

INFORMATIKAI BIZTONSÁG ALAPJAI

Levelező - 2. konzultáció

Göcs László
főiskolai tanársegéd
*Neumann János Egyetem GAMF Műszaki és Informatikai Kar
Informatika Tanszék*

Felhasználók azonosítása



A hagyományos azonosítás alapjai

- **Személy, objektumleírás**

Az azonosítani kívánt elem adatait feljegyzik

Hiba: hiányos információ, a felismerést személy végzi

- **Aláírás vizsgálat**

Eltárolt aláírást a pillanatnyival hasonlítanak össze

Hiba: könnyen hamisítható, összehasonlítás nem megbízható

- **Kulcs vagy kulcsszó használata**

Az objektum vagy személy rendelkezik egy olyan tárggyal, kulccsal, vagy jelszóval, amit ismer az azonosító fél

Hiba: a technológia széles körben ismert, hamisítható

Elektronikus azonosító rendszerek

- A hagyományos azonosítást használják, de az emberi azonosításnál megbízhatóbbak

Hiba: a berendezés is elromolhat, és a berendezést is ember kezeli

Megfelelő humán háttér biztosítása

- Megfelelő oktatás
- Egyszerű kezelhetőség biztosítása
- Segítséget nyújtó rendszerek
- Külső felügyelő

Megfelelő technikai háttér biztosítása

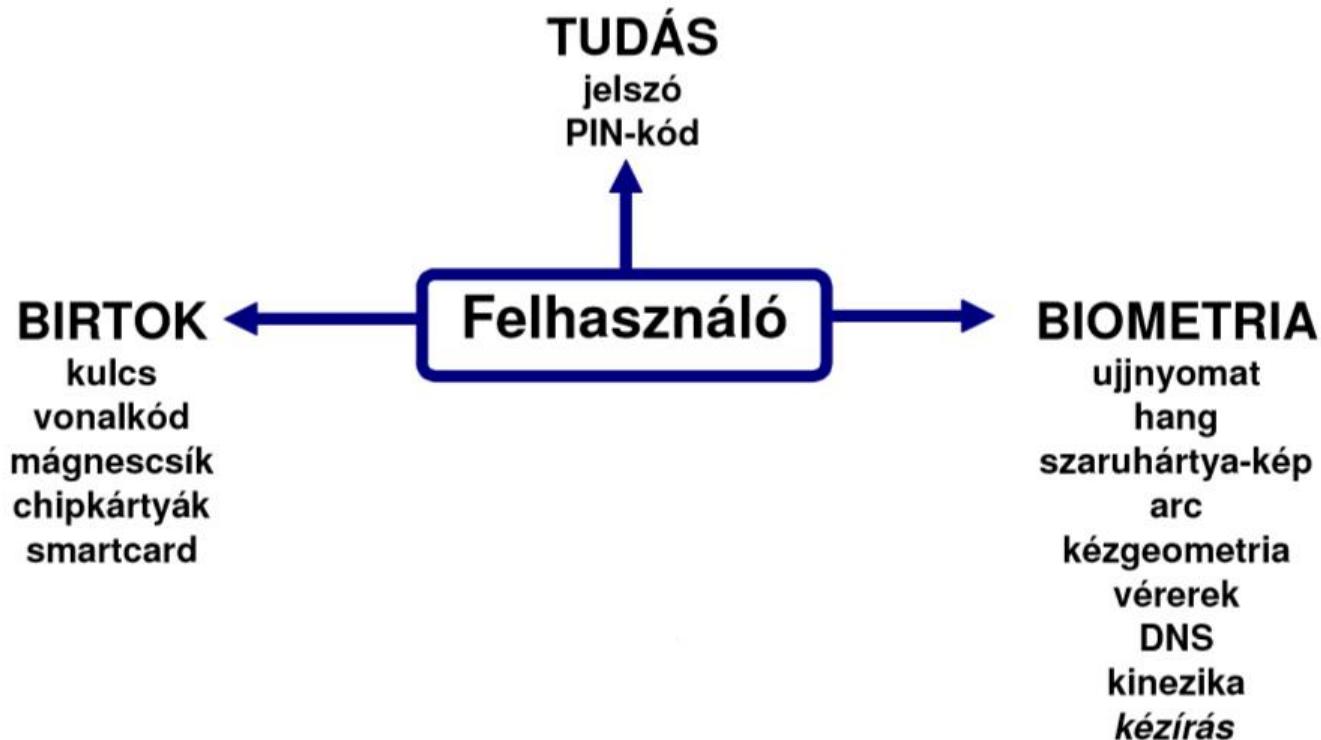
- A feladat által megkívánt rendszer biztosítása
(igényfelmérés, ár-megbízhatóság, körülmények)
- Igénybevételnek megfelelő rendszer
(felmerülő fizikai, kémiai igénybevétel)
- A rendszer megkívánt kiépítése
(teljes, használható, hozzáférhető, igény szerint kihasználható)

Felhasználó azonosítás

Egy személyt több jellemzője alapján is lehet azonosítani!

- Mit tud?
- Mi van nála?
- Fizikai-biológiai értelemben kicsoda?

A felhasználó-azonosítás alapmódjai:



Tudás

- Használata egyszerű
- Olcsó
- Észrevétlenül másolható és tulajdonítható el
(nincs visszajelzés ha más birtokába került)
- Erős védelem megjegyezhetősége nehéz

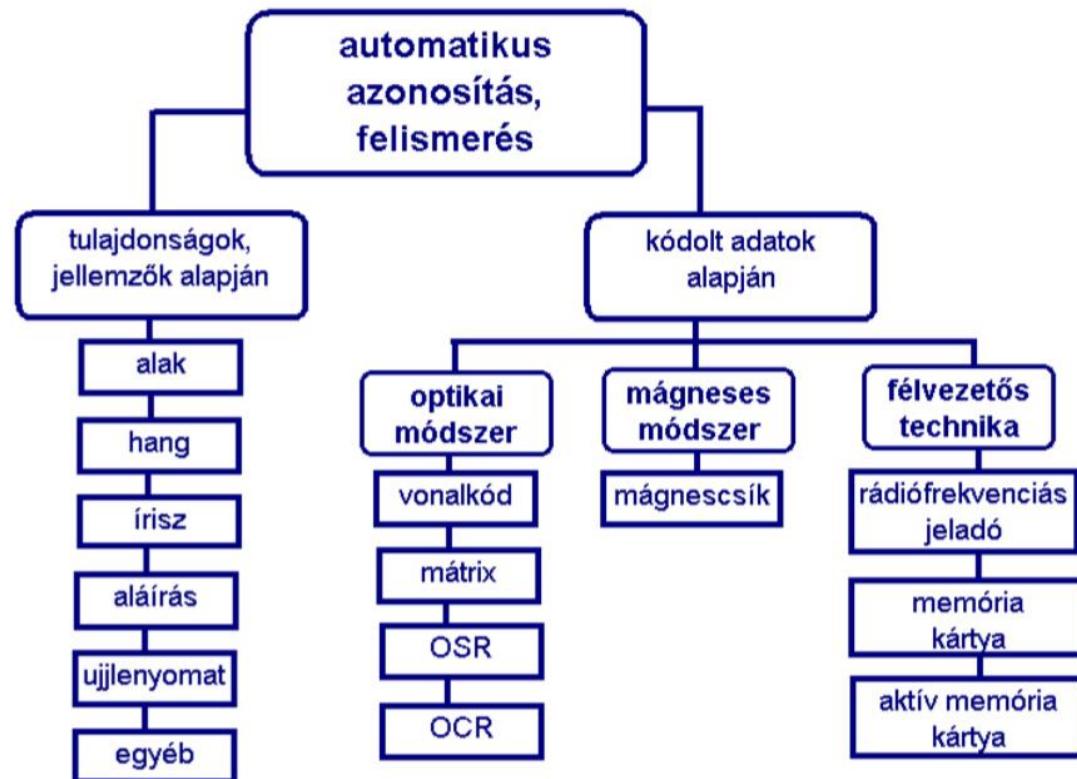
Birtok

- Egyszerű használat.
- Olcsótól a drágáig.
- Eltolajdonítható (*érzékelhető, letiltható*)
- Másolás elleni védelem fontossága! (*titokban ne lehessen másolni, mert nincs visszajelzés*)
 - Másolás szempontjából:
 - Passzív, csak olvasható (vonalkód)
 - Aktív, írható/olvasható (mágneskártyák, chipkártyák, telefonkártyák)
 - Intelligens, kriptográfiai műveletek (másolásvédelem)

Biometria

- Néhol nehézkes az alkalmazása de megbízható
- Egyszerű megoldások nem biztonságosak, kijátszhatóak.
- A komoly megvalósítások drágák.
- Jogi, adatvédelmi problémák (*biometrikus adatok tárolása*)
- Egészségügyi problémák

Technikai megvalósítás:



Jelszó alapú azonosítás

A személyt azonosító titkos információ (jelszó) titokban tartása lehetetlen



gyenge védelem

(kifigyelhető, megszerezhető)

Jelszavak

- Felhasználók által kitalált
- Számítógép által generált
- PIN-kódok
- Kérdés és válasz kódok
- Kombinációs jelszavak
- Jelmondatok
- Jelmondat alapú betűszavak
- Algoritmikus jelszavak

Azonosítási technikák

Eszközök azonosítása

Vonalkódos rendszerek

A vonalkód **vékony** és **vastag** vonalakból áll. A vonalkód olvasó fotóérzékelővel a kódot elektromos jellé változtatja olvasás közben, és méri a **relatív szélességét** a vonalaknak és a **helyeket** a vonalak közt.

Így fordítja az olvasó a vonalkódokat írásjelkre, és küldi a számítógéphez vagy kézi terminálhoz.



Vékony-Vastag-Vékony-Vékony-Vastag-Vékony-Vastag-Vékony-Vékony

010010100

(Code 39 Start/Stop írásjel)

Vonalkódos rendszerek

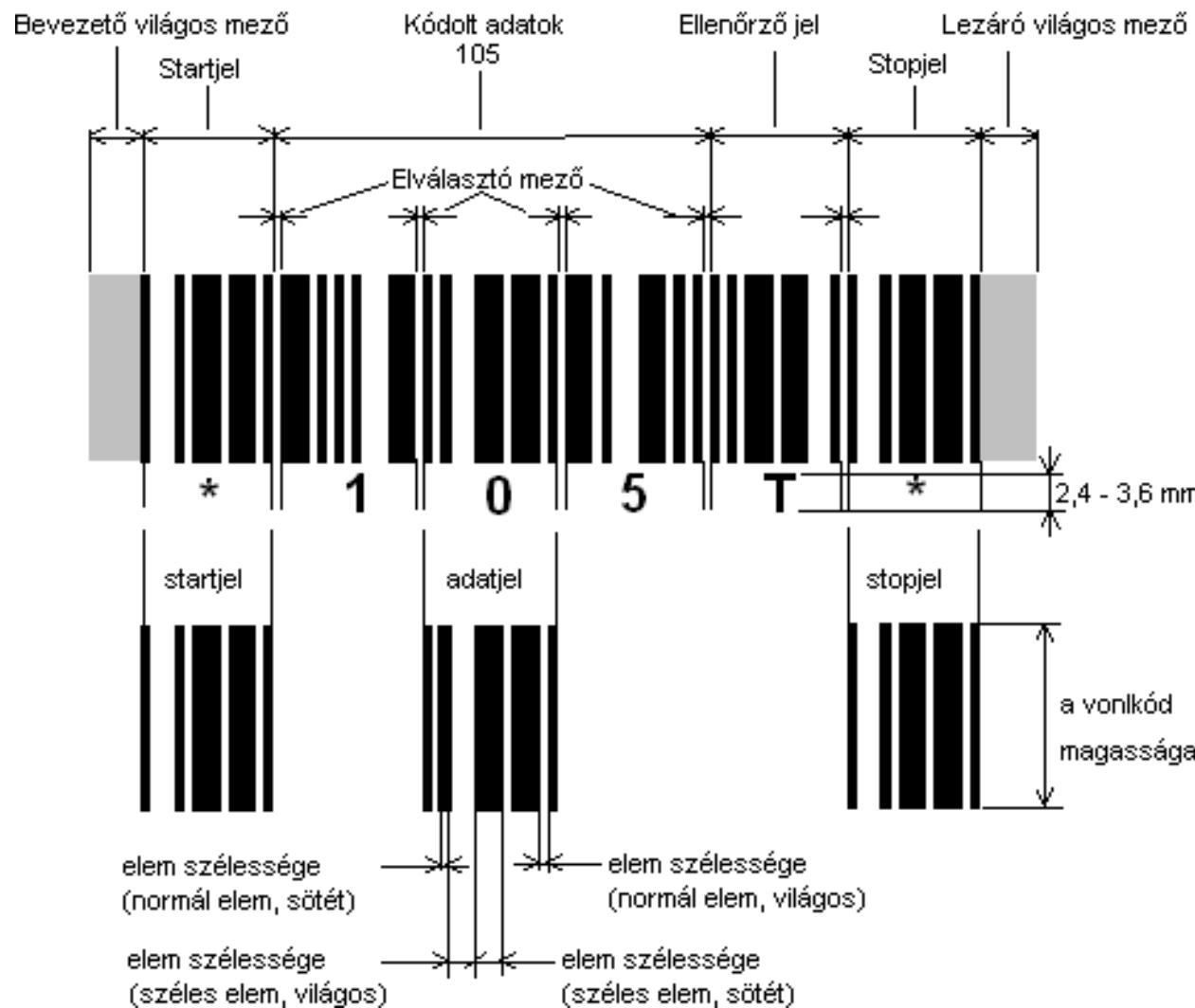
Minden vonalkód egy különleges **Start** és **egy Stop** jellel rendelkezik. Így tudja az olvasó felismerni, ha előre vagy visszafelé olvasta a vonalsorozatot.

Továbbá, egyes vonalkódoknak **checkszum jele** is van közvetlen a Stop jel előtt. A checkszum nyomtatás közben van kiszámítva, a vonalkód karakterek alapján.

A vonalkód olvasó **ugyanezt a számítást végrehajtja**, és hozzáhasonlítja az eredményt a checkszumhoz.

Ha a két szám nem egyezik, az olvasó **hibát feltételez**, és újból próbálkozik.

Vonalkódos rendszerek



EAN-13 -t világszerte használják kiskereskedelemben. A jel 13 karaktert kódol: az első két vagy három vonal az **országkód** mely jelezi. Az országkódot fojtatja 9 vagy 10 **adat** jegyszám, és egy **checkszum**. Két vagy öt jegyszámú kiegészítő vonalkód hozzáadható. Így elérhető a 14 vagy 17 jegyszámú vonalkód.

Modulo 10 kalkuláció a checkszum:

Add össze a páros számú számjegyeket: 2, 4, 6, stb.

Az eredményt 3 -al beszorozni.

Add össze a páratlan számú számjegyeket: 1, 3, 5, stb.

Add össze a 2. és 3. végeredményét.

A check karakter a legkisebb szám mely a 4. lépéshoz adható, hogy a 10 többszöröse legyen az eredmény.

Például: Legyen a vonalkód adata = 001234567890

$$0 + 2 + 4 + 6 + 8 + 0 = 20$$

$$20 * 3 = 60$$

$$0 + 1 + 3 + 5 + 7 + 9 = 25$$

$$60 + 25 = 85$$

$$85 + X = 90 \text{ (10 többszöröse legyen az eredmény), tehát } X = 5 \text{ (checkszum)}$$



EAN-8 az EAN-13 kód rövidített változata. Az első két vagy három vonal az országkód, 4 of 5 adat számjegy (az országkód hosszúságán függő), és a checkszum. Igaz, hogy lehetséges plusz 2 vagy 5 számjegyes hosszabbítást tenni a kódhoz, az EAN-8 kód fő célja minél kisebb helyet foglaljon el.



A **UPC-A 12** számjegyű kódot tartalmaz. Az első számjegy a számlolórendszeret azonosítja.

A következő 5 számjegyű kód a gyártót azonosítja.

A ezután levő 5 számjegy a tárgyat azonosítja, és ezt a számot a gyártó adja meg.

Az utolsó számjegy a checkszum.



UPC-E az UPC-A variációja, amelyet a 0-s számú rendszerre használható. UPC-E kódok nagyon kicsi helyen elférnek mivel a 0 -t kiszűrik.



Interleaved 2 of 5 számokból álló vonalkód, melyet főleg áruraktárakban, és ipari műhelyekben használnak. Az adatnak páros számú számjegyből kell állnia.

A karakterek 5 elemből állnak, 5 vonal, vagy 5 space.

Két elem az ötből vastag, valamint három vékony.

Szomszédos karakterek összefésültek, tehát alternálódik a space és vonal egyik karaktertől a következőig.



Codabar a számokat (0-9), hat jelét (-:\$/+), és a start/stop karaktereket (A, B, C, D, E, *, N, vagy T) kódol. A start/stop karakterek párokban vannak, és nem szerepelhetnek többször a vonalkódban.

Codabar-t könyvtárak, csomagkiszállító szolgáltatók, véradó központok, és más adatfeldolgozó alkalmazások használják. Nincs előírt checksum, viszont egyes iparágak kifejlesztették a saját checksum standardeket.



123456789012

A Code 39 teljes karakter sorozata 0-9, A-Z (csak nagy betűk), és a space, mínusz (-), plusz (+), pont (.), dollár (\$), slash (/), és százalék (%).

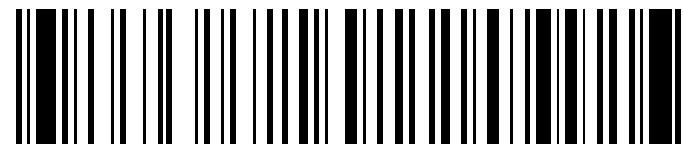
A start/stop karakter a kód elején és végén található, és a vonalkódnak nincs maximum hosszassága, viszont 25 -nél több karakter terheli kapacitását.

Minden egyes karakter 9 elemből áll: 5 vonal, és 4 üres hely. Egy karakter 3 vastag, és 6 vékony elemből áll.

Code 93 egy kisebb fajtája a Code 39-nek. Ugyanazokat a karaktereket használja, mint a Code 39, de karakterenként csupán 9 vonalkód elemet használ a 15 helyett. A Modulus 43 checksum nem kötelező, úgy, mint a Code 39 esetében.



12345ABCDE



12345ABCDE

Code 128 kitűnően tömörít numerikus és alphanumerikus adatoknak.

Előnyösebb, mint a Code 39, mivel karakterválasztéka bővebb, és tömörebb. A Code 128-nak teljes karakter sorozata 0-9, A-Z (nagy és kis betűk), és az összes standard ASCII jelek és kontrol kódokból áll.

A kódok három alegységre vannak választva: A, B és C.

- Az A alegység a standard ASCII jeleket, számokat, nagybetűket és kontrol kódokat tartalmazza;
- A B alegység standard ASCII jeleket, számokat, nagybetűket és kisbetűket foglalja össze; és a
- C alegység két számot tömörít egy karakterbe.

Ráadásul, mindegyik alegység tartalmaz kontrol karaktereket, ami engedi a váltást egyik alegységtől a másikig egy vonalkódban. Végül, három külön start kód létezik, mely jelezzi, hogy melyik alegységet használja.



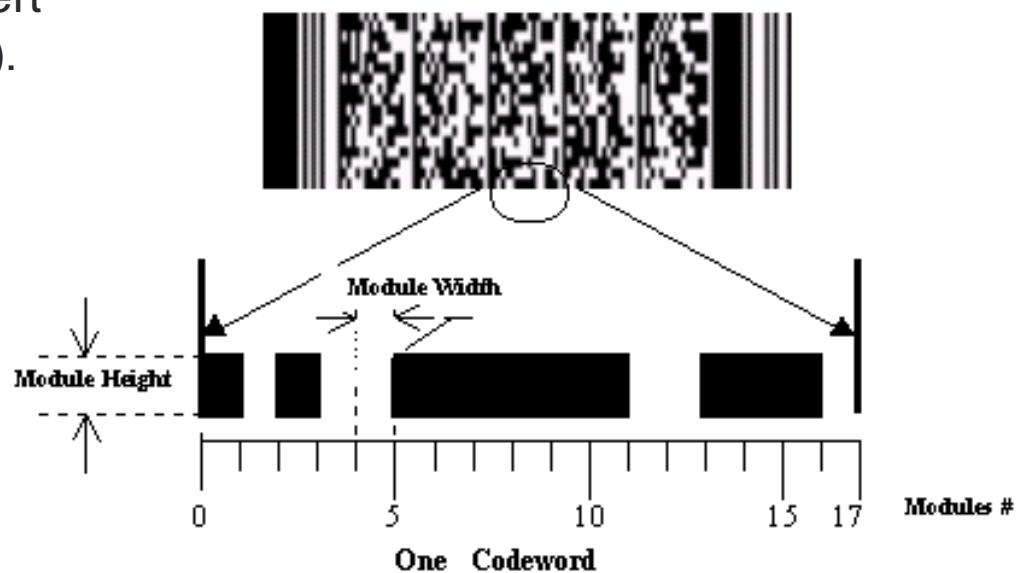
PDF-417 2-dimeziós vonalkód, ami 1 800 nyomtatható ASCII karaktert, vagy 1 100 bináris karaktert tud tárolni.

A jel négyzetes, a hosszassága növekedhet az adat mennyiségétől függően. Többszörös PDF-417 jelekre is lehet szétválasztani az adatokat, melyek összefűzhetők, tehát nincs határa a PDF-417 csoport tartalom képességének.

A PDF-417 hasznos eljárás, főleg mikor az adatok a termékkel utaznak, például mikor az adatbázis nem elérhető. A PDF-417-at általában veszélyes anyagok megjelöléséhez, ujjlenyomatok és fényképek kódolásához főleg jogosítványokon, és műszaki cikkek részletezésére használják.

PDF-417 jelei kétdimenziós szkennert igényelnek;
vagy egy standard CCD-t vagy lézer szkennert
és egy speciális dekódoló-szoftvert
(a wand olvasó nem fog működni).

PDF417 SYMBOL



A **DataMatrix** egy két-dimenziós vonalkód, ami 1 - től 2 000 karaktert tud tárolni. A négyzet - alakú jel lehet 0.001 arasz nagyságútól 14 arasz is. A kód denzitása példájuként, 500 számos kód, minden össze egy arasz nagyságú DataMatrix. A felül látható DataMatrix, 20 ASCII karakter kódja.

Termékek és sorozat számok kódolhatóak DataMatrix-al.

A DataMatrix olvasásához csupán a két-dimenziós vonalkód olvasó használható, ami lézer, és CCD kamera technológiát igényel, tehát a lineáris vonalkód olvasók nem alkalmasak. DataMatrix jelek nyomtatásához a termál transzfer vonalkód nyomtató használható.



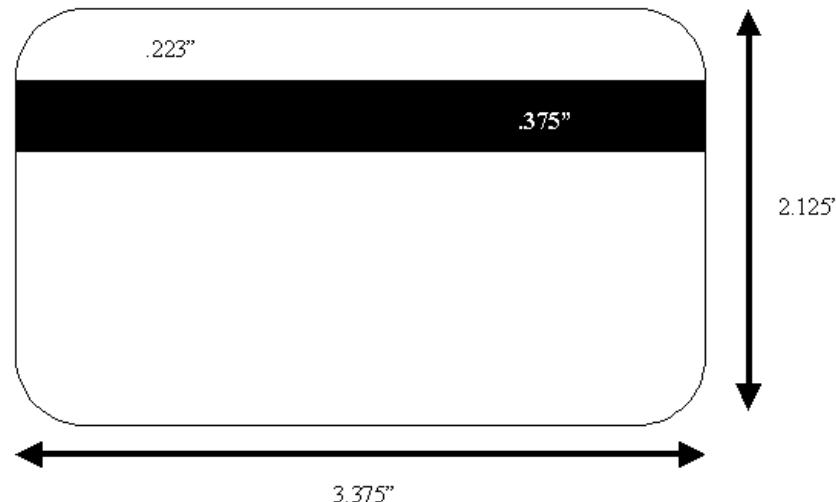
IR vonalkód

A kód nem látható, mert olyan réteggel vonják be, ami a fénynek csak az infra részét engedi át.
Használatához infra megvilágítás és olvasás szükséges.

Felhasználók beléptetése

Mágneskártya

A mágnescsík tartalma nem más, mint **mágneses mezők váltakozása**, amely lényegében minden olyan tulajdonsággal rendelkezik, amivel a hagyományos vonalkódok, csak éppen a kiolvasáshoz az egyszerű optikai leolvasás helyett **elektromágneses eljárás** szükséges.



