цел да се провери дали доаѓа до смалување на зеницата.

Скенирање на ирисот

- Iris scan

- Iris scan



Грешки кај биометриски системи

- Fingerprint biometric systems – 5 %.

Изненадувачки но вистинито, резултат на тоа што овие системи се најчесто евтини уреди.

- Hand geometry biometric devices – 10 ^-3.

Најчесто софистицирани и скапи уреди.

- Iris scanning systems – 10^-5.

Во пракса е многу тешко да се постигнат овие бројки.

- Сите горе наведени стапки на грешки се однесуваат на лабораториски услови и во пракса ретко се совпаѓаат.
- Во праксата fingerprint системите се многу точни.

Биометриски системи

- Биометриските системи имаат предности и заостанувања во однос на другите системи.
- Потенцијал да ги заменат системите кои се засноваат на лозинки.
- Поголема безбедност = повисока цена.
- Проблем – софтверско базирани напади кои се тешко решливи.

Нешто што имаш

- Смарт картиците или други хардверски токени можат да бидат искористени за автентикација. Смарткартиците се уреди со големина на кредитна картица кои што имаат мала меморија и пресметковни ресурси за да бидат во можност да зачуваат криптографски клучеви или друг вид на тајни.

- Од друга страна читачите на овие смарт картици ја извршуваат втората половина од процесот на автентикација со тоа што ја читаат запишаната тајна или клуч и го автеникуваат корисникот. Бидејќи се користат клучеви, а клучевите се генерираат по случаен избор, нападите со погодување на лозинки во овој случај се елиминирани.

Нешто што имаш

- Постојат и други примери од овој метод на автентикација:
  - Лаптоп компјутер - преку неговата MAC адреса
  - Картица за банкомати
  - Генератор на лозинки

“Two – factor” автентикација

- Потребата да се искористат два од трите познати методи за автентикација е познато под името two – factor автентикација.
- Генаратор на лозинки = “something you have” (password generator) + “something you know” (PIN кодот).
- Други примери:

  - АТМ картичка.
  - кредитна картичка со потпис.
  - смарт картичка со ПИН код.