Mágneskártya

A kártya működése egy nagyon egyszerű fizikai jelenségen alakul, miszerint ha egy mágneses mező és egy vezető relatív **mozog**, akkor a mező **feszültséget indukál a vezetőben**.

Ezt kihasználva a csíkon mágneses területeket alakítanak ki, amelyek így lehúzáskor az olvasóban feszültséget indukálnak és így olvassák ki a rajta lévő tartalmat.



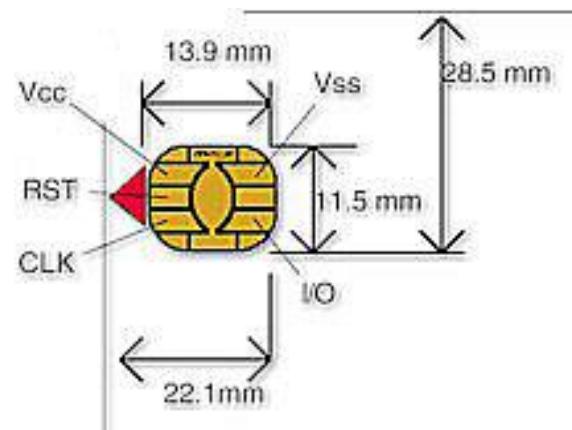
Chipkártya

A chipkártyák, vagy más néven intelligens kártyák nem hasonlíthatók technológiailag a mágneskártyákhoz. Mondhatni, hogy szinte **csak az alakjuk egyezik meg**, minden más tulajdonságuk teljesen eltérő.

A hordozó nem más, mint egy **műanyagból készített lap**.



Az általánosan használt chipek mérete 10-20 mm² és jellemző vastagsága kevesebb, mint 0,2 mm. Ezekkel a paraméterekkel biztosítani lehet, hogy a kártya a használat során fellépő hajlítási igénybevételnek ellenáll az elektronika sérülése nélkül.



Chipkártya

- **memóriakártyák:** azok a fajta kártyák, amelyek CPU-t nem tartalmaznak, de leg-alább 100 byte memóriakapacitással rendelkezik. Tipikus példája a telefonkártya.
- **intelligens kártyák:** ezekre a kártyákra integrálnak egy mikrokontrollert, a mi szempontunkból CPU-t, ami képes különböző műveletek végrehajtására, tehát lényegében egy programozható eszközzel állunk szemben.
Ennek 3 fontos fajtája van, melyek különböző további részekre bonthatók:
 - **Érintkezéses (contact) kártyák:** a legelterjedtebb fajta. A kártyakezelő eszközzel fizikailag is érintkezik a működése során.
 - **Érintkezésmentes (contactless) kártyák:** rádiós kapcsolattal kommunikál a kezelőegységgel
 - **Hibrid és kombi kártyák:** Az előző 2 fajta keresztezése, bizonyos esetekben 2 különböző chippel.

Biometriai azonosítás

Biometria

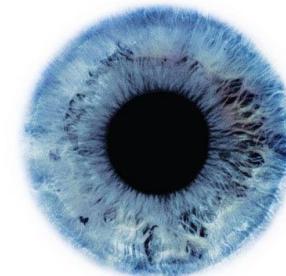
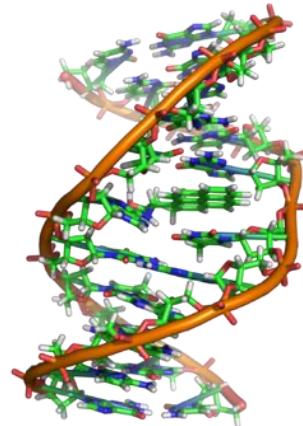
A biometria olyan testi, illetve viselkedésbeli **jellemvonások összessége**, melyek mérése alkalmas arra, hogy egy adott személyt **egyértelműen azonosítani** lehessen.

Minden egyes ember saját, **egyedi-egyszer-megismételhetetlen** jellemzőkkel rendelkezik.

Biometria

A biometrikus azonosítás legfőbb előnye, hogy **magát az embert azonosítja**.

Mivel a biometrikus mérés az **adott személyre** egyedileg jellemző jegyeket azonosítja, gyakorlatilag kizárátható a tévedés lehetősége.



Kézírás

A slide features a large, stylized, handwritten signature in black ink that reads "Signature". The signature is fluid and cursive, with varying line thicknesses and ink saturation.

- Nem tiszta biometriai azonosítás
- A kézírás nem igényel komolyabb olvasó berendezést
- Nem csak az írásképet, hanem a vonalvezetés dinamizmusát is ellenőrizni kell
- Hatékony azonosításhoz:
 - Betűk alakja, mérete, dőlése, kötése
 - Ékezetek formája, dőlése, betűhöz viszonyított helyzete
 - Tollemelés stb.
- Nem megbízható, mert a fizikai és lelki állapot befolyáshaltja.

Ujjnyomat



- **Optikai**, melyek az ujjnyomat fodorszál-szerkezetét a látványa alapján rögzítik: általában látható/nem látható tartományba eső hullámhosszúságú fénnnyel megvilágítják, az ujjat, és "lefényképezik". Ezek az olvasók a bőr legfelső, egyben legsérülékenyebb felületét látják csak. Érzékenyek a **bőr szennyezettségére**, a **bőr minőségére** (száraz, repedezett, nedves, kopott).

Ujjnyomat



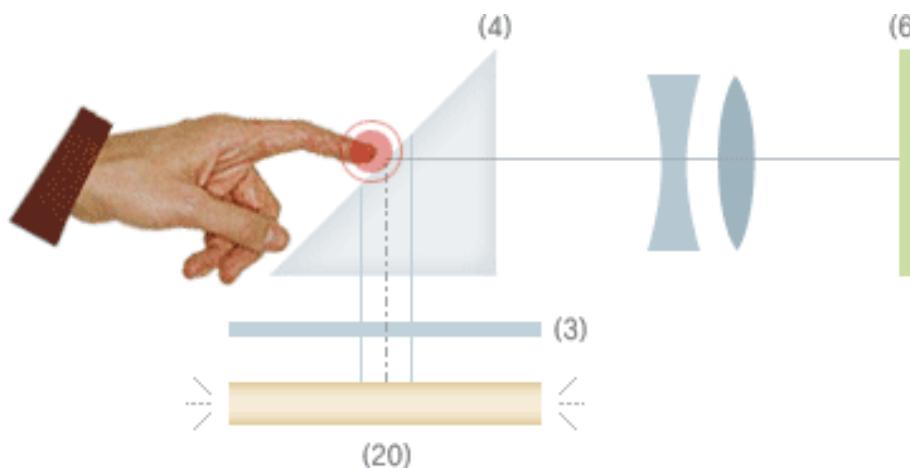
- A **kapacitív** és a **nyomásérzékelős** elven működő eszközök eltérő jeleket érzékelnek a bőrredők dombos vagy völgyes részein.

Ujjnyomat



- Az **ultrahangos** és a **rádiófrekvenciás** szenzorok az újra bocsátott és visszavert hang illetve rádiófrekvenciás jelek különbségei alapján térképezeik fel a bőr redőzöttségét.

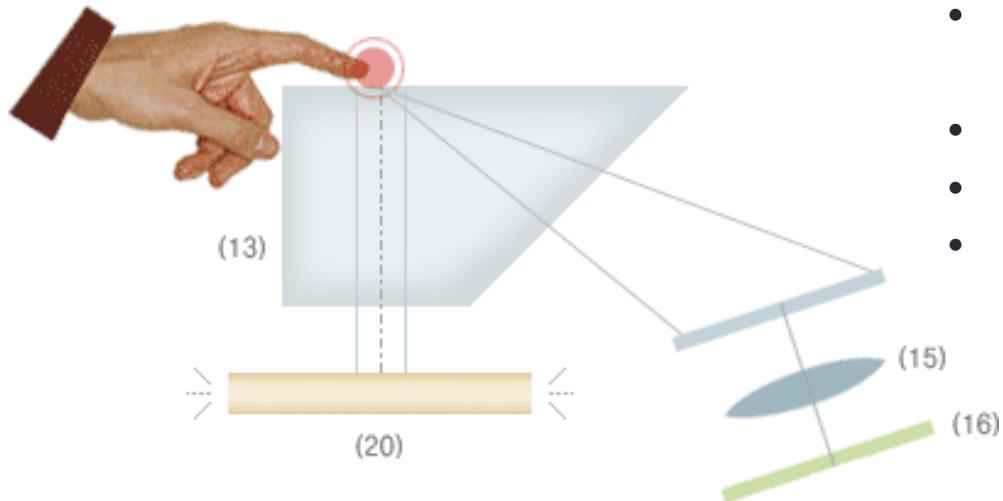
Abszorpciós elven működő optikai olvasók. A képalkotáshoz egy prizmát használnak.



- derékszögű háromszög prizma (4)
- fényforrás (20)
- diffúziós lemez (3)
- lencse-csoport és a képérzékelő (6)

A teljes **fényvisszaverődés megszűnik**, amennyiben az üvegfelülettel érintkezik a bőrfelület, a "hegygerinc". Itt elnyelődik a fény, mert kilép a prizmából.
A fodorszálak fekete vonalként jelennek meg a lencserendszer utáni képalkotó felületen, általában CCD elemen.

Ennél a másik kialakításnál mintha **inverz képet** készítenénk: a völgy lesz sötét, és a hegygerinc világos: csak az ujjról visszaverődött fény jut el a CCD elemhez.

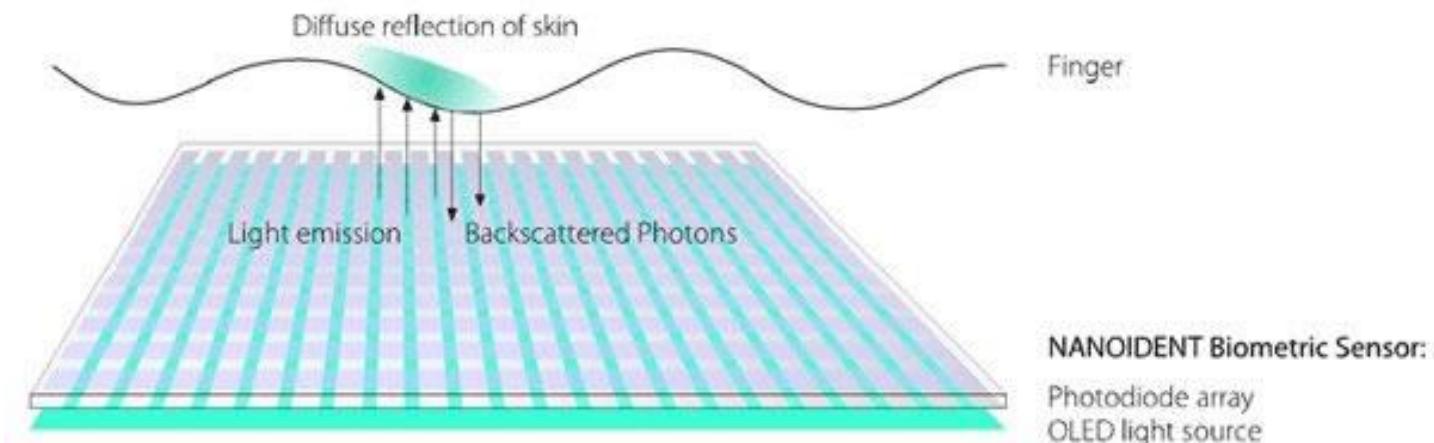


- négyzetes-háromszög prizma (13)
- fényforrás (20)
- lencse csoport (15)
- képérzékelő (16)

Ez a kialakítás jobb, kontrasztosabb képet ad, de drágább. (Az elsőnél a teljes CCD felületre jutó összfénymennyiséget "csökkentjük", amikor az ujj érintkezik a felülettel, az utóbbinál a CCD-re csak az ujjfelületről visszaverődött fény kerül.)

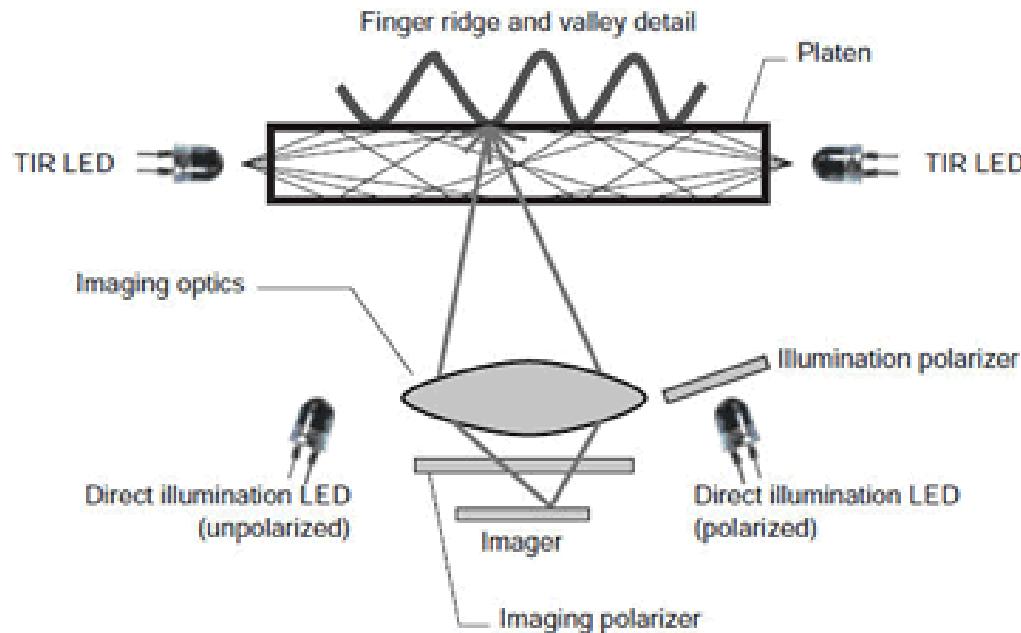
Touchless optikai olvasó

Vannak olyan optikai olvasók, melyeknél kihagyják a prizmát. Ezek közvetlenül, érintés nélkül fényképezik az ujjat. Használatánál figyelni kell az ujj-kamera távolságára.



InfraLED-ekkel világítják meg a speciális "touch" lapot két szélről, valamint szemből polarizált fénnyel is.

Több képet készítenek, melyből egy MSI módszerrel szerkesztenek össze egy képet.

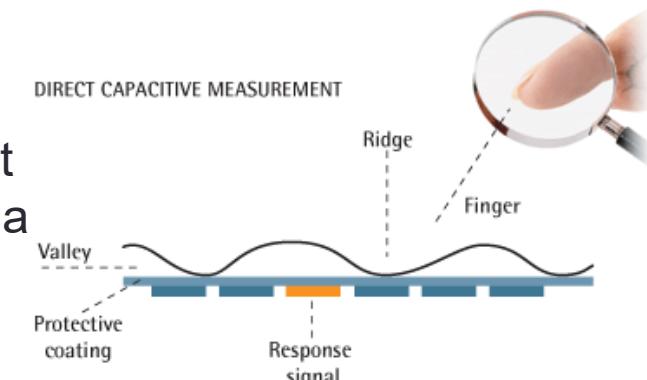


Kapacitív olvasók

A kapacitív olvasók a touch felület és a bőr közötti **elektrosztatikus kapacitást** mérik, és alakítják azt át képpé.

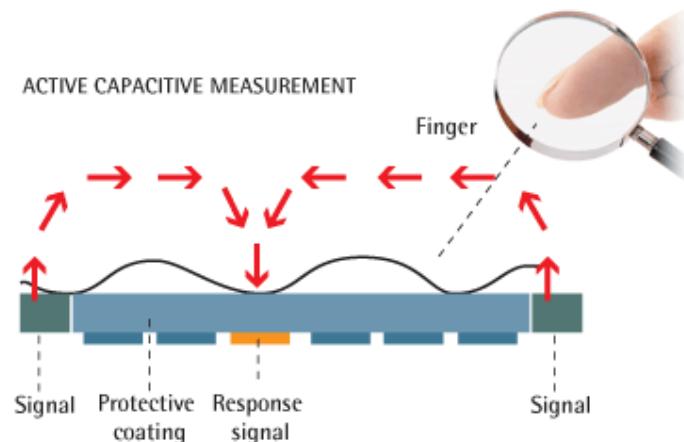
Passzív kapacitív olvasók

A bőr és a touch felület közötti kapacitást méri: mást mér a völgyeknél, mert itt a bőr és a felület távolsága nagyobb, és mást mér a hegyerincen.



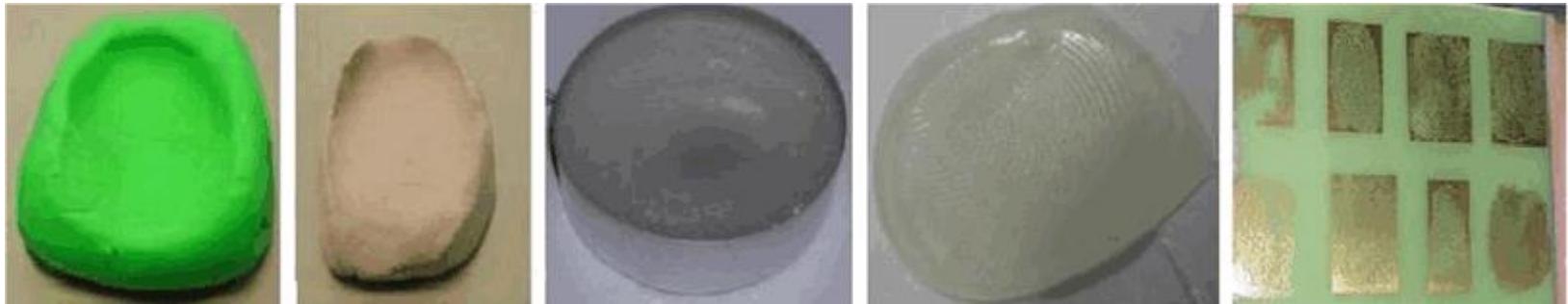
Aktív kapacitív olvasók

A kapacitás mérés előtt "töltést" kap az ujj is.



Ujjnyomat hamisítás

Mára a legtöbb olvasó érzékelni, hogyha "hamis ujjal" próbálják becsapni. (De vannak technológiára épülő olvasók, melyek eleve csak "élő" ujjról képesek felvételt készíteni.)



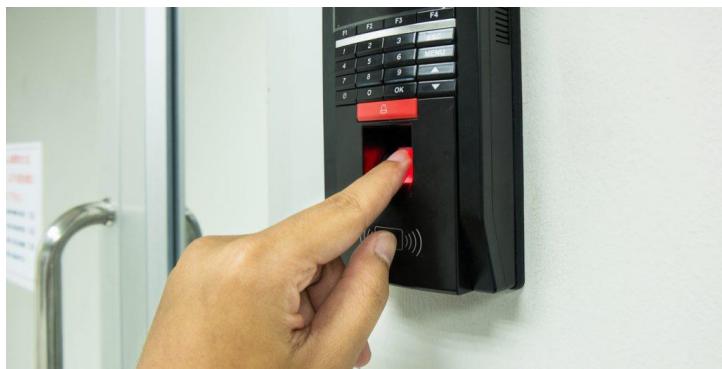
Ujjnyomat hamisítás

Az ellenőrzési módszerek a legkülönfélébbek:

- érzékelik az "élő bőr" elektromos vezetőképességét,
- vér oxigén szintjét mérik
- pulzust mérik
- vizsgálják a véráramlást
- vagy a hamis ujjkészítéshez általában hasznát vegyszer szagát érzékelik
- az élő és a hamis ujjról alkotott képek között különbséget tudnak tenni az alkalmazott képalkotási technológia miatt

Alkalmazás

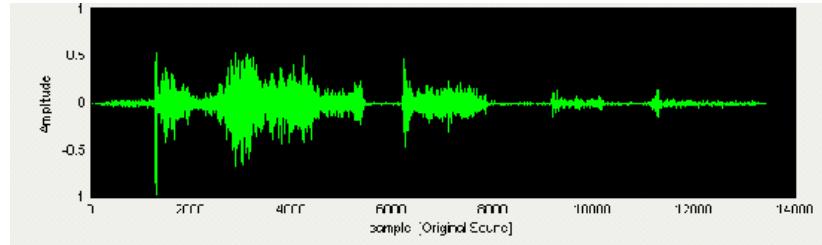
- Okmányok
- Telefon
- Beléptetés objektumba
- Azonosítás (bűnöldözés)



Hang azonosítás

- Az azonosítandó személy egy-egy rövid tárolt hangmintáját hasonlítják össze az éppen elmondott szövegel.
- A beszédstílus jellemzői alapján történik az azonosítás több hangminta alapján.
- Hangminták összehasonlítására elektronikák az időtartományból frekvenciatartományba konvertálnak.

Hang azonosítás



Speaker recognition

Magának a hangnak az azonosítása szolgál, mely a beszélőre egyedileg jellemző.

A beszélő mindenkor ugyanazt mondja (szövegfüggő azonosítás), vagy szöveg független (bármit mondhat) azonosítás.

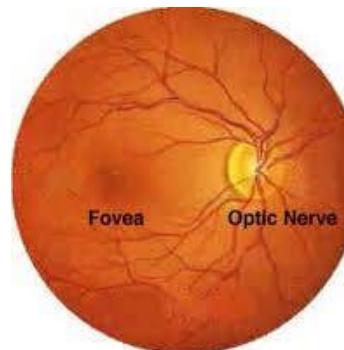
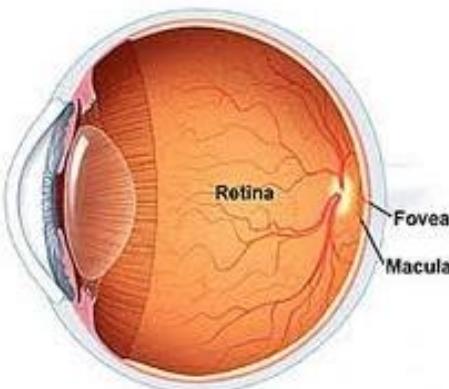
Speech recognition

A beszédnek az azonosítása/felismerése szolgál.

A speaker és speech recognition szinte adja magát a **multimódusos biometriára** (a kettő együttes alkalmazása).

Retina azonosítás

- Az emberi szem hátsó falán található vérerek mintázatán alapul.
- Nagy pontosságú.
- A felhasználók számára sokszor kellemetlen a mintavétel.
- Felléphetnek fertőzésveszélyek, cukorbetegség esetén az érhálózat sérülhet.



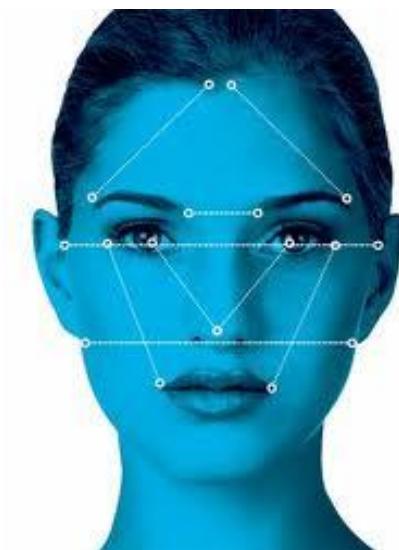
Írisz azonosítás

- A feldolgozás a zajszűréssel kezdődik.
(Zavarok:szempilla, szemhéj, pupilla, tükrözések)
- Utána történik meg az írisz struktúra felismerése, majd az Irisz kód előállítása.
- Az írisz kód egy polárkoordináta-rendszerben leírt sajátosságok sorozata, melyet a pupillától kifelé haladva körkörösen vesznek fel.
- Az írisz kód 256 byte hosszú (Dr. John Daugmann 1998 - 400 különböző tulajdonságot azonosított be)
- A minta idővel nem változik.



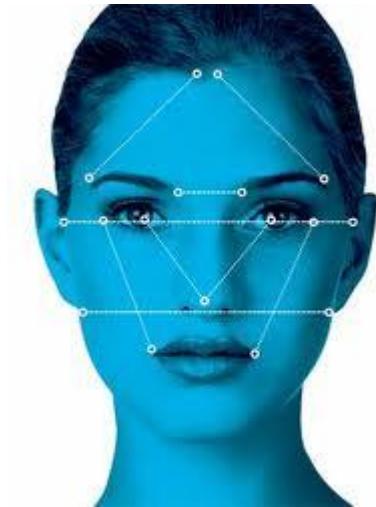
Arc felismerés

- Az azonosítást nehezíti a képminőség (megvilágítás) és az arckifejezés.
- Az arc **nem tartós** biometriai jellemző, öregszik, betegségre is érzékeny, és a nézőponttól erősen függ a geometriája.
- Jó azonosítási módszer: nem igényel együttműködést, nagy adatbázis áll rendelkezésre, messziről is, térfolyamú kamerákkal alkalmazható, eszközei olcsók, társadalmi elfogadottsága jó.



Arc felismerés elemzési módszerei

- **PCA**, (Principal Components Analysis), mely alapvetően a **frontális arckép** elemzését jelenti. (Önmagában legfeljebb 1/1000 a szelektivitása.)
- **LDA** (Linear Discriminant Analysis), **minta osztályok** és **alosztályok** létrehozásával és az azokba történő besorolással is vizsgál.
- **EBGM** (Elastic Bunch Graph Matching) a lineáris karakterisztika vizsgálat által nem megválaszolt **problémákra** próbál megoldást adni, mint pl. megvilágítás, pozíció (nem szemből), vagy arckifejezés). Lényegében a három dimenziós vizsgálatot jelenti.



Kéz geometria

- A kéz körvonalának geometriáját hasonlítja össze az előre felvett mintával. A felvételt olcsó, tömegcikknek számító CCD kamerával készíti.
- A tenyér felülete elég nagy, így viszonylag sok mérhető sajátosságot lehet találni rajta.



Kéz geometria

Az összehasonlításban a sok hasonló analóg sajátosság vesz részt:

- ujjak hossza,
- az ujj-izületek távolsága,
- az ujjak vastagsága,
- a tenyérszélességi adatai, hossza.
- Az adatok kevés byteon tárolhatók, így kicsi a template, és gyors az összehasonlítás.



Véredény azonosítás

- **Infra fénnyel** megvilágított testrészek véredényeinek geometriai struktúráját elemzi, azonosítja. Előnyösen a kézen, a tenyéren és az ujjon.
- A véredények geometriai struktúrájának jellemzői **állandóak** és **egyediek**.
- Hamisításuk szinte **lehetetlen**, mert változtatni rajta nem lehet.
- Az azonosításhoz szükséges képet **csak eleve élő szervezet** ad (a képalkotáshoz kell a véráramlás is az erekben).
- Az infraledes fényforrás fénye behatol a kézfej bőrébe, és másképp verődik vissza az erekről és másképp a többi testszövetről.



Biometriai összehosanlítás

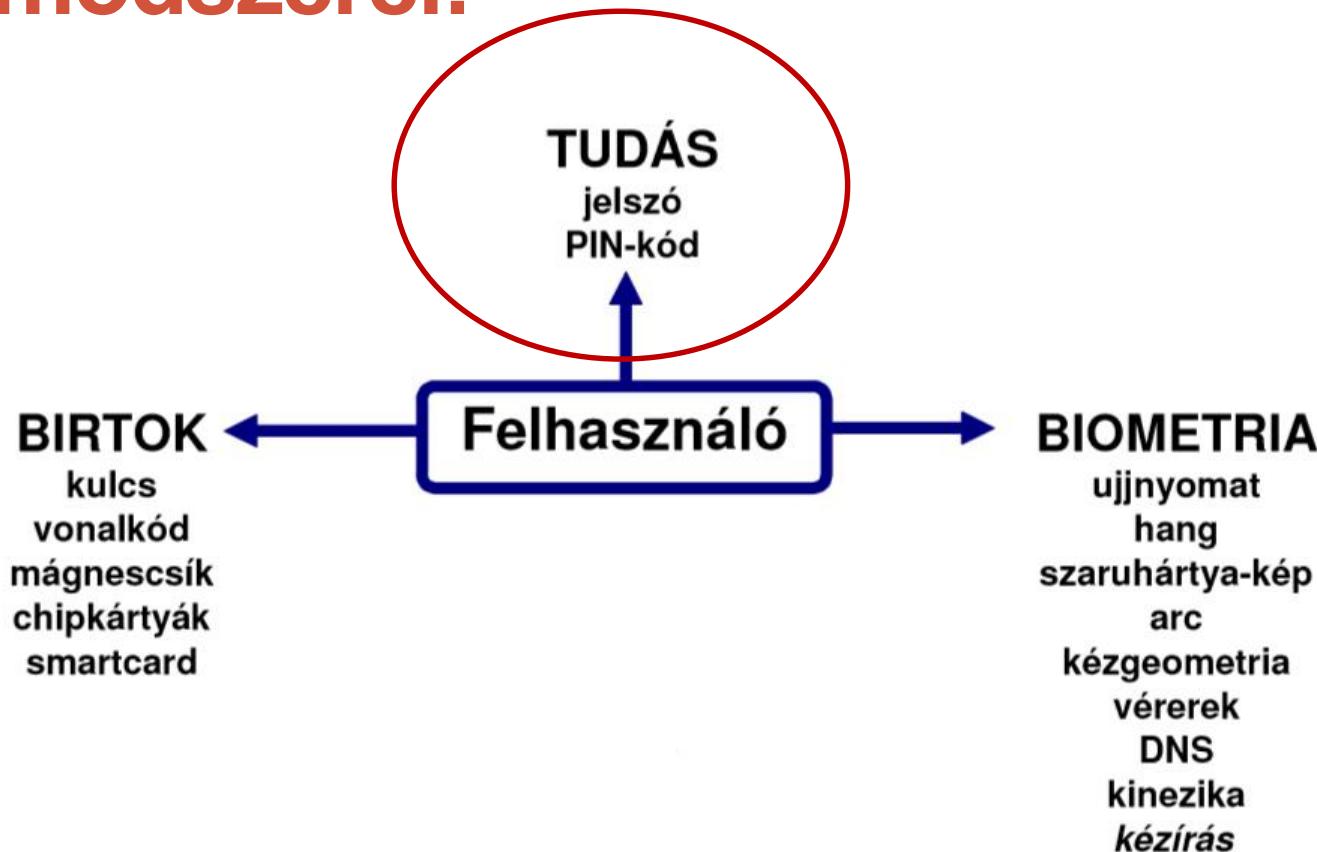
Hasonlítsuk össze néhány biometrikus rendszer FAR mutatóját (hány helyes azonosításra jut egy téves):

Arcfelismerés	2000:1
Hangazonosítás	500:1
Ujjlenyomat azonosítás	1 000 000:1
Íriszvizsgálat	10 000 000:1
Retinaazonosítás	10 000 000:1

Jelszavak szerepe, fontossága



A felhasználó-azonosítás alapmódjai:



Tudás

- Használata egyszerű
- Olcsó
- Észrevétlenül másolható és tulajdonítható el
(nincs visszajelzés ha más birtokába került)
- Erős védelem megjegyezhetősége nehéz

A jelszó minőségek meghatározói

Hosszúság

minden egyes hozzáadott karakter növeli a jelszó értékét; 8 vagy annál több karakter minimum szükséges egy erős jelszóhoz, de 14 vagy annál több lenne az ideális.

Komplexitás

minél többféle karaktert alkalmazunk, annál nehezebb kitalálni a jelszót, használjuk a teljes billentyűzetet.

Könnyű észben tartani, nehéz kitalálni

úgy a legkönnyebb egy jelszót kezelní tartani, ha leírjuk valahová; habár ezt egyáltalán nem javasolt, de ha mégis így járnánk el, akkor rejtsük el biztonságos helyre!



Leggyakoribb jelszavak

- **123456** – Ez a leggyakrabban használt jelszó. És igen, létezik olyan, aki fontos adatok hozzáféréséhez használja ezt a jelszót.
- **jelszó** – A kreativitás csúcsa, amikor valaki ezt a szót választja jelszóként.
- **Fradi, fradi, fradi** – Gyakori, hogy valaki a kedvenc csapatát vagy játékosát választja jelszó gyanánt. Ezt sem túl nehéz kitalálni, ha valaki egy kicsit is ismeri az illetőt.
- **Petike** – Amikor a jelszó az illető keresztnévénak becélése. Még durvább, ha még csak nem is becézi, hanem egyenesen beírja a nevét.
- **0740174156** – A ismerősöm telefonszáma, vagy saját szám.

Leggyakoribb jelszavak

- **asdf** – mindenki más kipróbálja
- **alma** – Vagy angolban a **monkey**. mindenki kedvenc szavai, divatszavak bizonyos körökben.
- **ábécé** – Sorban az ábécé betűi. Ez sem egy nehéz rejtvény.
- **19820906** – Bármennyire is tudják, hogy ez nem egy jó ötlet, fantáziáhiány miatt mégis rengetegen választják a születési dátumukat jelszó gyanánt.
- **szerelmünk neve** – Elsőre lehet, hogy jó ötletnek tűnik, de ezt az információt a neten keresgélve még egy ezer idegen is megszerezheti.

Hogyan védd a jelszavadat?

- **Ne mond el és ne add oda másnak!** Tartsd a jelszavadat távol a családodtól, barátaidtól és a gyerekeidtől, akik esetleg továbbadhatnák másnak. Légy elővigyázatos a jelszó-emlékeztető kérdésekkel: ne válassz olyan kérdést, amely mások által is kitalálható.
- **Vigyázz a leírt vagy mentett jelszavakra!** Ne őrizz jelszavakat fájlokban a számítógépeden, ugyanis itt keresik először. Ne tudd a jelszavadat a pénztárcádban, se a billentyűzet alá.
- **Sose írd meg a jelszavadat e-mailben, és ne válaszolj a jelszavadat elkérő levelekre!** Ha valaki e-mailben kéri el a jelszavadat, akkor szinte bizonyosan valamilyen átverésre, csalásra kell gondolni. Ez érvényes az általad megbízhatónak tartott cégekre/személyekre is, ugyanis a csalók könnyen álcázhatsák magukat más valakinek.

Hogyan védd a jelszavadat?

- **Ne írd be a jelszavadat olyan számítógépen, amelyet nem ismersz!** minden olyan számítógép, amely internetkávészókban, laborokban, osztott rendszereken, konferenciákon, reptereken stb. található nem tekinthető biztonságosnak, mert nem tudhatjuk, milyen szoftverek rögzítik minden billentyűleütésünket. Ne használjuk ezeket a számítógépeket internetes utalásra, e-mailezésre, vagy bármi olyan művelethez, ahol fontos adatokhoz férünk hozzá.
- **Használj több mint egy jelszót!** Legyen különböző jelszavad a különböző webes szolgáltatásokhoz. Gondolj bele, ha az egyik szolgáltatónál kitudódna a jelszavad, akkor azzal mindenhol beléphetnék.

Az erős jelszavak:

- **legalább hét karakterből** állnak.
- kis- és nagybetűket, számokat és a második és a hatodik karakter között egy szimbólumot tartalmaznak.
- **véletlenszerű** karaktersorozatnak tűnnek.
- nem tartalmaznak **ismétlődő** karaktereket.

Az erős jelszavak:

- nem tartalmaznak **egymás után következő** karaktereket, például 1234, abcd vagy qwerty.
- nem tartalmaznak mintákat, témaikat vagy (valamilyen nyelven) **felismerhető** teljes szavakat.
- nem tartalmaznak hasonló betűket **helyettesítő** számokat vagy szimbólumokat, például \$ jelet az S betű helyett, vagy az 1 számot az I karakter helyett, mivel ezek segítik a jelszó kitalálását.
- nem tartalmazhatják az internetre vagy egy hálózatba történő belépéshez használt felhasználói nevének egyetlen részletét sem.

Jelszó használat

Mobil eszközök

- **PIN kód**

Egy négy számjegyből álló kód 10 ezer lehetőséget rejt, azonban a felhasználók 15%-a ebből csupán 10-et használ (1234, 2222, 0000, 1991...).

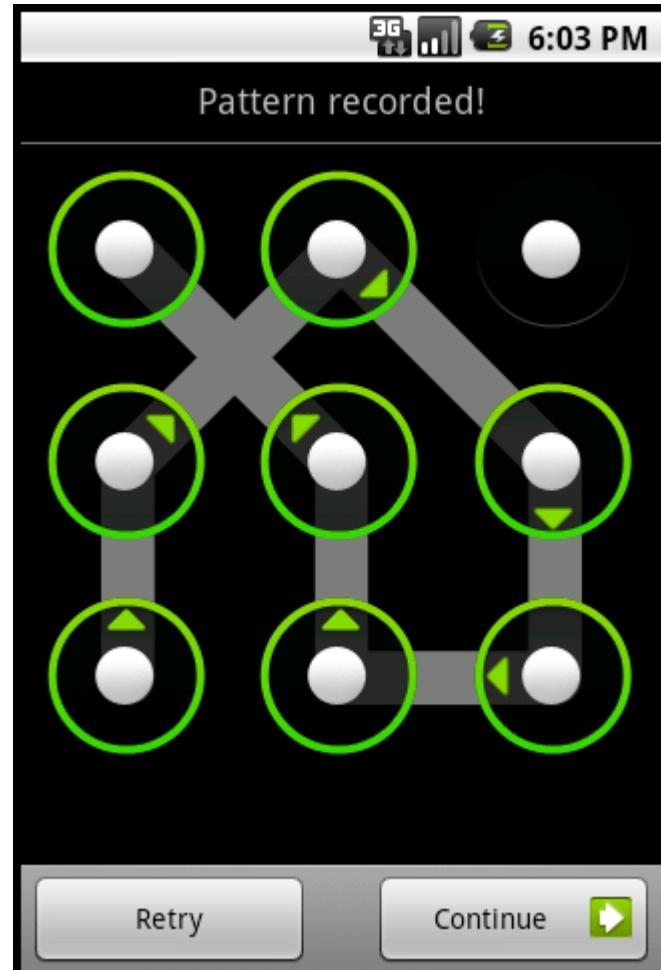


Mobil eszközök

- **Android belépési minta**

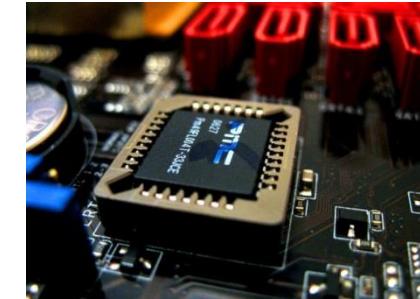
9 pont elhelyezve egy négyzetesen, egy megadott útvonalat kell bejárni az újjunkkal.

Hátrány: Az újaink nyomot hagyhatnak és könnyen megfejtethető a kód



BIOS

A **BIOS** az angol **Basic Input/Output System** kifejezés rövidítése, ami magyarul alapvető bemeneti/kimeneti rendszert jelent, és a számítógép szoftveres és hardveres része közötti interfész megvalósítására szolgál.



- Hardverek ellenőrzése (POST – Power-On Self Test)
- Hardverek vezérlőinek betöltése
- Rendszerkonfiguráció
- Az operációs rendszer merevlemezről, floppyról, SCSI egységről, USBről, hálózati kártyáról vagy egyéb tárolóról való elindítása
- BIOS interfész biztosítása az operációs rendszer számára

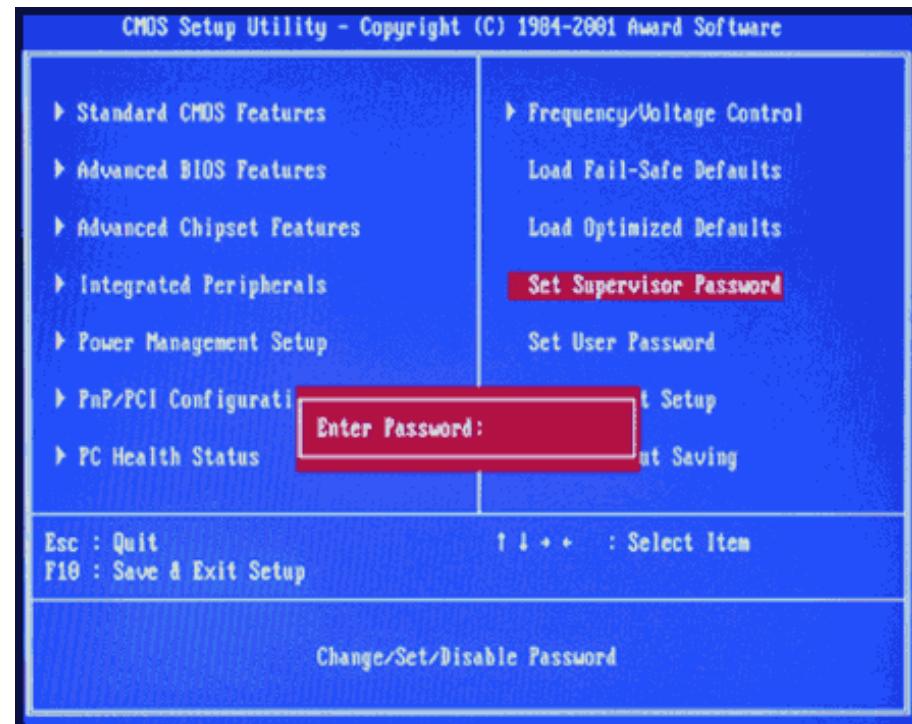
BIOS jelszó

User password

A beállításokhoz fér hozzá

Supervisor password

A beállításokhoz vagy épp a bootoláshoz ad jelszót



BIOS jelszó

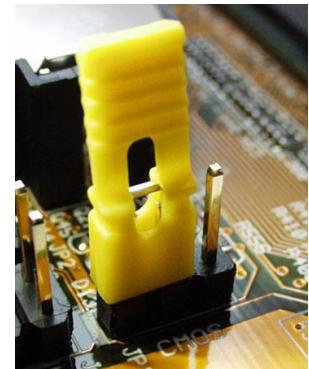
A boot-olás előtt kér jelszót



BIOS jelszó

A jelszó „kiütése” egy ismert egyszerű hardveres művelettel megoldható.

Ezért fontos a számítógépek házainak biztonságos lezárása!!!!

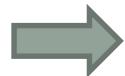


Operációs rendszer belépési jelszava



Operációs rendszer belépési jelszava

Vezérlőpult



Felhasználói fiókok és családbiztonság

Fióktípus módosítása

Családbiztonság beállítása bármely felhasználóhoz



A fiókhöz tartozó név módosítása

A jelszó módosítása

Családbiztonság beállítása

Fióktípus módosítása

Fiók törlése

Másik fiók kezelése



Göcs László - GAMF
Helyi fiók
Jelszóvédett

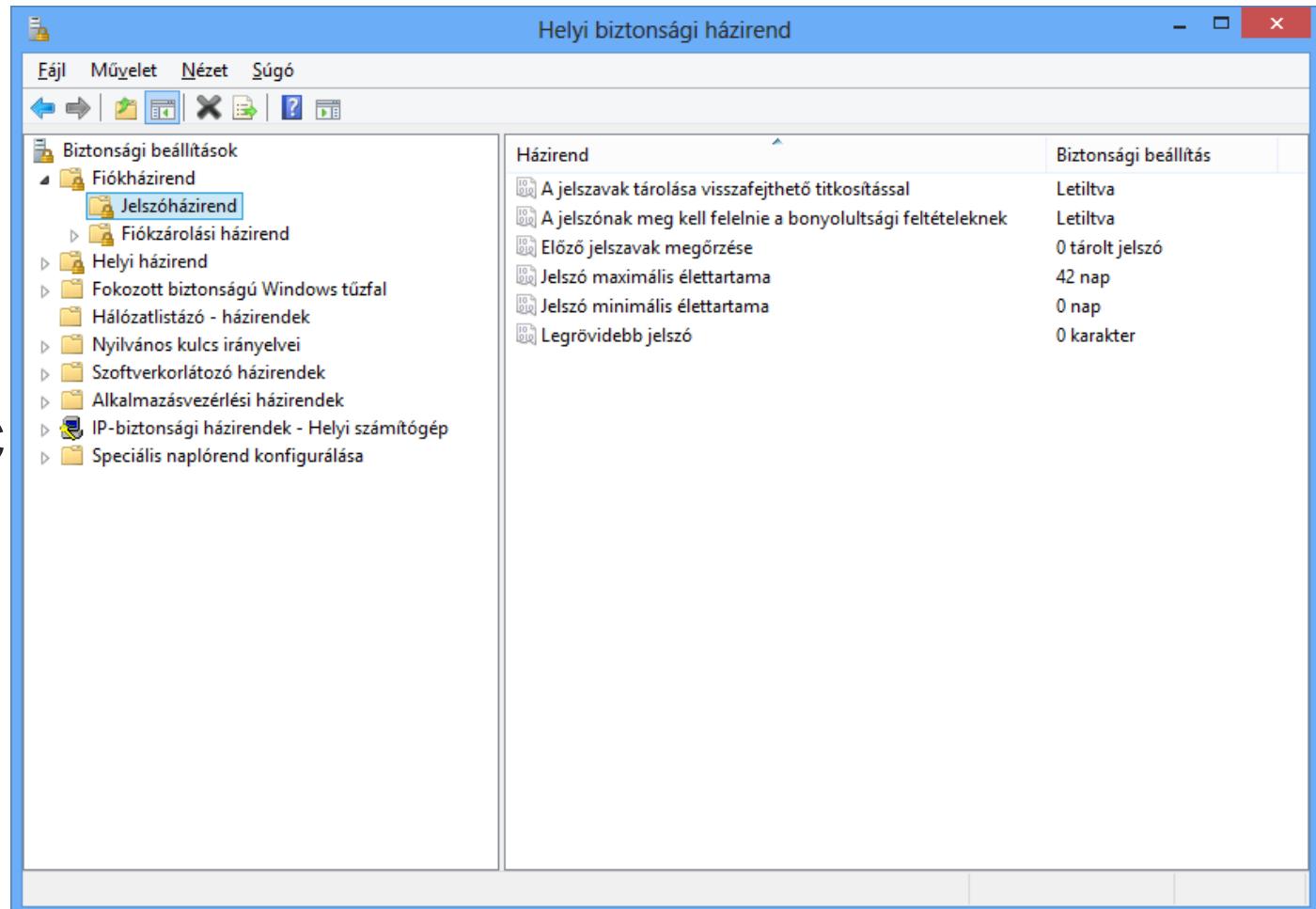
Fontos, hogy a VENDÉG Fiók tiltva legyen



Vendég
Vendégiók letiltva

Helyi biztonsági házirend beállítása

secpol.msc



Jelszó Bonyolultsági feltételek

- **Legrövidebb jelszó:** 1..14 (0-nem kell jelszó)

Meghatározza, hogy a felhasználói fiókokhoz tartozó jelszavaknak legalább hány karakterből kell állniuk.

- **Minimális élettartam:** 1..999 (0-azonnal változtatható)

Ez a biztonsági beállítás azt az időtartamot adja meg (napokban), ameddig egy jelszót kötelező használni, mielőtt a felhasználó megváltoztathatná azt.

Jelszó Bonyolultsági feltételek

- A jelszónak meg kell felelnie a bonyolultsági feltételeknek
 - Nem tartalmazhatják a felhasználói fiók nevét vagy a felhasználó teljes nevének két egymás utáni karaktert meghaladó részletét
 - Legalább hat karakter hosszúságúnak kell lenniük
 - Tartalmazniuk kell az alábbi négy kategória közül legalább háromnak az elemeit:
 - Angol nagybetűs karakterek (A-tól Z-ig)
 - Angol kisbetűs karakterek (a-tól z-ig)
 - Az alapvető 10 számjegy (0-tól 9-ig)
 - Nem betű jellegű karakterek (például !, \$, #, %)

A bonyolultsági feltételeknek a jelszavak létrehozásakor vagy módosításakor kell érvényesülniük.

Jelszó Bonyolultsági feltételek

- **Maximális élettartam:** 1..42 (0-soha nem jár le)

Ez a biztonsági beállítás azt az időtartamot határozza meg (napokban), ameddig egy jelszó használható, mielőtt a rendszer felszólítaná a felhasználót a megváltoztatására

- **Előző jelszavak megőrzése:** 0..24 (alapért.:1)

Ez a biztonsági beállítás meghatározza, hogy hány új egyedi jelszó hozzárendelése szükséges egy felhasználói fiókhoz egy régi jelszó újrafelhasználása előtt. Az értéknek 0 és 24 jelszó között kell lennie.

www.strongpasswordgenerator.co m

Strong Password Generator

Strong Password Generator

Password length:

Punctuation (!, ", £, \$, %, and so on)

Your new password:
6enB] 3?3F1

Remember your new password as:
6 echo november BRAVO] 3 ? 3 FOXTROT 1



www.passwordmeter.com

Test Your Password		Minimum Requirements			
Password:	<input type="text"/>				
Hide:	<input checked="" type="checkbox"/>				
Score:	0%				
Complexity:	Too Short				
Additions					
<input checked="" type="checkbox"/> Number of Characters		Type	Rate	Count	Bonus
<input checked="" type="checkbox"/> Uppercase Letters		Cond/Incr	$+((len-n)*2)$	0	0
<input checked="" type="checkbox"/> Lowercase Letters		Cond/Incr	$+((len-n)*2)$	0	0
<input checked="" type="checkbox"/> Numbers		Cond	$+(n^4)$	0	0
<input checked="" type="checkbox"/> Symbols		Flat	$+(n^6)$	0	0
<input checked="" type="checkbox"/> Middle Numbers or Symbols		Flat	$+(n^2)$	0	0
<input checked="" type="checkbox"/> Requirements		Flat	$+(n^2)$	0	0
Deductions					
<input checked="" type="checkbox"/> Letters Only		Flat	$-n$	0	0
<input checked="" type="checkbox"/> Numbers Only		Flat	$-n$	0	0
<input checked="" type="checkbox"/> Repeat Characters (Case Insensitive)		Comp	-	0	0
<input checked="" type="checkbox"/> Consecutive Uppercase Letters		Flat	$-(n^2)$	0	0
<input checked="" type="checkbox"/> Consecutive Lowercase Letters		Flat	$-(n^2)$	0	0
<input checked="" type="checkbox"/> Consecutive Numbers		Flat	$-(n^2)$	0	0
<input checked="" type="checkbox"/> Sequential Letters (3+)		Flat	$-(n^3)$	0	0
<input checked="" type="checkbox"/> Sequential Numbers (3+)		Flat	$-(n^3)$	0	0
<input checked="" type="checkbox"/> Sequential Symbols (3+)		Flat	$-(n^3)$	0	0
Legend					
✖ Exceptional: Exceeds minimum standards. Additional bonuses are applied.					
✖ Sufficient: Meets minimum standards. Additional bonuses are applied.					
⚠ Warning: Advisory against employing bad practices. Overall score is reduced.					
✖ Failure: Does not meet the minimum standards. Overall score is reduced.					

Jelszó tárolás

- **Fejben tárolva**

Elfelejtődik, vagy ha túl bonyolult akkor nehéz megjegyezni. Több jelszónál még több probléma.

- **Fájlban tárolva (pl XLS)**

Jelszavas védelem a fájl megnyitására!

Fájl jelszavazás

A(z) jelszavak adatai
Z:\jelszavak.xlsx

Engedélyek
A munkafüzetet megnyitásához jelszó szükséges.

Füzetvédelem

Megjelölés véglegesként
Az olvasók értesítése a munkafüzet végleges állapotáról és a munkafüzet írásvédelettel történő védelméről.

Titkosítás jelszóval
Jelszó kérése a munkafüzet megnyitásához.

Aktuális lap védelme
Az aktuális lapon végezhető módosítástípusok szabályozása.

Munkafüzet-szerkezet védelme
A munkafüzet-szerkezet nem kívánt módosításainak (például lapok hozzáadásának) az elkerülése.

Engedélyek korlátozása személyek szerint
Személyek hozzáférésének biztosítása, egyúttal szerkesztési, másolási és nyomtatási engedélyük megszüntetése.

Digitális aláírás hozzáadása
A munkafüzet sértetlenségének biztosítása láthatatlan aláírás hozzáadásával.

Jelszótörő módszerek

- **Brute Force** (nyers erő)

Módszeresen az összes lehetséges jelkombinációt kipróbálja.

- Csak akkor, ha minden más eljárás eredménytelen
- Nagy teljesítményű gépet igényel
- A jelszó hosszától, illetve a használt jelektől függően nagyon sok időre van szükség
- A végeredmény sem biztos

Jelszótörő módszerek

- **Szótár alapú**

A legtöbb felhasználó a hétköznapi nyelvezetből, magánéletéből használja a szavakat, vagy szótöredékeket.

- Lényegesen kevesebb időt igényel
- Nem vezet mindig eredményre

Jelszótörés jogi háttere

Törvénytelen, ha valaki megpróbál engedély nélkül jelszófeltörő program segítségével olyan állományok tartalmához jutni, amelyekhez nincs jogosultsága.

10 karakter kombinációjából alkotott jelszó – 0123456789

Innen látható mennyire rossz ötlet csak számokat használni a jelszóban.

Jelszó		A feltöréshez használt számítógép típusa					
Hossz	Kombinációk	A típus	B típus	C típus	D típus	E típus	F típus
2	100	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
3	1000	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
4	10 000	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
5	100 000	10 mp	azonnal	azonnal	azonnal	azonnal	azonnal
6	1 millió	1½ perc	10 mp	azonnal	azonnal	azonnal	azonnal
7	10 millió	17 perc	1½ perc	1½ perc	azonnal	azonnal	azonnal
8	100 millió	2¾ óra	17 perc	1½ perc	10 mp	azonnal	azonnal
9	1 milliárd	28 óra	2¾ óra	17 perc	1½ perc	10 mp	azonnal

26 karakter kombinációjából alkotott jelszó –

ABCDEFGHIJKLMNPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Most pedig lássuk, mennyire nehéz kitalálni egy olyan jelszót, amelyben csak az angol ábécé kis- vagy nagybetűit találhatóak.

Jelszó		A feltöréshez használt számítógép típusa					
Hossz	Kombinációk	A típus	B típus	C típus	D típus	E típus	F típus
2	676	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
3	17 576	2 mp	azonnal	azonnal	azonnal	azonnal	azonnal
4	456 976	46 mp	5 mp	azonnal	azonnal	azonnal	azonnal
5	11,8 millió	20 perc	2 perc	12 mp	azonnal	azonnal	azonnal
6	308,9 millió	8½ óra	51½ perc	5 perc	30 mp	3 mp	azonnal
7	8 billió	9 nap	22 óra	2¼ óra	13 perc	1¼ perc	8 mp
8	200 billió	242 nap	24 nap	2½ nap	348 perc	35 perc	3½ perc
9	5,4 trilió	17 év	21 hónap	63 nap	6¼ nap	15 óra	1¼ óra
10	141 trilió	447 év	45 év	4½ év	163 nap	16 nap	39¼ óra
12	95 quadrillió	302 603 év	30 260 év	3026 év	302 év	30 év	3 év
15	1,6 sextillió	53 trillió év	532 millió év	53 millió év	5 millió év	531 855 év	53 185 év
20	19,9 octillió	63 quadrillió év	6,3 quadrillió év	631 trillió év	63,1 trillió év	6,3 trillió év	631 billió év

36 karakter kombinációjából alkotott jelszó –

ABCDEFGHIJKLMNPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789

A teljes angol ábécé (csak kis vagy csak nagybetűk) és a számok együttes használatával az eredmény csak egy picit jobb.

Jelszó		A feltöréshez használt számítógép típusa					
Hossz	Kombinációk	A típus	B típus	C típus	D típus	E típus	F típus
2	1 296	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
3	46 656	4 mp	azonnal	azonnal	azonnal	azonnal	azonnal
4	1,6 millió	2½ perc	16 mp	1½ mp	azonnal	azonnal	azonnal
5	60,4 millió	1½ óra	10 perc	1 perc	azonnal	azonnal	azonnal

52 karakter kombinációjából alkotott jelszó –

AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz

Most nézzük mi történik, ha vegyítjük a kis és nagybetűket.

Jelszó		A feltöréshez használt számítógép típusa					
Hossz	Kombináció	A típus	B típus	C típus	D típus	E típus	F típus
2	2704	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
3	140 608	14 mp	2 mp	azonnal	azonnal	azonnal	azonnal
4	7,3 millió	12½ perc	1¼ perc	8 mp	azonnal	azonnal	azonnal
5	380 millió	10½ óra	1 óra	6 perc	38 mp	4 mp	azonnal
6	19 billió	23 nap	2¼ nap	5½ óra	33 perc	3¼ perc	19 mp
7	1 trilió	3¼ év	119 nap	12 nap	28½ óra	3 óra	7 perc
8	53 trilió	169½ év	17 év	1½ év	62 nap	6 nap	15 óra
9	2,7 quadrillió	8815 év	881 év	88 év	9 év	322 nap	32 nap

**96 karakter kombinációjából alkotott jelszó – !#\$%&'()^+,-./;=>?@[{}]^_`{|}~
0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz**

Kis- és nagybetűk, számok, valamint néhány gyakori szimbólum használata a jelszóban.

Jelszó		A feltöréshez használt számítógép típusa					
Hossz	Kombinációk	A típus	B típus	C típus	D típus	E típus	F típus
2	9 216	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
3	884 736	88½ mp	9 mp	azonnal	azonnal	azonnal	azonnal
4	85 millió	2¼ óra	14 perc	1½ perc	8½ mp	azonnal	azonnal
5	8 billió	9½ nap	22½ óra	2¼ óra	13½ perc	1¼ perc	8 mp
6	782 billió	2½ év	90 nap	9 nap	22 óra	2 óra	13 perc
7	75 trillió	238 év	24 év	2½ év	87 nap	8½ nap	20 óra
8	7,2 quadrillió	22 875 év	2287 év	229 év	23 év	2¼ év	83½ nap

Példák

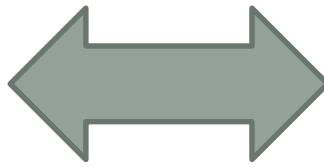
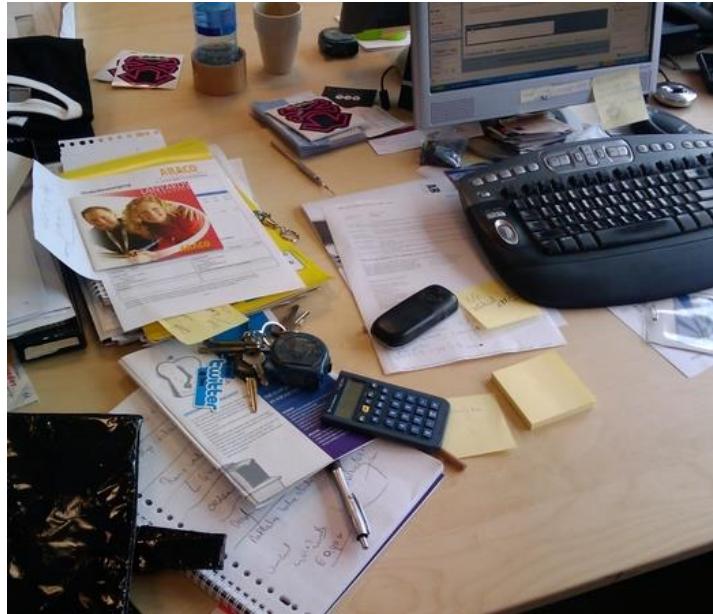
Most pedig lássunk néhány konkrét példát jelszavakra!

Jelszó		A feltöréshez használt számítógép típusa					
Jelszó	Kombinációk	A típus	B típus	C típus	D típus	E típus	F típus
Iacika	308,9 millió	8½ óra	51½ perc	5 perc	30 mp	3 mp	azonnal
P3terke	3,5 trillió	11 év	1 év	41 nap	4 nap	10 óra	58 perc
B33r&Mug	7,2 quadrillió	22 875 év	2287 év	229 év	23 év	2¼ év	83½ nap

A teszteken használt számítógép-típusok jellemzői

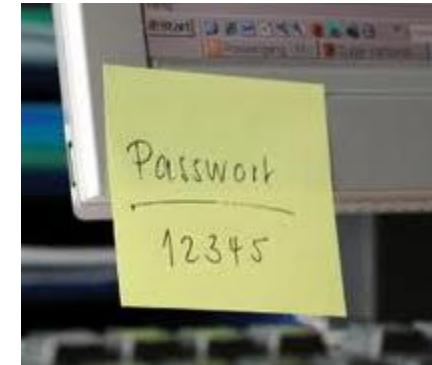
- **A típus** (10 000 jelszó/mp) – Tipikusan egy Microsoft Office jelszó feltörésére használható Pentium 100-as gép.
- **B típus** (100 000 jelszó/mp) – Tipikusan egy Windows Password Cache (.pwl) jelszó feltörésére használható Pentium 100-as gép.
- **C típus** (1 000 000 jelszó/mp) – Tipikusan egy ZIP vagy ARJ jelszó feltörésére használható Pentium 100-as gép.
- **D típus** (10 000 000 jelszó/mp) – Gyors PC, duplamagos processzorral.
- **E típus** (100 000 000 jelszó/mp) – Munkaállomás vagy több PC együttműködve.
- **F típus** (1 000 000 000 jelszó/mp) – Tipikus közepes vagy nagyméretű elosztott számítógép, szuperszámítógép.

Clean Desk Policy (CDP) - Tiszta Asztal Politika



Clean Desk Policy (CDP) - Tiszta Asztal Politika

- Belépési azonosító és jelszó
 - Papíralapon (Post-It, regisztrációs lap kinyomtatva)
 - Hardverre írva (monitor, billentyűzet)
- Személyes információk
 - Amiből a jelszavak megfejhetőek, kitalálhatóak
- Otthoni/Céges dokumentumok, leírások
- Mobiltelefon



Erős jelszó példa

- **Találj ki egy mondatot, amit könnyen észben tudsz tartani!**

Például: A *kisfiám Lacika nemsoká két éves.*

- **Alakítsd a mondatot jelszóvá!**

Használd minden szó első betűjét, hogy egy betűsorozatot gyárts: ***akInke***

- **Bonyolítsd a szöveget egy kis fantáziával!**

Vegyítsd a kis- és nagybetűket, használj számokat a betűk helyett. Például: *AkLn2e*

- **Vonj be speciális karaktereket!**

Használj olyan szimbólumokat, amelyek hasonlítanak bizonyos betűkhöz: ***Ak#L?n%2e!***

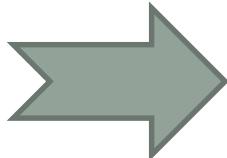
- **Tartsd titokban a jelszavadat!**

KeePass



Ingyenes, nyílt forráskódú jelszó menedzselő program.
Minden jelszót 1 adatbázisban lehet tárolni mesterkulcs segítségével.

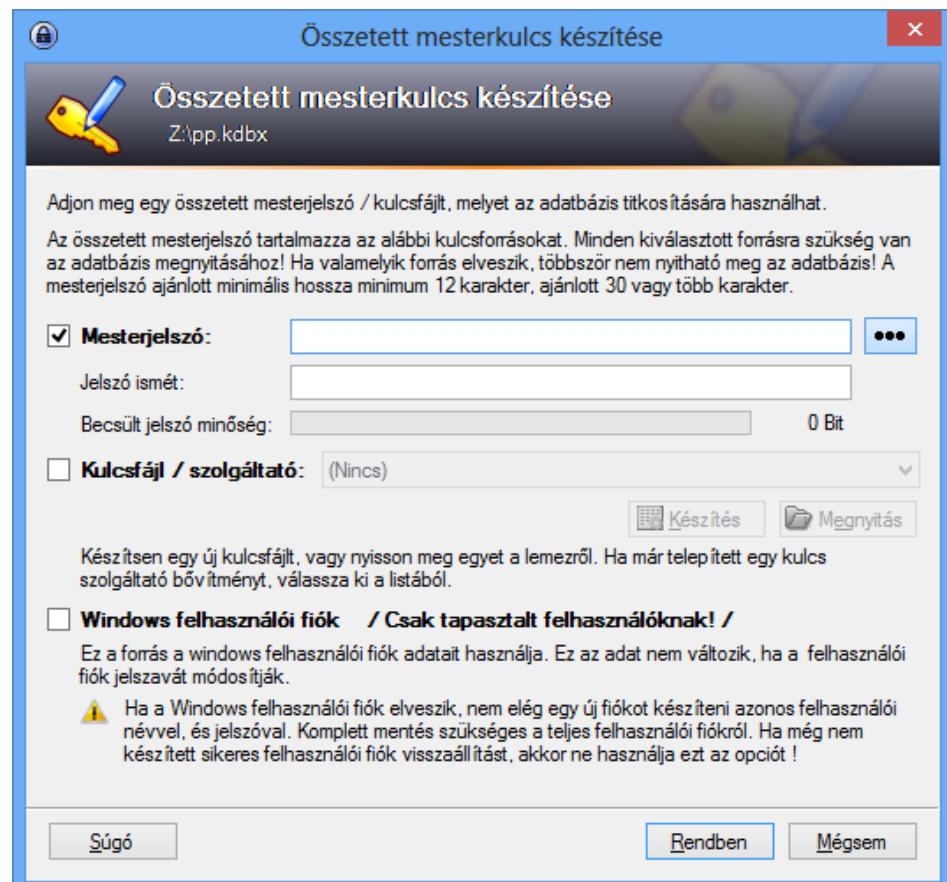
1 db Mesterkulcs



- Felhasználói jelszavak
- Email account-ok
- Windows hálózati belépések
- Webes jelszavak

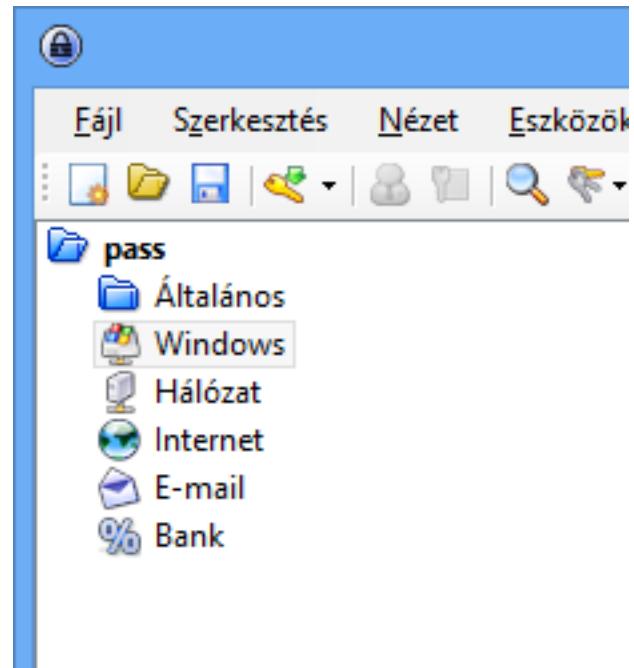
KeePass

Új adatbázis létrehozáshoz
egy **mesterkulcs**
szükséges



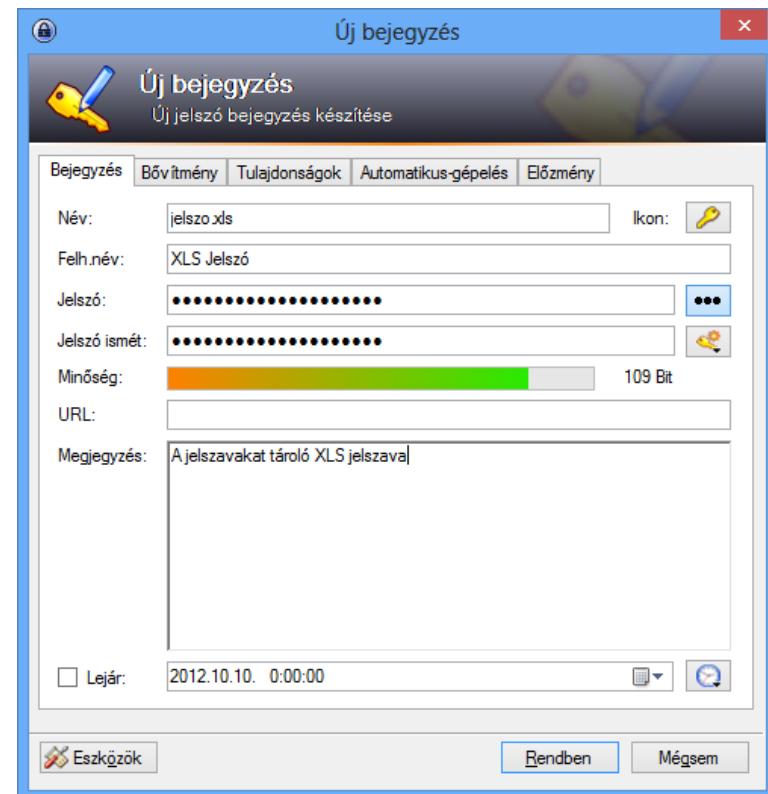
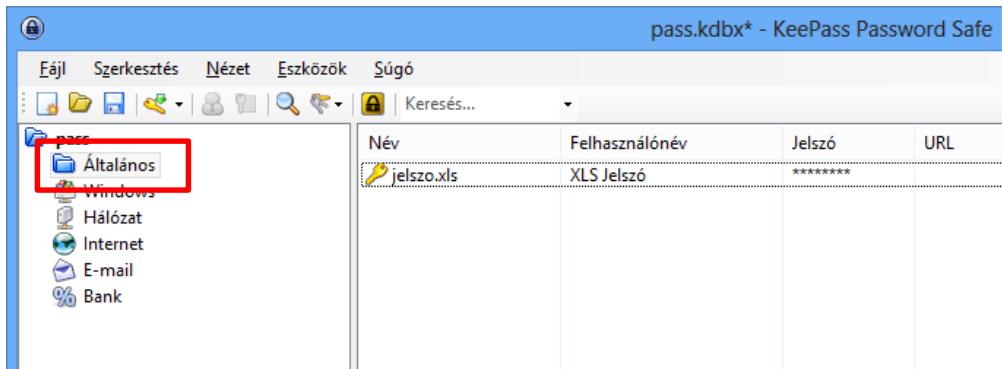
KeePass

Különböző téma körökhez lehet jelszavakat rendelni.



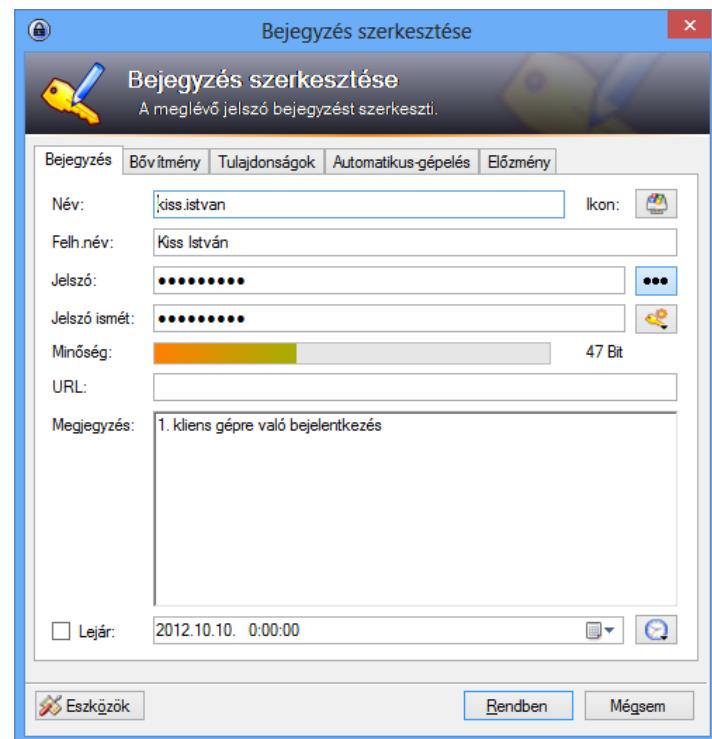
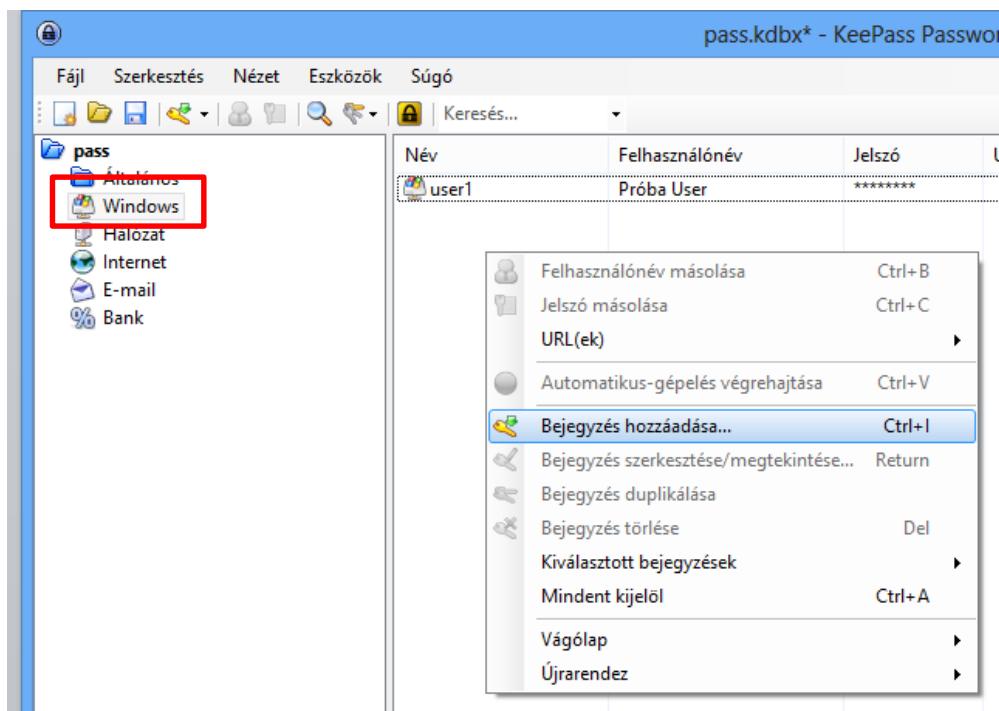
KeePass

Új bejegyzés létrehozása (Általános)



KeePass

Új bejegyzés létrehozása (Windows)



Vállalati biztonság

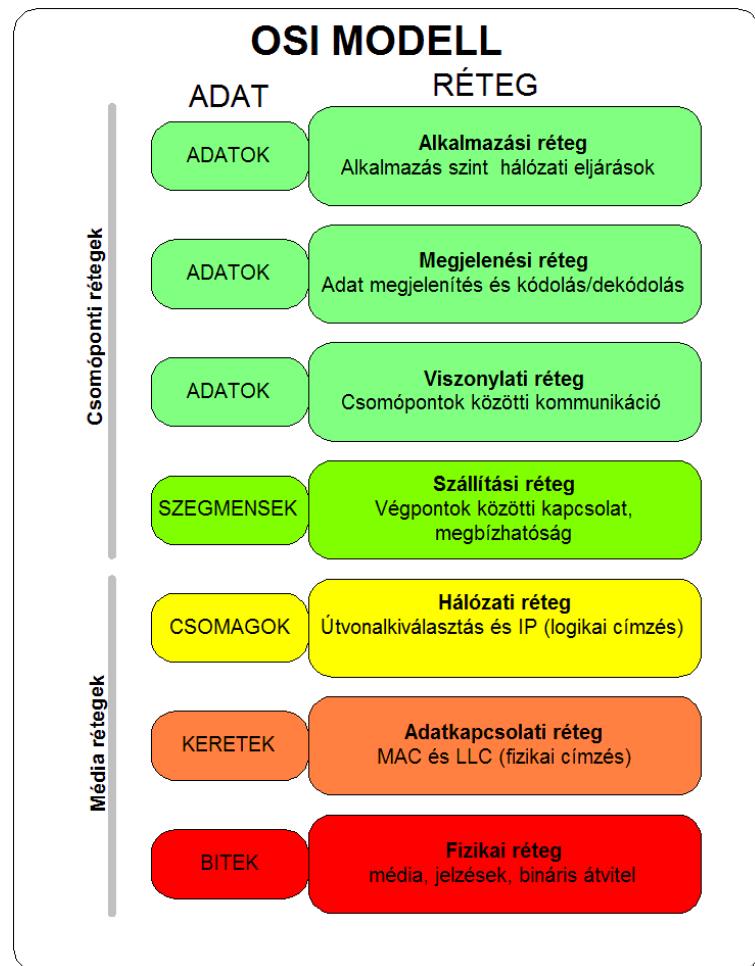


Előkészítés

- Az információbiztonsági osztály meghatározása (A,F,K)
- Rendelkezésre állás kalibrálása

OSI réteg védelme

- minden egyes rétegnél megvan a meghatározott védelme.
- Maximális védelem kialakítása minden rétegen.



Fizikai réteg védelme

- Itt történik a jeltovábbítás (Kábelezés, csatlakozás).
- A kábeleken lévő jeleket, biteket (1 0 0 1 1 0 1) kódolási eljárással és órajel segítségével továbbítják.

Fizikai réteg védelme

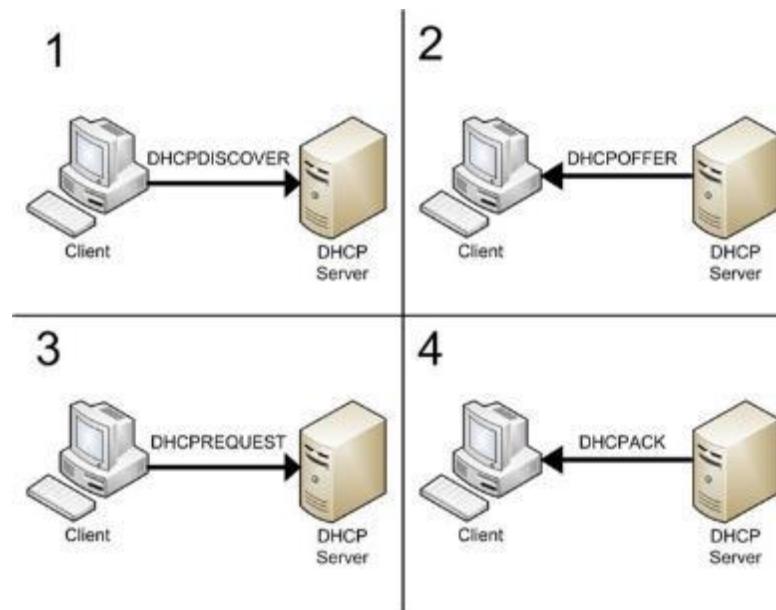
- A fizikai réteg védelme a helyiségek, berendezések biztonsága, hozzáférhetősége.
 - Tápellátás megszüntetése (szerver leállás)
 - Kábel megsértése (bejövő internet, helyi hálózat megszakítása)



Beléptetés, biztonságtechnikai felügyelet.

IP címek védelme

- **DHCP** (*Dynamic Host Configuration Protocol*).
Dinamikus IP cím kiosztás a hálózaton.



IP címek védelme

- Alhálózatok kialakítása (Maszkolási technika)

Jelöl	Címek	Alhálózati maszk	Alhálózati maszk binárisan
/22	4x256	255.255.252.0	11111111.11111111.11111100.00000000
/23	2x256	255.255.254.0	11111111.11111111.11111110.00000000
/24	1x256	255.255.255.0	11111111.11111111.11111111.00000000
/25	128x1	255.255.255.128	11111111.11111111.11111111.10000000
/26	64x1	255.255.255.192	11111111.11111111.11111111.11000000
/27	32x1	255.255.255.224	11111111.11111111.11111111.11100000
/28	16x1	255.255.255.240	11111111.11111111.11111111.11110000
/29	8x1	255.255.255.248	11111111.11111111.11111111.11111000
/30	4x1	255.255.255.252	11111111.11111111.11111111.11111100
/31	2x1	255.255.255.254	11111111.11111111.11111111.11111110
/32	1x1	255.255.255.255	11111111.11111111.11111111.11111111

IP címek védelme

- **MAC-cím** (*Media Access Control*) cím alapján történő IP cím kiosztás.

Egy **hexadecimális** számsorozat, amellyel még a **gyártás során** látják el a hálózati kártyákat.

A hálózati kártyák újlenyomata.

(parancssori utasítással: getmac)

A9-AF-23-C8-F2-2B -> 192.168.1.25

Menedzselhető switchek

- A switch portjait külön menedzselhetjük
 - VLAN-ok létrehozása
 - Port tiltások (80-as http port)
 - Port Sec



Vezeték nélküli kommunikáció (WiFi)

- **SSID**

Maga az azonosító szöveges és alfa numerikus karakterekből állhat és **maximum 32 karakter** hosszú lehet. Az egy hálózathoz tartozó eszközöknek ugyanazt az SSID-t kell használniuk.

- Fontos a jó elnevezés, mert a „default” beállításokból megfejthető a Router konfigurációs elérése.
- Az SSID elrejtése

TP_link_0234war -> 192.168.1.x -> admin

Vezeték nélküli titkosítás

A **Wired Equivalent Privacy (WEP)** = Vezetékessel Egyenértékű (Biztonságú) Hálózat mára már egy korszerűtlen algoritmus az IEEE 802.11-ben megfogalmazott vezeték nélküli hálózatok titkosítására.



Nem biztonságos, könnyen feltörhető.
Régi eszközök miatt még néhol használatos.

Vezeték nélküli titkosítás

A **Wi-Fi Protected Access** (WPA és WPA2) a vezeték nélküli rendszereknek egy a **WEP**-nél biztonságosabb protokollja.

A WPA tartalmazza az **IEEE 802.11i** szabvány főbb szabályait, és egy átmeneti megoldásnak szánták, amíg a 802.11i szabványt véglegesítik.

A **WPA2** a teljes szabványt tartalmazza, de emiatt nem működik néhány régebbi hálózat kártyával sem. Mindkét megoldás megfelelő biztonságot nyújt, két jelentős problémával:

Vezeték nélküli titkosítás

- Vagy a WPA-nak, vagy WPA2-nek engedélyezettnek kell lennie a WEP-en kívül. De a telepítések és beállítások során inkább a WEP van bekapcsolva alapértelmezettként, mint az elsődleges biztonsági protokoll.
- A „Personal” (WPA-PSK) módban, amit valószínűleg a legtöbben választanak otthon és kishivatali környezetben, a megadandó **jelszónak hosszabbnak** kell lennie, mint a jellegzetes 6-8 karakter, amit az átlagfelhasználók általában még elfogadhatónak tartanak.

MUNKACSOPORT / TARTOMÁNY

- 4-7 kliens gép

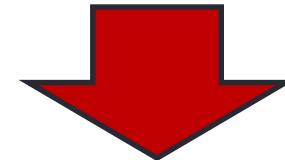


Munkacsoport

- 7-10 gépnél több állomás



Tartomány



KÖZPONTOSÍTOTT
FELÜGYELET

Központosított menedzsment

Központi beléptetés a kliens gépekre

- A Kliens gépeket Tartományba „fűzni”
- Az Active Directory –ban a felhasználók kezelése
- Központilag, 1 szerveren történik a menedzsment



Próba Eduárd PE. - tulajdonságok

A következő tagja	Behívás	Kömyezet	Munkamenetek	Távvezérés
Távoli asztali szolgáltatók profilja	Személyes virtuális asztal	COM+		
Általános	Cím	Fiók	Profil	Telefonszámok
				Szervezet

Próba Eduárd PE.

Vezetéknév: Próba Monogram: PE
Utónév: Eduárd
Megjelenítendő név: Próba Eduárd PE.
Leírás:
Iroda:
Telefonszám: Egyéb...
E-mail:
Weblap: Egyéb...

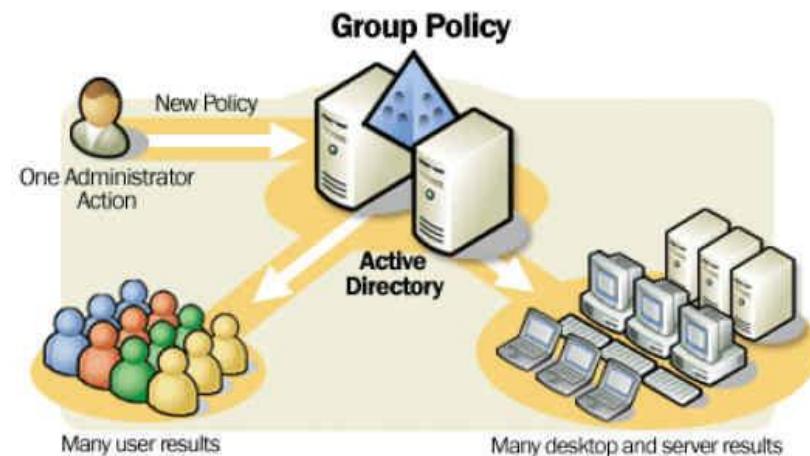
OK Mégse Alkalmaz Súgó

Egy nagy ADATBÁZIS a vállalatról

Központosított menedzsment

Központilag kezelt házirend (Group Policy)

- Felhasználóra vagy Kliens gépre történő beállítások
- Tiltások, engedélyezések



Központosított menedzsment

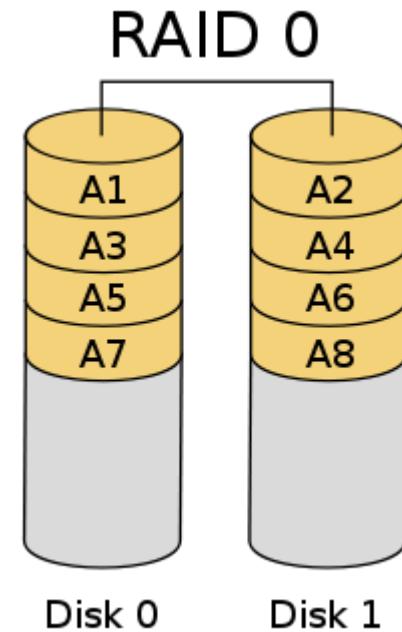
Adat Biztonság, adatvédelem

- RAID technológia
- Időzített biztonsági mentés (Backup)
- Replikáció
- Tükrözés

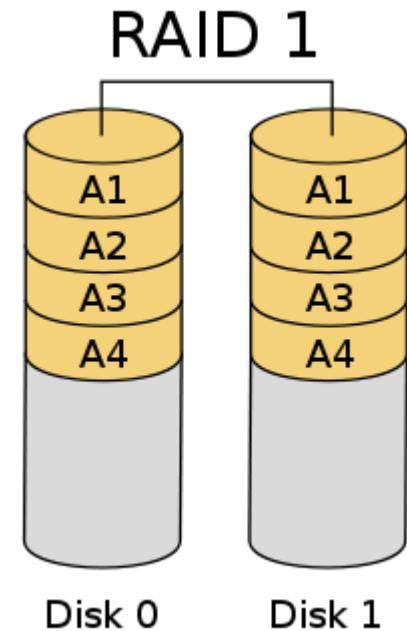
RAID

- A RAID technológia alapja az **adatok elosztása vagy replikálása több fizikailag független merevlemezen**, egy logikai lemez hozva létre.
- minden RAID szint alapjában véve vagy az adatbiztonság növelését vagy az adatátviteli sebesség növelését szolgálja.
- A RAID-ben eredetileg 5 szintet definiáltak (RAID 1-től RAID 5-ig). Az egyes szintek nem a fejlődési, illetve minőségi sorrendet tükrözik, hanem egyszerűen a különböző megoldásokat.

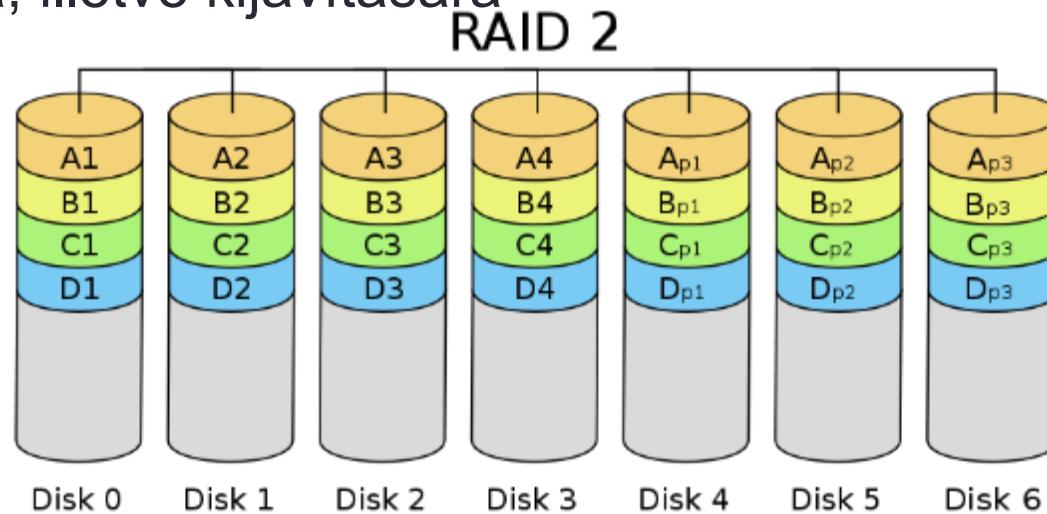
- A **RAID 0** az egyes lemezek egyszerű összefűzését jelenti, viszont semmilyen redundanciát nem ad, így nem biztosít hibatűrést, azaz **egyetlen meghajtó meghibásodása az egész tömb hibáját okozza.**
- A megoldás lehetővé teszi különböző kapacitású lemezek összekapcsolását is, viszont a nagyobb kapacitású lemezeken is csak a **tömb legkisebb kapacitású lemezének méretét** lehet használni (tehát egy 120 GB és egy 100 GB méretű lemez összefűzésekor mindössze egy 200 GB-os logikai meghajtót fogunk kapni, a 120 GB-os lemezen 20 GB szabad terület marad, amit más célokra természetesen felhasználhatunk).



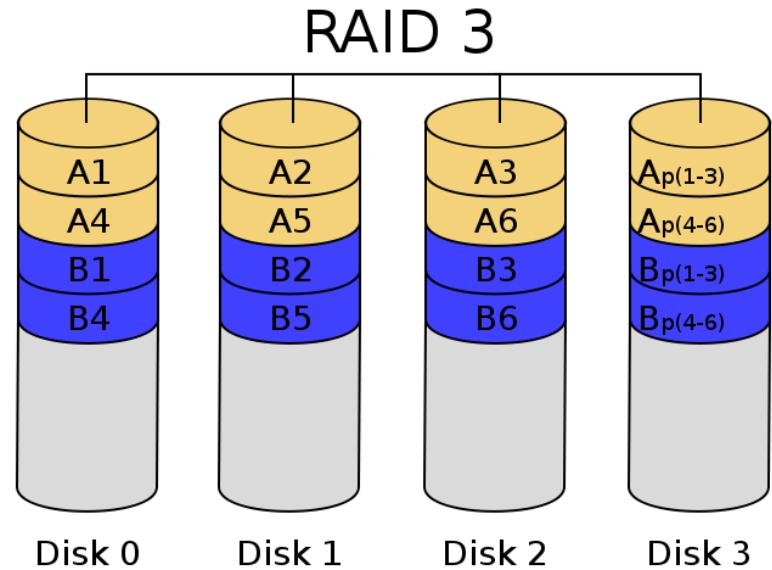
- A **RAID 1** eljárás alapja az adatok tükrözése (disk mirroring), azaz az információk **egyidejű tárolása** a tömb minden elemén.
- A kapott logikai lemez a tömb legkisebb elemével lesz egyenlő méretű. Az adatok **olvasása párhuzamosan történik** a diszkekről, felgyorsítván az olvasás sebességét; az **írás normál sebességgel**, párhuzamosan történik a meghajtókon.
- Az eljárás igen jó hibavédelmet biztosít, bármely meghajtó mehibásodása esetén folytatódhat a működés. A RAID 1 önmagában nem használja a csíkokra bontás módszerét.



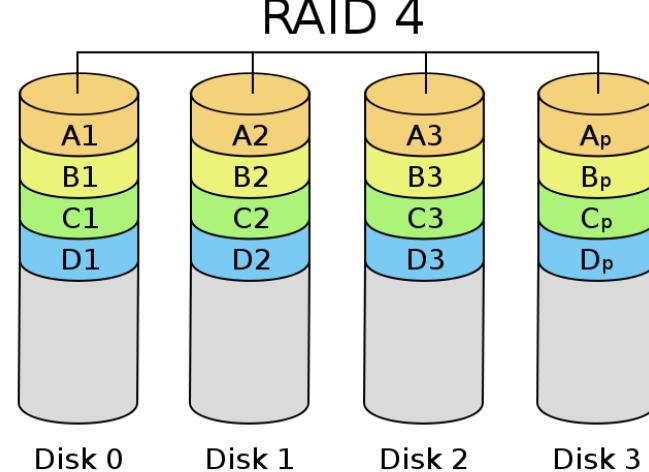
- A RAID 2 használja a csíkokra bontás módszerét, emellett egyes meghajtókat **hibajavító kód** (ECC: Error Correcting Code) tárolására tartanak fenn. A hibajavító kód lényege, hogy az adatbitekből valamelyen matematikai művelet segítségével redundáns biteket képeznek.
 - Ezen meghajtók egy-egy csíkjában a különböző lemezeken azonos pozícióban elhelyezkedő csíkokból képzett hibajavító kódot tárolnak. A módszer esetleges lemezhiba esetén képes annak detektálására, illetve kijavítására.



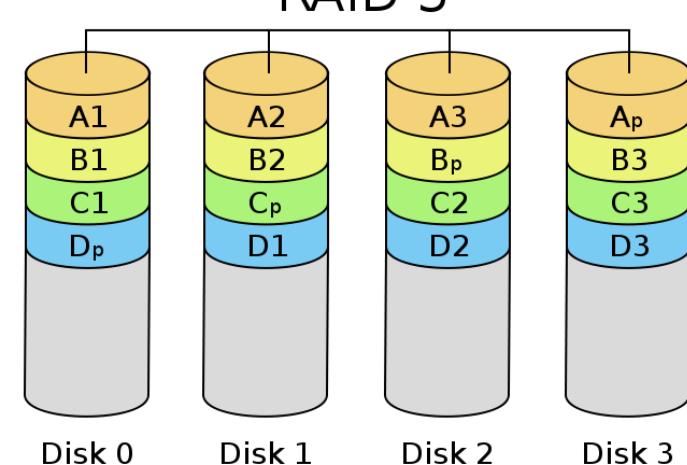
- A RAID 3 felépítése hasonlít a RAID 2-re, viszont nem a teljes hibajavító kód, hanem csak egy lemeznyi paritásinformáció tárolódik. Egy adott paritáscsík a különböző lemezekben azonos pozícióban elhelyezkedő csíkokból XOR művelet segítségével kapható meg.
- A rendszerben egy meghajtó kiesése nem okoz problémát, mivel a rajta lévő információ a többi meghajtó (a paritást tároló meghajtót is beleértve) XOR-aként megkapható.



- A **RAID 4** felépítése a RAID 3-mal megegyezik. Az egyetlen különbség, hogy itt **nagyméretű csíkokat definiálnak**, így egy rekord egy meghajtón helyezkedik el, lehetővé téve egyszerre több (különböző meghajtókon elhelyezkedő) rekord párhuzamos írását, illetve olvasását (multi-user mode).
- Problémát okoz viszont, hogy a paritás-meghajtó adott csíkját **minden egyes íráskor frissíteni kell** (plusz egy olvasás és írás), aminek következtében párhuzamos íráskor a paritásmeghajtó a rendszer szűk keresztmetszetévé válik. Ezenkívül valamely meghajtó kiesése esetén a rendszer olvasási teljesítménye is lecsökken, a paritás-meghajtó jelentette szűk keresztmetszet miatt.

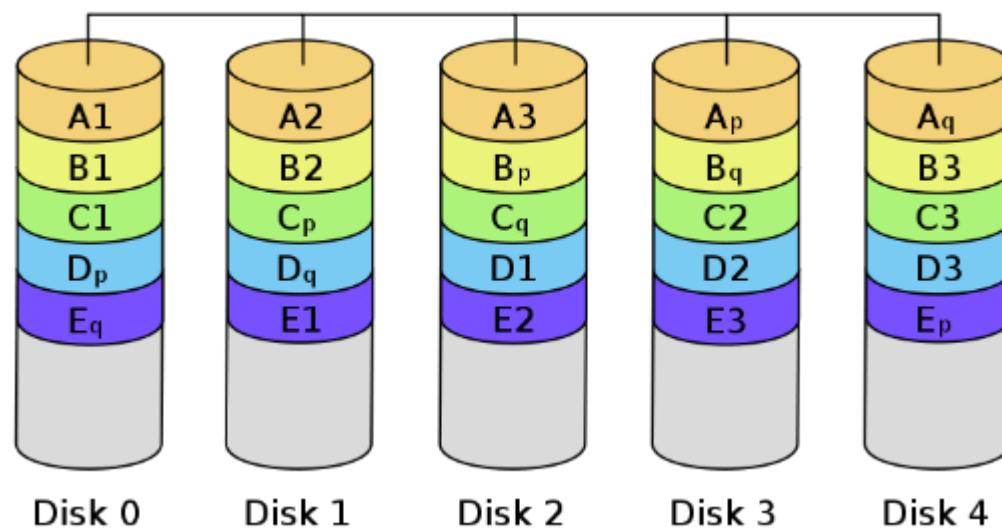


- A **RAID 5** a paritás információt nem egy kitüntetett meghajtón, hanem „**körbeforgó paritás**” (rotating parity) használatával, egyenletesen az összes meghajtón elosztva tárolja, kiküszöbölvén a paritás-meghajtó jelentette szűk keresztmetszetet. Minimális meghajtószám: 3. Mind az írási, mind az olvasási műveletek párhuzamosan végezhetőek.
- Egy meghajtó mehibásodása esetén az adatok sértetlenül visszaolvashatóak, a hibás meghajtó adatait a vezérlő a többi meghajtóról ki tudja számolni. A csíkméret változtatható; kis méretű csíkok esetén a RAID 3-hoz hasonló működést, míg nagy méretű csíkok alkalmazása esetén a RAID 4-hez hasonló működést kapunk. A hibás meghajtót ajánlott azonnal cserélni, mert két meghajtó mehibásodása esetén az adatok elvesznek!

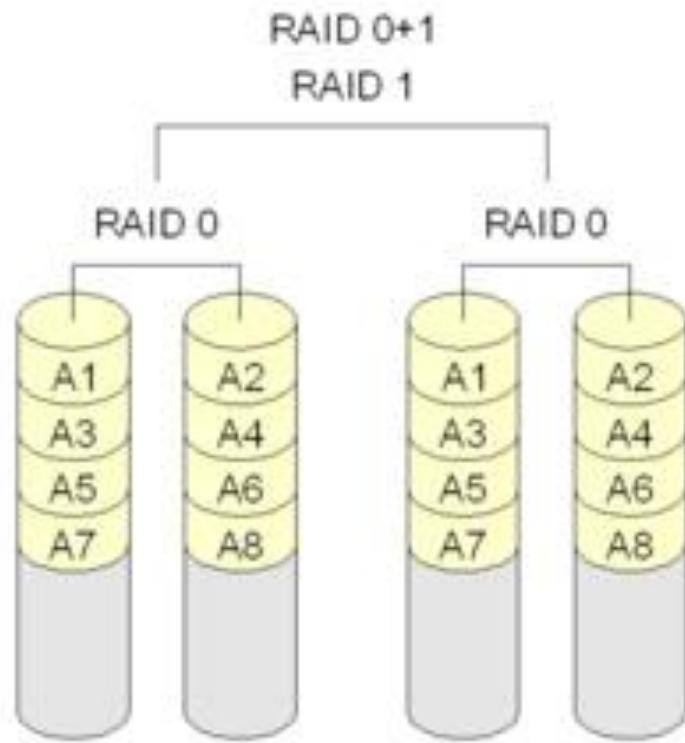


- A **RAID 6** tekinthető a RAID 5 kibővítésének.
- Itt nemcsak soronként, hanem oszloponként is kiszámítják a paritást. A módszer segítségével **kétszeres meghajtó meghibásodás** is kiküszöbölhetővé válik. A paritáscsíkokat itt is az egyes meghajtók között, egyenletesen elosztva tárolják, de ezek természetesen kétszer annyi helyet foglalnak el, mint a RAID 5 esetében.

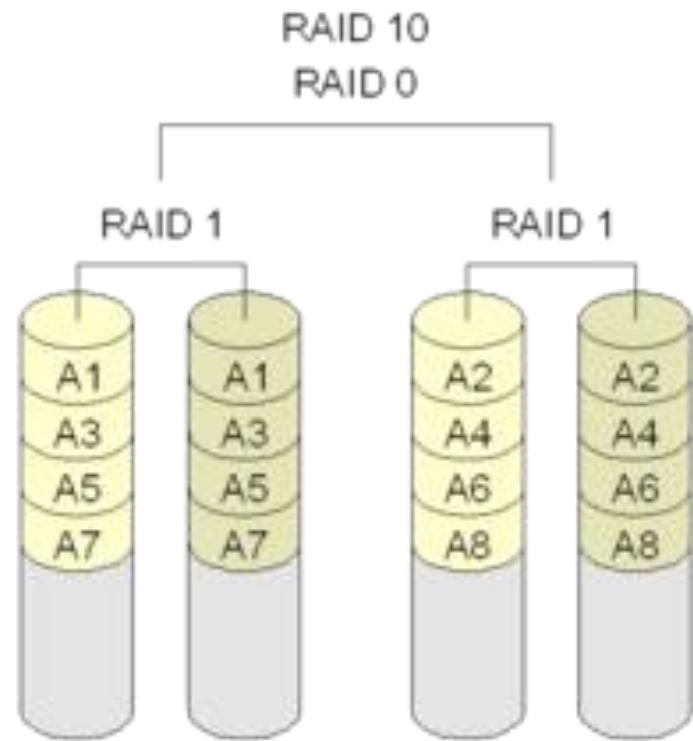
RAID 6



- Ez egy olyan hibrid megoldás, amelyben a RAID 0 által hordozott sebességet a RAID 1-et jellemző biztonsággal ötvözhetjük.
- Hátránya, hogy **minimálisan 4 eszközre** van szükségünk, melyekből 1-1-et összefűzve, majd páronként tükrözve építhetjük fel a tömbünket, ezért a teljes kinyerhető kapacitásnak mindössze a felét tudjuk használni.
- Mivel a tükrözés (RAID 1) a két összefűzött (RAID 0) tömbre épül, ezért egy lemez meghibásodása esetén az egyik összefűzött tömb mindenkorábban kiesik, így a tükrözés is megszűnik.

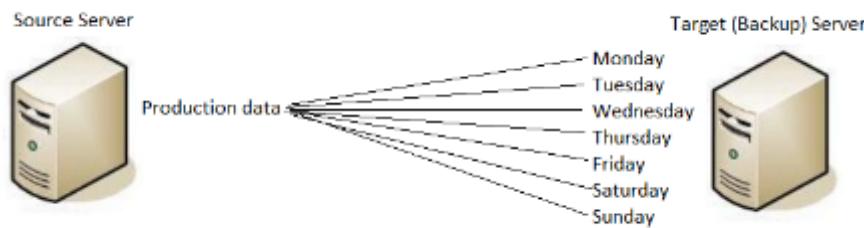


- Hasonlít a RAID 01 megoldáshoz, annyi különbséggel, hogy itt a lemezeket **először tükrözzük**, majd a kapott tömböt fűzzük össze.
- Ez biztonság szempontjából jobb megoldás, mint a RAID 01, mivel egy diszk kiesése csak az adott tükrözött tömböt érinti, a rá épült RAID 0-t nem; sebességben pedig megegyezik vele.



Biztonsági mentés

- A szerver beállításairól, megosztott mappákról időzített mentés.



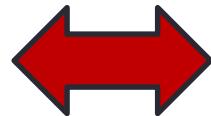
Biztonsági mentés típusok

- **Normál:** minden kiválasztott állományról az A attr.-tól függetlenül. Az A attr. törlődik.
- **Másolat:** minden kiválasztott állományról az A attr.-tól függetlenül. Az A attr. *nem* törlődik.
- **Különbségi:** a kiválasztottak közül csak az A attr.-al rendelkezőket. Az A attr. *nem* törlődik.
- **Növekményes:** a kiválasztottak közül csak az A attr.-al rendelkezőket. Az A attr. törlődik.
- **Napi:** a kiválasztottak közül csak azokat, amelyek módosultak a mentés napján. Az A attr. *nem* törlődik.

Biztonsági mentési terv példa

Mikor?	Milyen?	Mit ment?
Hétfő	Növekményes	Vasárnap óta változottakat
Kedd	Növekményes	Hétfő óta változottakat
Szerda	Növekményes	Kedd óta változottakat
Csütörtök	Növekményes	Szerda óta változottakat
Péntek	Növekményes	Csütörtök óta változottakat
Szombat	Növekményes	Péntek óta változottakat
Vasárnap	Normál	Mindent

SZERVERSZOBA KIALAKÍTÁSA



SZERVERSZOBA

- Biztonságtechnikai-, beléptető-, vagyonvédelmi rendszerek



SZERVERSZOBA

- Szünetmentes tápellátó berendezések (rendelkezésre állás)



SZERVERSZOBA

- Túlfeszültség-, és zavarvédelmi megoldások



SZERVERSZOBA

- Érintésvédelem

Az érintésvédelem üzemszerűen feszültség alatt nem álló, de meghibásodás esetén feszültség alá kerülő vezető részek érintéséből származó balesetek elkerülésére szolgáló műszaki intézkedések összessége.



SZERVERSZOBA

- Füstérzékelők, tűzérzékelő- és oltóközpontok, Tűzoltórendszerek



- **Szén-dioxid**

Oltóanyaga élelmiszeripari tisztaságú szén-dioxid, elsődlegesen éghető folyadékok és gázok tüzeinél oltására alkalmas. De alkalmas **feszültség alatti** berendezések oltására is. A Széndioxid térfogat-kitekercsben megállítja az égést, azaz lecsökkenti az égéshez szükséges Oxigén mennyiséget.



SZERVERSZOBA

- Páratajtalom, hőmérséklet



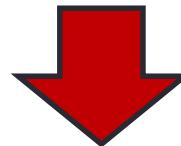
Adatmegsemmisítés

Fájl törlése

- Lemezterület felszabadítása
- Az ismétlődő vagy szükségtelen adatok eltávolítása
- Érzékeny információk elérhetetlenné tévése mások számára

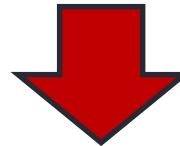
Véletlen eltávolítás érdekében

- Később bebizonyosodik hogy fontos az adat



Biztonsági másolat

- Nem törlődik azonnal, hanem áthelyezésre kerül



Lomtár



Véletlen eltávolítás érdekében

- MS-DOS korszakban **UNDELETE**

Akkor lehetett alkalmazni ,ha más egyéb fájl nem használta fel a blokkot.

- Fájlok csak olvasási joggal rendelkezzenek **Read Only**

Hardveres adatmegsemmisítés

A legegyszerűbb megoldás, ha egy kalapáccsal az adathordozót megsemmisítjük, de vannak erre intelligensebb megoldások. Erre a célra kifejlesztett HDD fizikai megsemmisítő alkalmas. Vannak olyan berendezések, amelyek az adathordozót teljes mértékben bezúzzák újrahasznosítás céljából.



PD-4

HDD Fizikai megsemmisítő

Célja fizikailag tönkretenni a merevlemezt. Nagynyomású fej egysége tengely irányban fejt ki hatását, így megrepeszte a burkolatot, meghajlítva vagy épp eltörve az adattárolást szolgáló lemezeket, megsemmisítve az író/olvasó fejet, és minden belső elektronikát.

Ha magát az adathordozót nem akarjuk megsemmisíteni, csak az adatokat törölni, akkor mágneses törlést kell alkalmazni.



HD-2 Hard Drive Degausser Merevlemeztörlő berendezés

Nagy erejű mágneses teret gerjesztve, a törlendő mágneses adathordozókon található minden információ véglegesen a semmivé lesz

<http://garner-products.com>

Szoftveres adatmegsemmisítés

Az operációs rendszerünkben történő adattörlés vagy akár egy partíció formázása nem jelent kellő biztonságot adatunk törlésére. Egyszerű szoftverekkel visszanyerhetőek az adtok. Ahhoz hogy vélegesen törölni tudjuk az adatainkat, pontosabban hogy ne lehessen helyreállítani a törölt adatokat, bizonyos algoritmikus eljárásokat kell alkalmazni az adathordozón.

- Pseudorandom Data
- First/Last 16kB
- British HMG IS5
- Russian GOST P50739-95
- US Army AR380-19
- US AirForce 5020
- British HMG IS5
- German VSITR
- Schneier
- RCMP TSSIT OPS-II
- US DoD 5220.22-M (8-306./E, C&E)
- Gutmann (35)

- **Guttmann-35**
 - **Pass 1 - 35:** Writes a random character
- **DoD 5220.22-M**
 - **Pass 1:** Writes a zero and verifies the write
 - **Pass 2:** Writes a one and verifies the write
 - **Pass 3:** Writes a random character and verifies the write

- **RCMP TSSIT OPS-II**
 - **Pass 1:** Writes a zero
 - **Pass 2:** Writes one
 - **Pass 3:** Writes a zero
 - **Pass 4:** Writes one
 - **Pass 5:** Writes a zero
 - **Pass 6:** Writes one
 - **Pass 7:** Writes a random character and verifies the write

- **Schneier -7**
 - **Pass 1:** Writes a one
 - **Pass 2:** Writes a zero
 - **Pass 3:** Writes a random character
 - **Pass 4:** Writes a random character
 - **Pass 5:** Writes a random character
 - **Pass 6:** Writes a random character
 - **Pass 7:** Writes a random character

- **German VSITR -7**

- **Pass 1:** Writes a zero
- **Pass 2:** Writes a one
- **Pass 3:** Writes a zero
- **Pass 4:** Writes a one
- **Pass 5:** Writes a zero
- **Pass 6:** Writes a one
- **Pass 7:** Writes a random character

- **British HMG IS5 -3**
 - **Pass 1:** Writes a zero
 - **Pass 2:** Writes a one
 - **Pass 3:** Writes a random character and verifies the write
- **US AirForce 5020 -3**
 - **Pass 1:** Writes a zero
 - **Pass 2:** Writes a one
 - **Pass 3:** Writes a random character and verifies the write

- **US Army AR380-19 -3**
 - **Pass 1:** Writes a random character
 - **Pass 2:** Writes a specified character (i.e. zero)
 - **Pass 3:** Writes the complement of the specified character (i.e. one) and verifies the write
- **Russian GOST P50739-95 -2**
 - **Pass 1:** Writes a zero
 - **Pass 2:** Writes a random character

- **British HMG IS5 -1**
 - **Pass 1:** Writes a zero
 - **Pass 2:** Writes a one
 - **Pass 3:** Writes a random character and verifies the write

TÁMADÁSOK ÉS VÉDEKEZÉSEK AZ IT RENSZEREKBEN

2016. május. 13. 15:33 · MTI · VILÁG

Berlin Oroszországot vádolja egy tavalyi hackertámadásért

Egy az orosz állam által irányított csoport állhatott egy tavalyi Bundestag elleni kibertámadás mögött a német hírszerzés szerint.

2016. április. 02. 21:06 · MTI · ITTHON

Bakondi: Még támadás alatt áll a kormányzati hálózat

Szombaton este azt mondta Orbán Viktor belbiztonsági tanácsadója, hogy nem tudja, ki támadta meg a kormányzati honlapokat, de a támadás még tart.

2016. április. 27. 14:01 · hvg.hu · TECH

Vírust találtak az egyik német atomerőműben

Két rosszindulatú programot is talált az üzemeltető a bajor létesítményben. Konkrét veszély most nincs, de innentől már tényleg csak egy lépés, hogy legyen.

Kína beismerte, hogy vannak kiberháborús kommandói

Kína mindeddig visszautasította azokat a vádakat, hogy amerikai cégeknél kémkedne vagy képes lenne kibertámadásokra, most azonban egy amerikai kutató szerintegy hivatalos kiadványban ismerte be, folytat ilyen tevékenységet.

2014. február. 12. 23:10 · MTI · TECH

Megtámadtak egy magyar számítógépyárat, lopott mobilokat akartak legalizálni

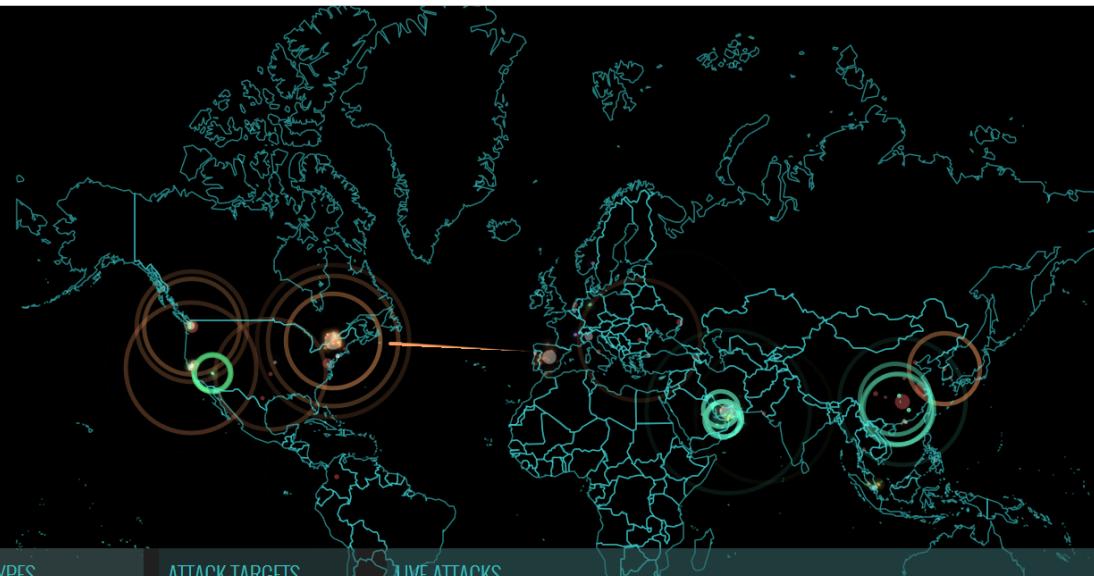
Öt ember, köztük két román állampolgár ellen emelt vádat a Zalaegerszegi Járású Ügyészség, amiért a Flextronics zalaegerszegi gyárában behatoltak a cégek számítógépes rendszerébe, majd azon keresztül a kanadai cégpontba, hogy egyebek mellett lopott mobiltelefonokat legalizáljanak.

TOP 10 (Balabit felmérés)

- Social engineering (például adathalászat)
- Kompromittált hozzáférések (gyenge jelszó)
- Web alapú támadások (SQL/command injection)
- Kliens oldali támadások (például dokumentum olvasó, web böngésző)
- Szerverfrissítésekre írt exploit-ok (például OpenSSL, Heartbleed)
- Nem menedzselt privát eszközök (például rossz BYOD szabályzat)
- Fizikai behatolás
- Árnyék informatika
- Külső szolgáltatók igénybevétele (kiszervezett infrastruktúra)
- Felhő infrastruktúrába kihelyezett adatok megszerzése (például IAAS, PAAS)



NORSE



ATTACK ORIGINS

#	COUNTRY	#	PORT	SERVICE TYPE
95	China	57	23	telnet
67	United States	47	25	smtp
7	Ukraine	42	8080	http-alt
6	Netherlands	12	5900	rbf
3	Moldova	10	3389	ms-wbt-server
3	South Korea	5	50864	xsan-filesystem
3	Colombia	5	3306	mysql
2	Turkey	4	445	microsoft-ds
2	Romania	3	22	ssh

ATTACK TYPES

#	COUNTRY	#	PORT	SERVICE TYPE
92	United States	57	23	telnet

ATTACK TARGETS

#	COUNTRY	TIMESTAMP
92	United States	16:57:49.768
51	United Arab Emirates	16:57:49.767
36	Spain	16:57:49.766
11	Italy	16:57:49.763
5	Singapore	16:57:49.349
1	Saudi Arabia	16:57:49.021
1	Portugal	16:57:49.017
1	Norway	16:57:48.718
	Hong Kong	16:57:48.532

LIVE ATTACKS

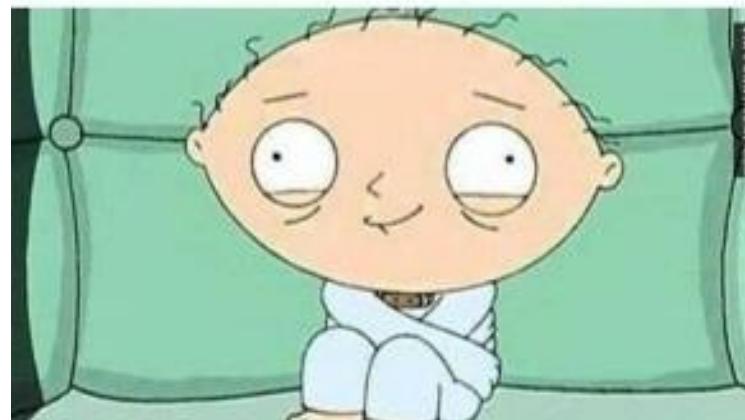
#	COUNTRY	TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
92	United States	16:57:49.768	Chinanet Hubel Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
51	United Arab Emirates	16:57:49.767	Chinanet Hubel Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
36	Spain	16:57:49.766	Chinanet Hubel Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
11	Italy	16:57:49.763	Krnic	211.36.143.216	Anyang-Dong, KR	De Kalb Junction, US	telnet	23
5	Singapore	16:57:49.349	Microsoft Corporation	207.46.100.251	Redmond, US	De Kalb Junction, US	smtp	25
1	Saudi Arabia	16:57:49.021	Microsoft Corporation	157.56.111.245	Redmond, US	De Kalb Junction, US	smtp	25
1	Portugal	16:57:49.017	Cox Communications	70.183.54.227	Tulsa, US	De Kalb Junction, US	telnet	23
1	Norway	16:57:48.718	Romtelecom Data Network	92.82.237.58	Bucharest, RO	San Francisco, US	telnet	23
	Hong Kong	16:57:48.532	Chinanet Hubel Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080

[HOME](#)[EXPLORE](#)[WHY NORSE?](#)

<http://map.norsecorp.com/#/>

Legbiztosabb módszer a védekezésre?

LIFE WITHOUT
INTERNET



Tűzfal

- A tűzfal **két vagy több hálózat között** helyezkedik el és ellenőrzi a közöttük zajló forgalmat, valamint segíti a jogosulatlan hozzáférés elleni védelmet.
- A tűzfal az egyik leghatékonyabb olyan biztonsági eszköz, mely a **belső hálózati felhasználók külső veszélyektől való megvédésére** rendelkezésre áll.
- A tűzfal-termékek akár többféle szűrést is támogathatnak.
- Ezen kívül a tűzfalak gyakran hálózati címfordítást (Network Address Translation, **NAT**) is végeznek.

Tűzfal

- Csomagszűrés - az IP vagy MAC-cím alapján akadályozza meg vagy engedélyezi a hozzáférést.
- Alkalmazás/Webhely szűrés - Az alkalmazás alapján akadályozza meg vagy engedélyezi a hozzáférést.
- A webhelyek, egy meghatározott weblap URL címe vagy kulcsszavak alapján blokkolhatók.

SPI

- Állapot-alapú csomagvizsgálat (Stateful Packet Inspection, SPI) - A bejövő csomagok csak a belső hálózat állomásairól kezdeményezett kérések válaszcsomagjai lehetnek.
- A **nem kívánatos csomagokat** külön engedély hiányában kiszűri. Az SPI felismerhet és kiszűrhet bizonyos típusú támadásokat is (pl.: DoS).

Tűzfal megvalósításai

- Eszköz-alapú tűzfal
- Kiszolgáló-alapú tűzfal
- Integrált tűzfal
- Személyes tűzfal

Eszköz alapú tűzfal

- Egy biztonsági készülékként ismert **célhardverbe** van beépítve.
- Nem rendelkezik perifériával és merevlemezzel.
- **Gyors**abban képes a forgalmat megvizsgálni.



Kiszolgáló alapú tűzfal

- Egy tűzfalalkalmazás, amely valamilyen hálózati operációs rendszer alatt fut (Network OS: UNIX, Windows, Novell).
- SPI tűzfalat és az IP cím vagy alkalmazás alapú hozzáférést kombinálja.
- Kevésbé biztonságos az általános célú OS biztonsági hiányosságai miatt.



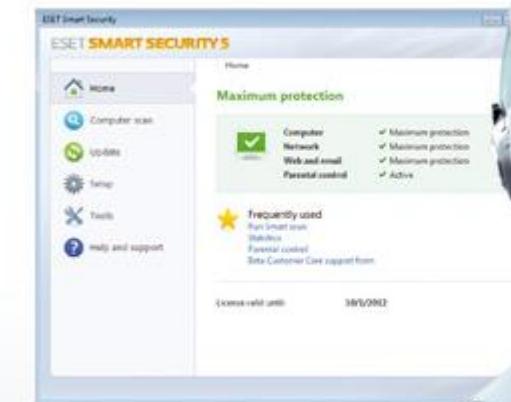
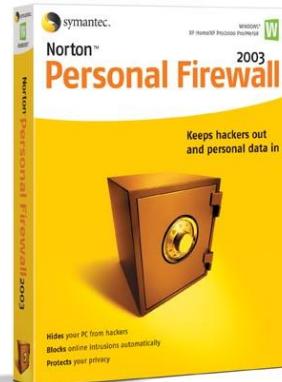
Integrált tűzfal

- Egy meglevő eszköz (pl.: forgalomirányító) tűzfalszolgáltatással kiegészítve.
- Az integrált forgalomirányítók rendelkeznek alapvető tűzfal szolgáltatással (csomag, alkalmazás, webhely szűrés)
- A nagy teljesítményű forgalomirányítók is rendelkeznek tűzfal szolgáltatással.



Személyes tűzfal

- A **munkaállomáson** helyezkedik el, nem LAN megvalósításra terveztek.
- Lehet az operációs rendszer **beépített** szolgáltatása, vagy származhat **külső** gyártótól is.



Személyes tűzfal

- A személyes tűzfal külön álló asztali rendszerek védelmére kifejlesztett alkalmazás, mely **hálózati csatoló** és az azt igénybe vevő **operációs rendszer**, illetve annak alkalmazásai között a beállított szabályok szerint vizsgálja a hálózati forgalmat.

Személyes tűzfal

- A személyes tűzfalak általában háromféle feladatot látnak el:
 - A **beérkező** forgalmat blokkolni tudják szolgáltatás/program, port és protokoll (TCP/UDP) szerint.
 - A **kimenő** forgalmat blokkolni tudják program, port és protokoll szerint.
 - A bejövő forgalomra általában valamilyen **tartalom szerinti szűrést** is végeznek (scriptek, cookie-k, ... stb blokkolása).

Személyes tűzfal

- A személyes tűzfalak, egy "tanulási" folyamattal jutnak el ahhoz, hogy mely kommunikációt engedélyezzenek, ezért konfigurálásuk lényegében nem szükséges.
- minden egyes új kommunikáció kezdeményezésekor megkérdezik, hogy azt engedélyezzük-e? (permit - deny) És ha igen, hogy ezt általános szabályként akarjuk-e, emlékezzék-e erre?
- Amennyiben ezt általános szabályként akarjuk, többet nem kérdeznek arra a programra. Így az elindulás után sokat kérdez(het)nek, de utána már csendben vannak.
- A konfigurálásuk ezért meglehetősen egyszerű. Mindegyiknél van mód a szabályok későbbi megtekintésére és azokat akkor módosíthatjuk is.

A tűzfal használata

- A tűzfalaknak mint határkészüléknek, a belső hálózat (intranet) és az Internet közé helyezésével minden **kifelé** és **befelé** irányuló **Internet forgalom** megfigyelhető és ellenőrizhető.
- Mindemellett néhány külső ügyfélnek szüksége lehet a belső erőforrások használatára. Ennek biztosítására lehet kiépíteni a **demilitarizált zónát (DMZ)**.

Demilitarizált zónát (DMZ)

- Azt a területet írja le, amely a belső és külső hálózat (internet) **között** helyezkedik el.
- Ide kerülhetnek a webkiszolgálók, FTP kiszolgálók, SMTP kiszolgálók, DNS kiszolgálók.
- Mind a belső, mind a külső felhasználók számára **hozzáférhető**.
- A belső hálózatot, a DMZ-t és a külső hálózatot egy vagy több tűzfallal különítik el.

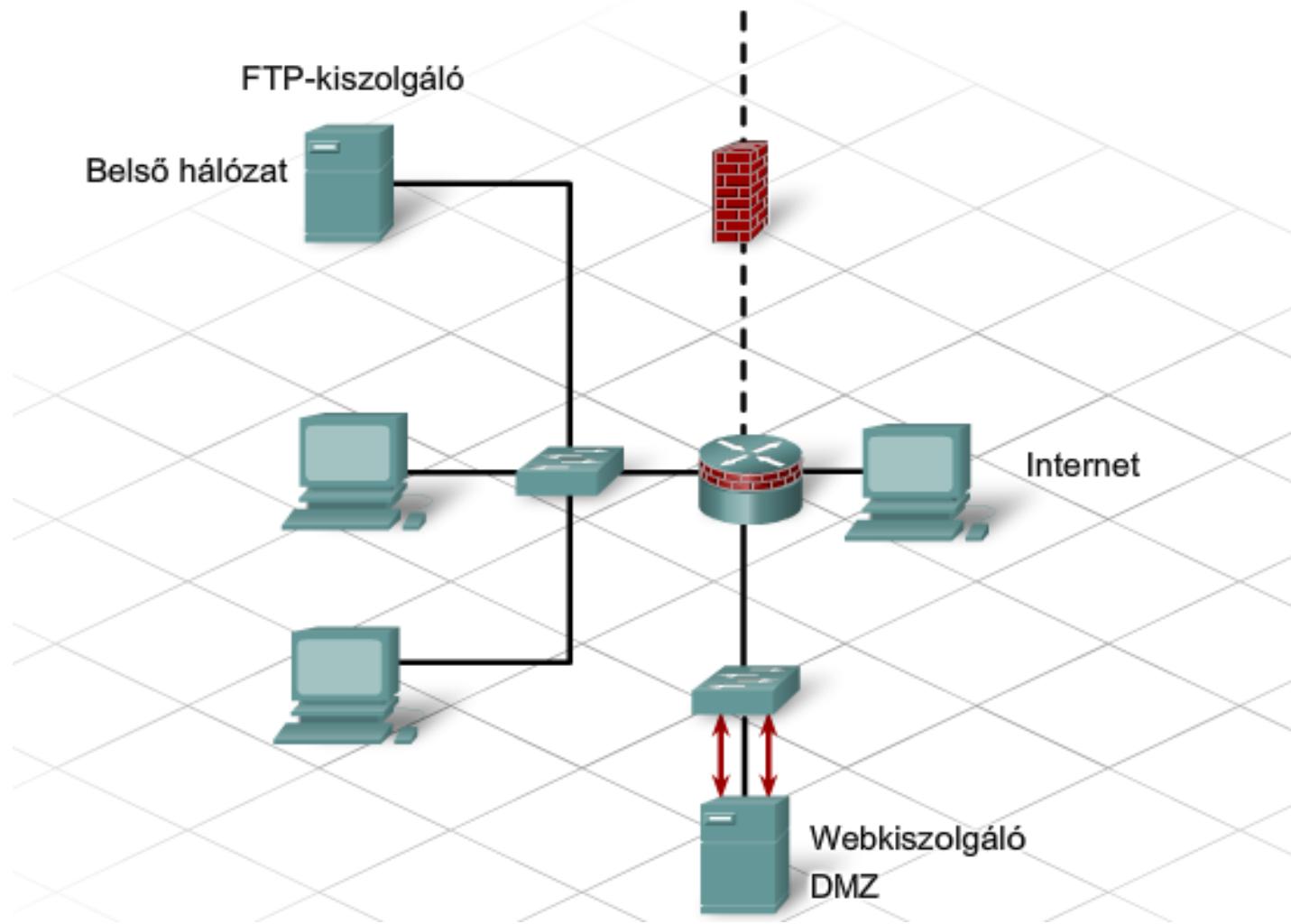
Egytűzfalas konfiguráció

- Az egyedüli tűzfal három területtel rendelkezik, egy-egy területtel a külső hálózat, a belső hálózat, és a DMZ számára.
- **Minden külső hálózatból** származó forgalom a tűzfalhoz kerül elküldésre.
- A tűzfallal szembeni elvárás az is, hogy **ellenőrizze** a forgalmat és határozza meg, hogy mely forgalmat kell a DMZ-be, melyet kell a belső hálózatba továbbítani és melyet kell végképp elutasítani.

Egytűzfalas konfiguráció

- Az egytűzfalas konfiguráció a **kisebb**, kevésbé terhelt hálózatokhoz megfelelő.
- Az egytűzfalas konfiguráció **egyetlen meghibásodási ponttal** rendelkezik és **túlterhelhető**.

Egy tűzfalas konfiguráció

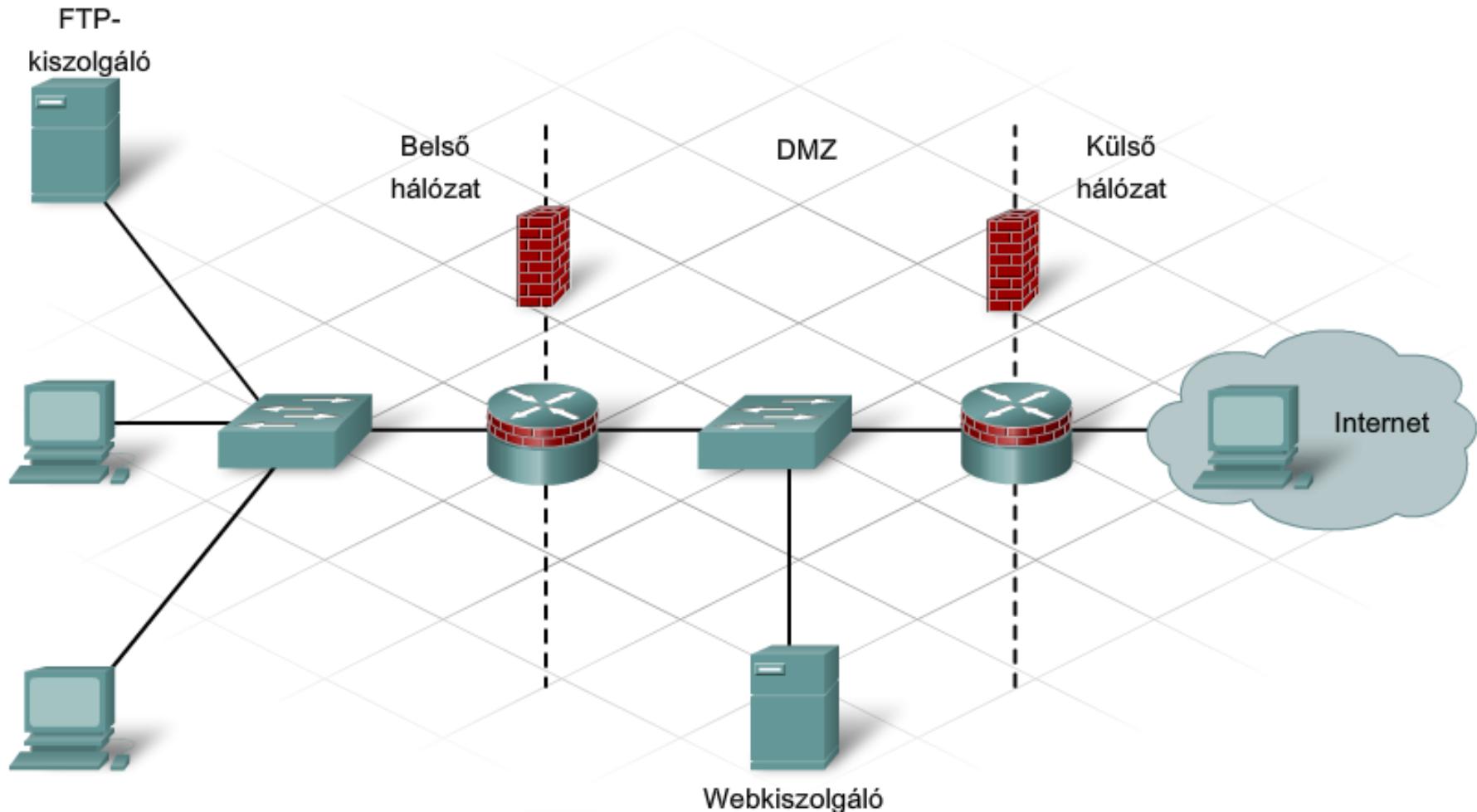


Kéttűzfalas konfiguráció

- A két tűzfalas konfigurációnál **egy belső és egy külső** tűzfal taláható a kettőjük között elhelyezkedő DMZ-vel együtt.
- A külső tűzfal kevésbé korlátozó és megengedi, hogy az **Internet** felhasználók **hozzáférjenek** a DMZ-ben levő szolgáltatásokhoz valamint megengedi, hogy bármely **belső felhasználó** által kért forgalom **áthaladjon rajta**.

Kéttűzfalas konfiguráció

- A belső tűzfal **jóval korlátozóbb** és védi a belső hálózatot a jogosulatlan hozzáféréstől.
- A kéttűzfalas konfiguráció inkább az olyan nagyobb, összetettebb hálózatok számára alkalmas melyek jóval **nagyobb forgalmat** bonyolítanak le.



Tűzfalak használata

- Sok otthoni eszköz, mint például egy integrált forgalomirányító, gyakran többfunkciós tűzfalszoftvert tartalmaz.
- Az ilyen tűzfal jellemzően:
 - Hálózati címfordítás (**NAT**),
 - Állapot alapú csomagvizsgálat (Stateful Packet Inspection, **SPI**),
 - IP, alkalmazás és webhely **szűrő** képességgel rendelkezik.
 - Támogatja a **DMZ** lehetőségét is.

A Tűzfal használata

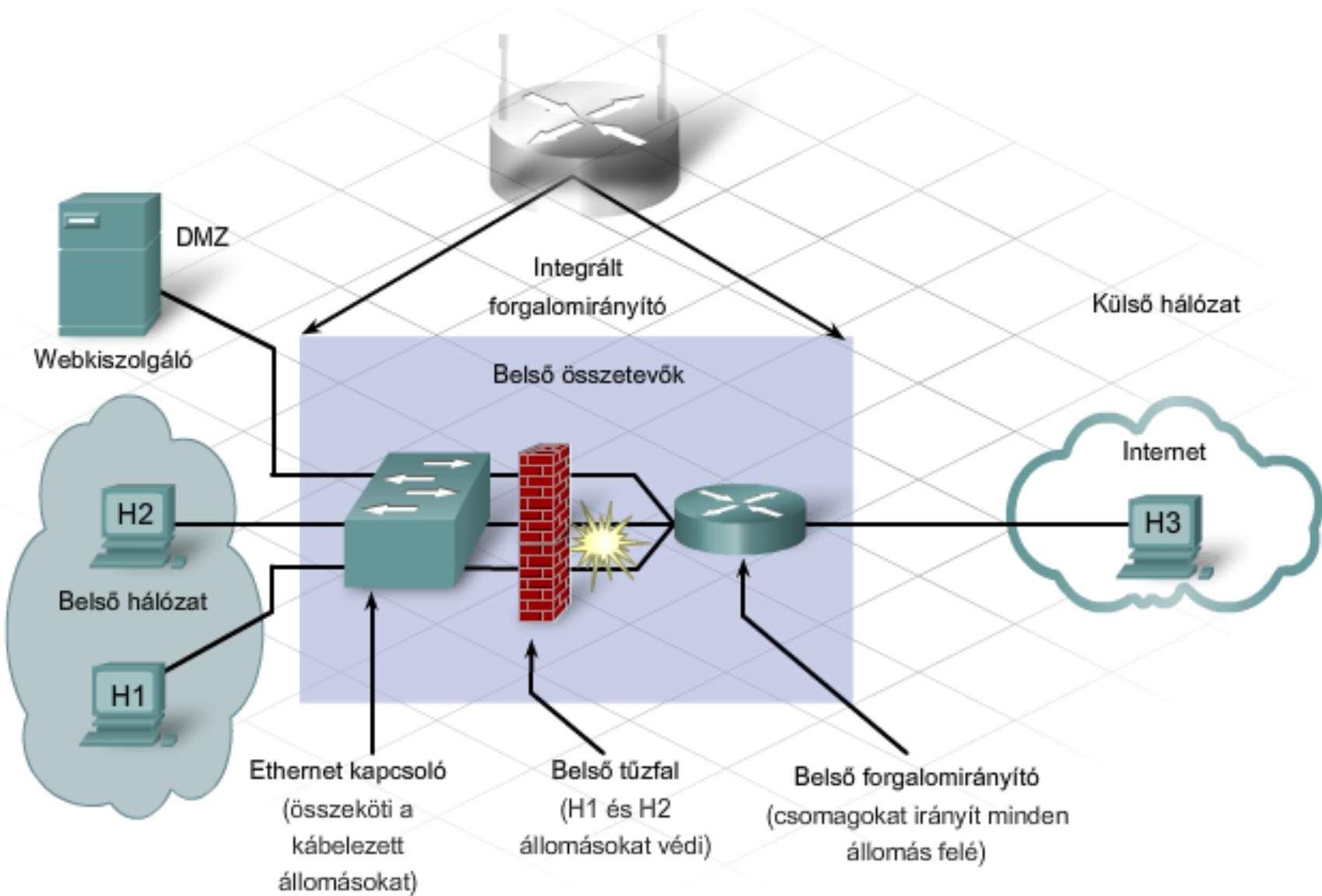
- Az integrált forgalomirányítóval egy olyan egyszerű DMZ állítható be, amely megengedi hogy egy belső kiszolgáló a külső állomások számára hozzáférhető legyen.
- Ennek megvalósítása érdekében a **kiszolgálónak statikus IP-címre** van szüksége, melyet a DMZ konfigurációban meg kell határozni.
- Az integrált forgalomirányító elkülöníti a meghatározott cél IP-című forgalmat.
- Ez a forgalom csak ahoz a **kapcsoló-porthoz** lesz továbbítva amelyhez a kiszolgáló kapcsolódik.
- Az összes többi állomást így még inkább védi a tűzfal.

A tűzfal használata

- A port-alapú továbbítás használatával jóval korlátozóbb DMZ állítható be.
- A port-alapú továbbítás esetén meg vannak határozva azok a portok melyek a kiszolgálón elérhetők.
- Ebben az esetben csak az adott célportokra irányuló forgalom engedélyezett, minden más forgalom tiltott.

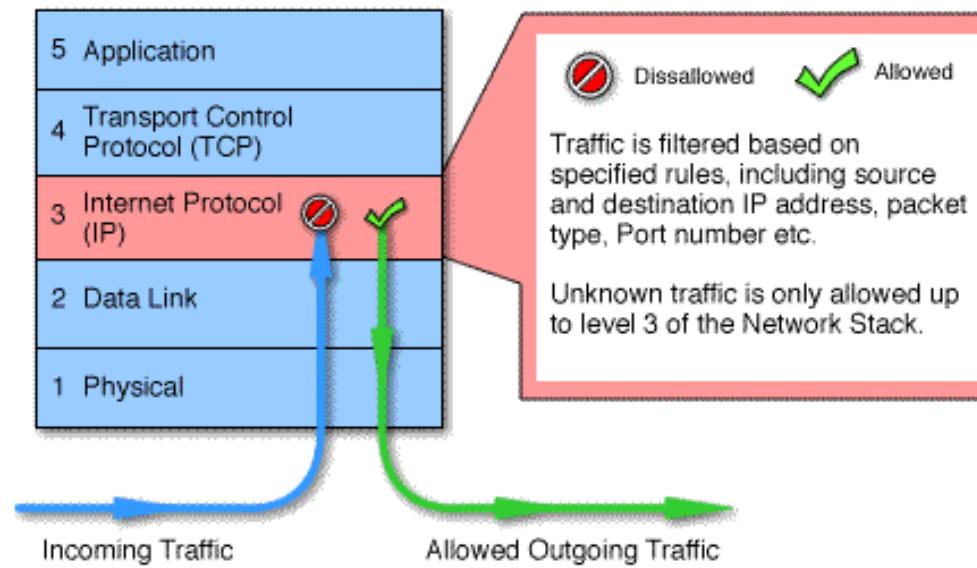
A tűzfal használata

- Az integrált forgalomirányítón belüli **vezeték nélküli** elérési pont a **belő hálózat** részének tekintendő.
- Fontos annak megértése, hogy ha a vezeték nélküli elérési pont **nem biztonságos**, bárki, aki ahhoz csatlakozik a belő hálózat védett részére, a **tűzfal mögé** kerül.
- A hekkerek (hacker) így a biztonsági szolgáltatások kikerülésével juthatnak a belő hálózatba.



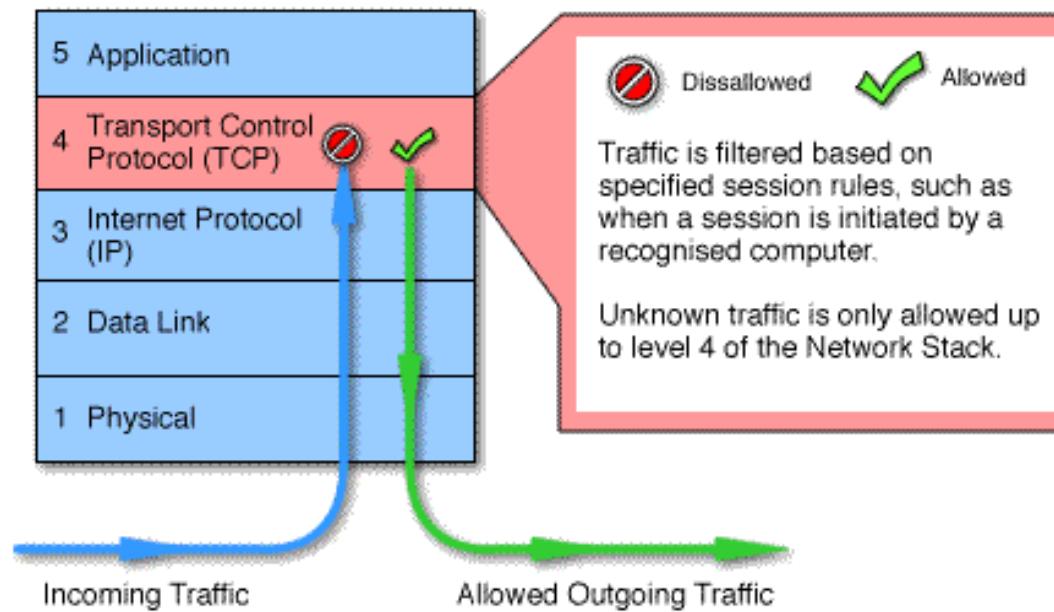
TÚZFAL KATEGÓRIÁK

Csomagszűrős tűzfal (Packet Filtering)



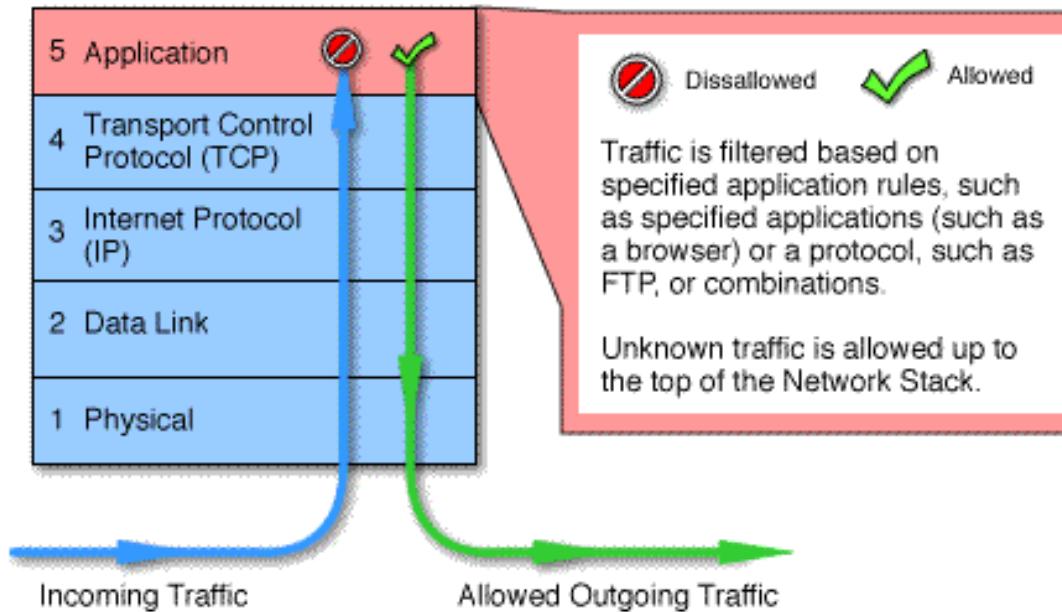
- A továbbküldés előtt minden csomag eleget kell tegyen egy bizonyos kritériumnak: forrás és cél IP, csomag típus, port szám.

Circuit-Level gateway



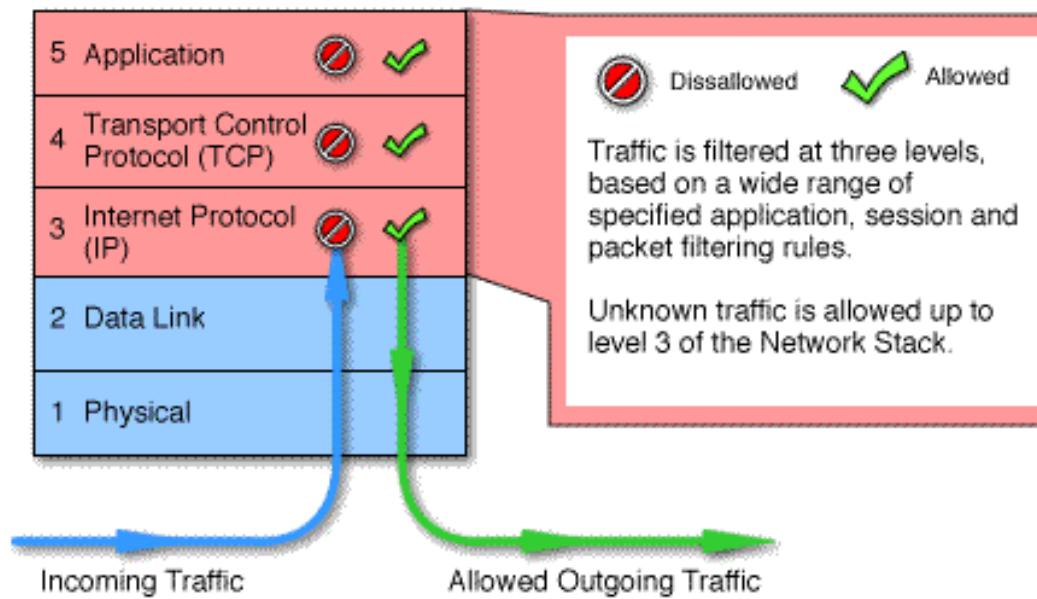
- A csomagok közötti kapcsolat felépítésére vonatkozó ajánlatokat felügyelik.

Application Level Gateway



- Amikor csomagok kívülről érkeznek, megvizsgálja és értékel, hogy a csomag bekerülhet-e a belső hálózatra. A szerver kiértékeli az IP-címét, de emellett értékeli az adatokat és a csomagokat, hogy nehogy hackerek támadják az információkat, a csomagokat.

Stateful Inspection



- Az előző három túzfal tulajdonságait egyesíti. Kliens és gazda között direkt összeköttetést létesít, ezáltal megoldja a többi hibáit. Felismeri és kezeli az alkalmazás szintű adatokat. Nagy sebesség, magas biztonság.

PROXY SZERVER

Mi a PROXY?

- Speciális tűzfal-típus, amely a közvetlen kommunikációt a külső és a védett hálózat között nem teszi lehetővé.
- E helyett a **belső hálózatról érkező kéréseket feldolgozza**, majd azokkal azonos értelmű kérést küld a külső szerver felé, az azokra érkező válaszokat pedig ismét a belső hálózat felé továbbítja.
- A proxy szerverek sok esetben **tartalmi gyorsítótárat** is magukban foglalnak, így bizonyos esetekben jelentős mértékben **csökkenthalik a kifelé irányuló forgalmat**.

Mi a PROXY?

- Az Interneten arra használják, hogy a szolgáltatások elérésére irányuló kéréseket **ne saját maga válaszolja** meg, hanem irányítsa azokat egy közelí (innen a név: proxy -- **közelben lévő**) kiszolgálóhoz, amely az adott szolgáltatással rendelkezik és nagyobb teljesítményt produkál.
- A proxyk biztonsági szerepet is játszhatnak (pl. tűzfalak), de gyakran a cél csupán az **ellenőrizhetőség** és **naplózhatóság** (pl. egy cégnél lévő alkalmazottak HTTP proxy-n át érhetik el az internetet, így tevékenységeiket ellenőrizni és megfigyelni is lehet).

Gyorsító tárazás

- Másik igen jelentős felhasználási terület a rendelkezésre álló **sávszélesség kihasználtságának javítása** illetve annak kímélése a végfelhasználótól egészen a kiszolgáló webszerverig.
- Az igény szerinti **gyorsító tárazási modell** intelligens módon, felhasználói kérések alapján **tárolja a letöltött adatokat**. Mindezért annak érdekében, hogy a lehető leghatékonyabb módon végezze a tartalom változásának követését, annak frissítését és az adatok szolgáltatását.

Gyorsító tárazás

- Több felhasználós környezetben (hálózatban kötött gépek) gyakran előfordulhat **ugyanazon oldalak ismétlődő látogatása**.
- A proxy szerver letölти és elmenti az oldalak tartalmát egy **átmeneti tárolóban**, majd újabb kérés esetén a tartalom egyezőségét illetve annak változását több előre beállított szempont szerint is megvizsgálja.
- Végezetül eldönti hogy újratölти az **egészét**, az oldal **egy részét**, illetve a tartalom **megegyezik** az átmeneti tárban lévővel így azt továbbítja a felhasználó felé.

Proxy

- A kis, a közép és a nagyvállalati környezetben is alapvető elvárás a különböző hálózati protokollokon alkalmazott **tartalomszűrési lehetőség**:
- **HTML Tag Filters** (OBJECT, EMBED, APPLET, SCRIPT, IMG illetve adott a lehetőség tetszőleges számú és tartalmú szűrő létrehozására).
- **MIME Filters** ebben az esetben a rendelkezésünkre áll a teljes MIME táblázat tartalma (pl: application/zip, video/mpeg, audio/x-wav).
- **URL** alapján történő szűrés” (előre elkészített lista vagy reguláris kifejezések alapján).

ROUTEREK HOZZÁFÉRÉSI LISTÁJA

Biztonság

- A vállalati hálózaton belül a biztonság alapvető fontosságú.
 - Illetéktelen felhasználók belépésének megakadályozása.
 - Hálózat védelme a különféle támadásokkal (pl.: DoS támadás) szemben.
- Mindkét eset idő- és pénzveszteséggel jár a vállalat számára.

Forgalomszűrés

- Segítségével a hálózati rendszergazda felügyelheti a hálózat különböző részeit.
- A szűrés a csomagtartalom elemzésének folyamata, amely alapján eldönthető, hogy egy adott csomagot átengedünk vagy blokkolunk.
- A forgalomszűrés javítja a hálózat teljesítményét.

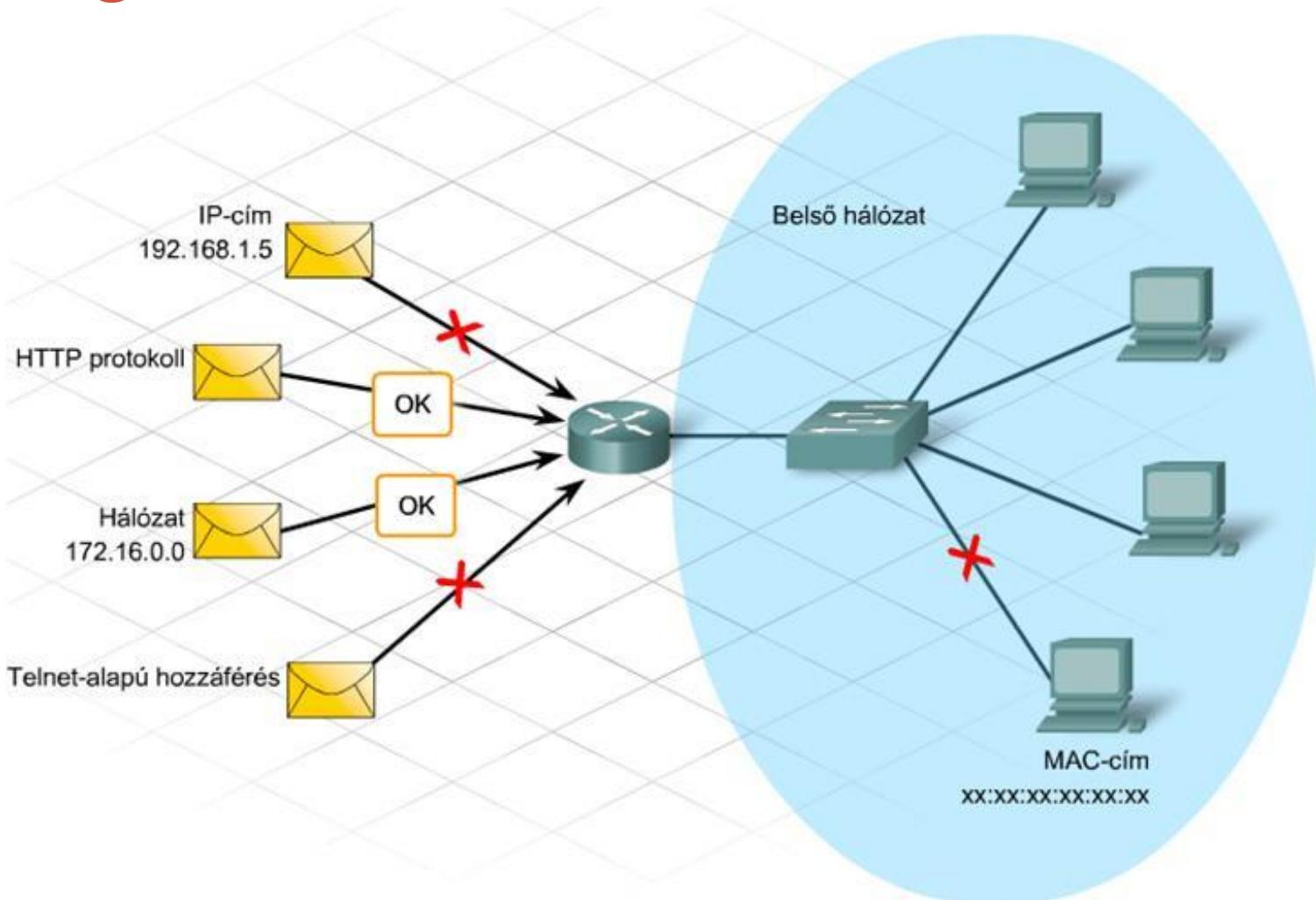
Forgalomszűrés

- A forgalom engedélyezése vagy tiltása az alábbiak szerint történhet:
 - Forrás IP-cím
 - Cél IP-cím
 - MAC-cím
 - Protokollok
 - Alkalmazástípus

Forgalomszűrés menete

- Be kell állítani a forgalomirányítót a nemkívánatos forgalom azonosítására.
- A nemkívánatos forgalom forráshoz közeli tiltásával a forgalom nem halad keresztül a hálózaton, és nem pazarol el értékes erőforrásokat.

Forgalomszűrés



Forgalomszűréshez használt eszközök

- Integrált forgalomirányítóba épített tűzfalak
- Adatbiztonsági funkciókat ellátó célkészülékek
- Kiszolgálók

Forgalomirányító forgalomszűrés

- Szinte minden forgalomirányító képes a
 - Forrás és cél IP-cím alapján történő csomagszűrésre.
 - Meghatározott alkalmazások és protokollok (pl. IP, TCP, HTTP, FTP és Telnet) szerinti szűrésre.

ACL - Access Control List

- A forgalomszűrés legáltalánosabb módja.
- A hálózatba belépő és az onnan távozó forgalom ellenőrizhető és szűrhető.
- Lehet egy adott forrásból érkező forgalmat engedélyező vagy tiltó egyetlen parancs,
- Lehet több száz parancsból álló lista is, ami különböző forrásból érkező csomagok átengedéséről vagy tiltásáról dönt.

ACL további használata

- A belső állomások meghatározása címfordításhoz.
- A speciális funkciókhoz (pl. QoS) tartozó forgalom azonosítása és csoportosítása.
- A forgalomirányítási frissítések tartalmi korlátozása.
- A hibakeresési üzenetek korlátozása.
- A forgalomirányítók virtuális terminálról történő elérésének szabályozása.

ACL-ek használatából eredő problémák

- Az összes csomag ellenőrzése terhelést jelent a forgalomirányítónak.
- A rosszul megtervezett ACL-ek még nagyobb terhelést okoznak, ami zavart okozhat a hálózat használatában.
- A nem megfelelően elhelyezett ACL-ek blokkolhatják az engedélyezni kívánt, és engedélyezhetik a blokkolni kívánt forgalmat.

ACL típusok

- Normál ACL
- Kiterjesztett ACL
- Nevesített ACL

Normál ACL (Standard ACL)

- Forrás IP-cím alapján végzi a szűrést
- A teljes (pl. IP) protokollműködés alapján engedélyezi vagy tiltja a forgalmat
- Adott PC vagy LAN számára engedélyezheti vagy tilthatja az összes szolgáltatás elérését
- Azonosítási száma 1-99, 1300-1999

Normál

```
Router(config)#access-list 1  
permit host 172.16.2.88
```

- Egy bizonyos IP-címet engedélyez.

Kiterjesztett ACL (Extended ACL)

- Forrás IP-cím, cél IP-cím, protokoll és portszámok alapján szűrhet.
- Elterjedtebb, mivel specifikusabbak és jobb ellenőrzést tesznek lehetővé.
- Azonosítási száma 100-199, 2000-2699

Kiterjesztett	Router(config)#access-list 100 deny tcp 172.16.2.0 0.0.0.255 any eq telnet	<ul style="list-style-type: none">• Tiltja a 172.16.2.0/24 alhálózat számára bármely más állomás elérését, amennyiben telnetkapcsolatot próbálnak létesíteni.
---------------	--	---

Nevesített ACL (Named ACL, NACL)

- Szám helyett névvel hivatkozunk
- Normál vagy kiterjesztett hozzáférési lista
- NACL üzemmód

Nevesített	<pre>Router(config)#ip access-list standard permit-ip Router(config-ext-nacl)#permit host 192.168.5.47</pre>	<ul style="list-style-type: none">• Létrehoz egy permit-ip nevű normál hozzáférési listát.• Engedélyezi a hozzáférést a 192.168.5.47 IP-címről.• Az első parancs a forgalomirányítót NACL konfigurációs almódba helyezi.
------------	---	--

ACL felépítése

- A hozzáférési listák egy vagy több utasításból állnak.
- A forgalmat minden egyes utasítás a megadott paraméterek alapján engedélyezheti vagy tilthatja.
- Az ACL utolsó utasítása mindig implicit tiltás.
 - Automatikusan odakerül minden egyik ACL végére.

ACL felépítése

- Az engedélyező utasítást nem tartalmazó ACL minden forgalmat tilt, mivel minden ACL végén szerepel az implicit tiltás.
- Az ACL tehát minden olyan forgalmat tilt, ami nincs konkrétan engedélyezve.

ACL felépítése

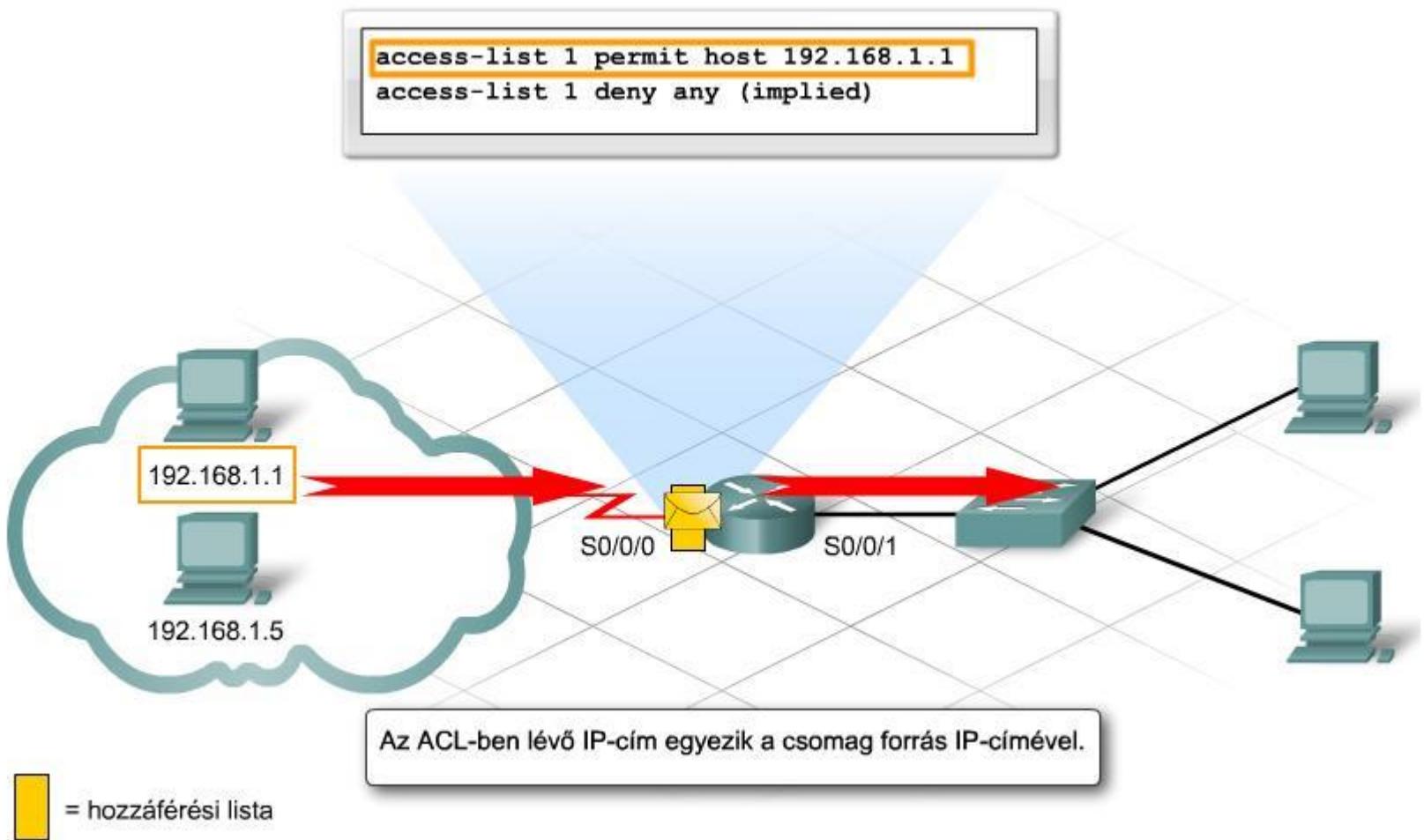
- A forgalmat sorban össze kell vetni az ACL-ben található utasításokkal míg egyezést nem találunk vagy el nem érjük az utasításlista végét (implicit tiltás).
 - Az implicit tiltás semmilyen forgalmat nem engedélyez.
 - Az implicit tiltás funkció megakadályozza a nemkívánatos forgalom véletlen áthaladását.

ACL elhelyezése

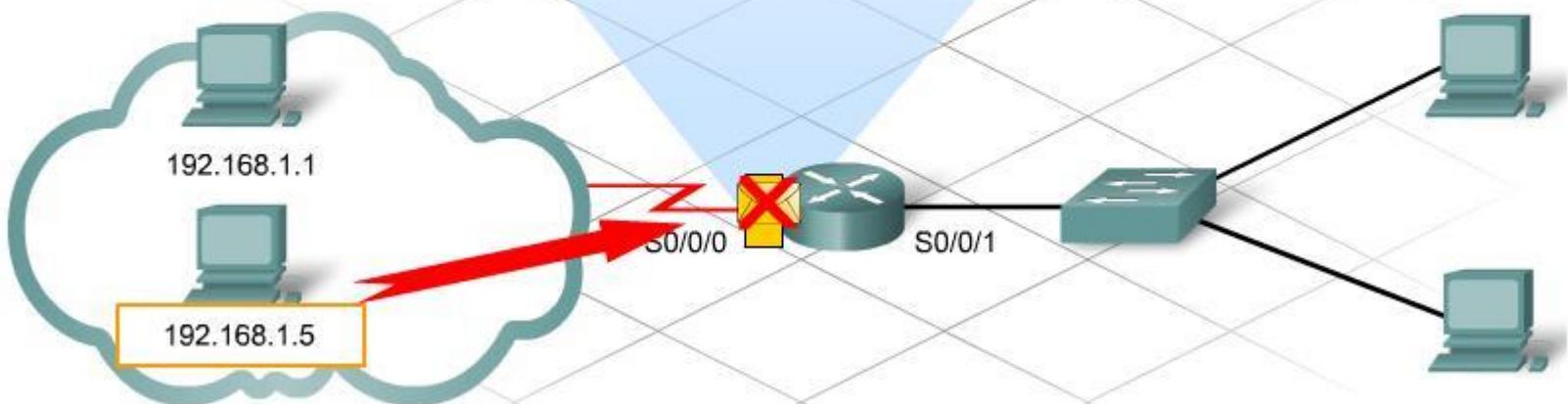
- A hozzáférési lista akkor lép működésbe ha elkészítése után hozzárendeljük a megfelelő interfészhez.
- Az ACL az interfészen vagy a bejövő vagy a kimenő forgalmat figyeli.
 - Az irányt mindig a forgalomirányító szemszögéből nézzük.

ACL működése

- Létezik-e az interfészhez rendelt ACL lista?
- Az ACL lista a bejövő vagy a kimenő forgalomra vonatkozik?
- A forgalomra teljesül-e valamely engedélyező vagy tiltó feltétel?
 - Az összes csomag címrészét össze kell hasonlítani az ACL-utasítások megfelelő címrészével.



```
access-list 1 permit host 192.168.1.1  
access-list 1 deny any (implied)
```

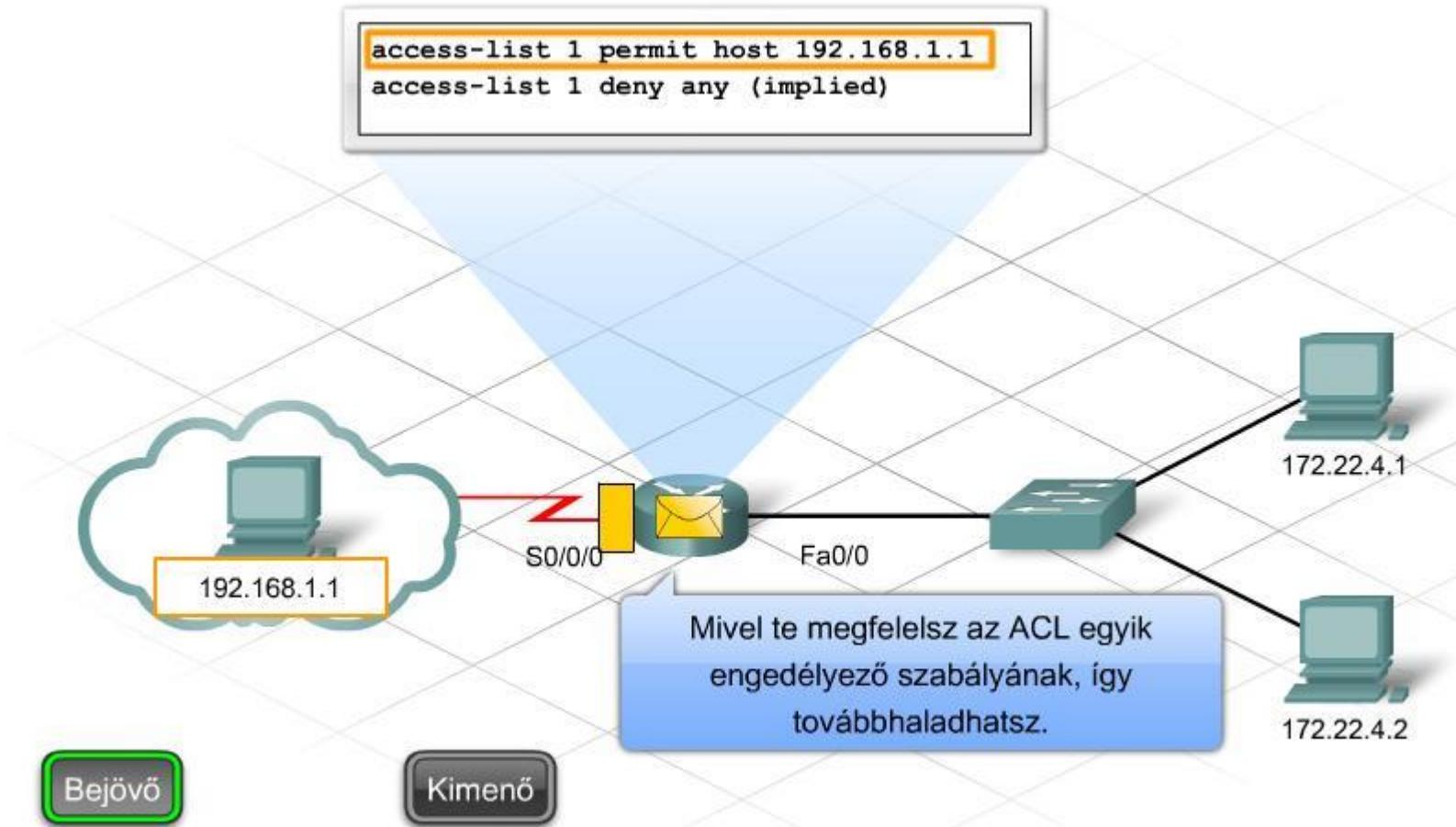


= hozzáférési lista

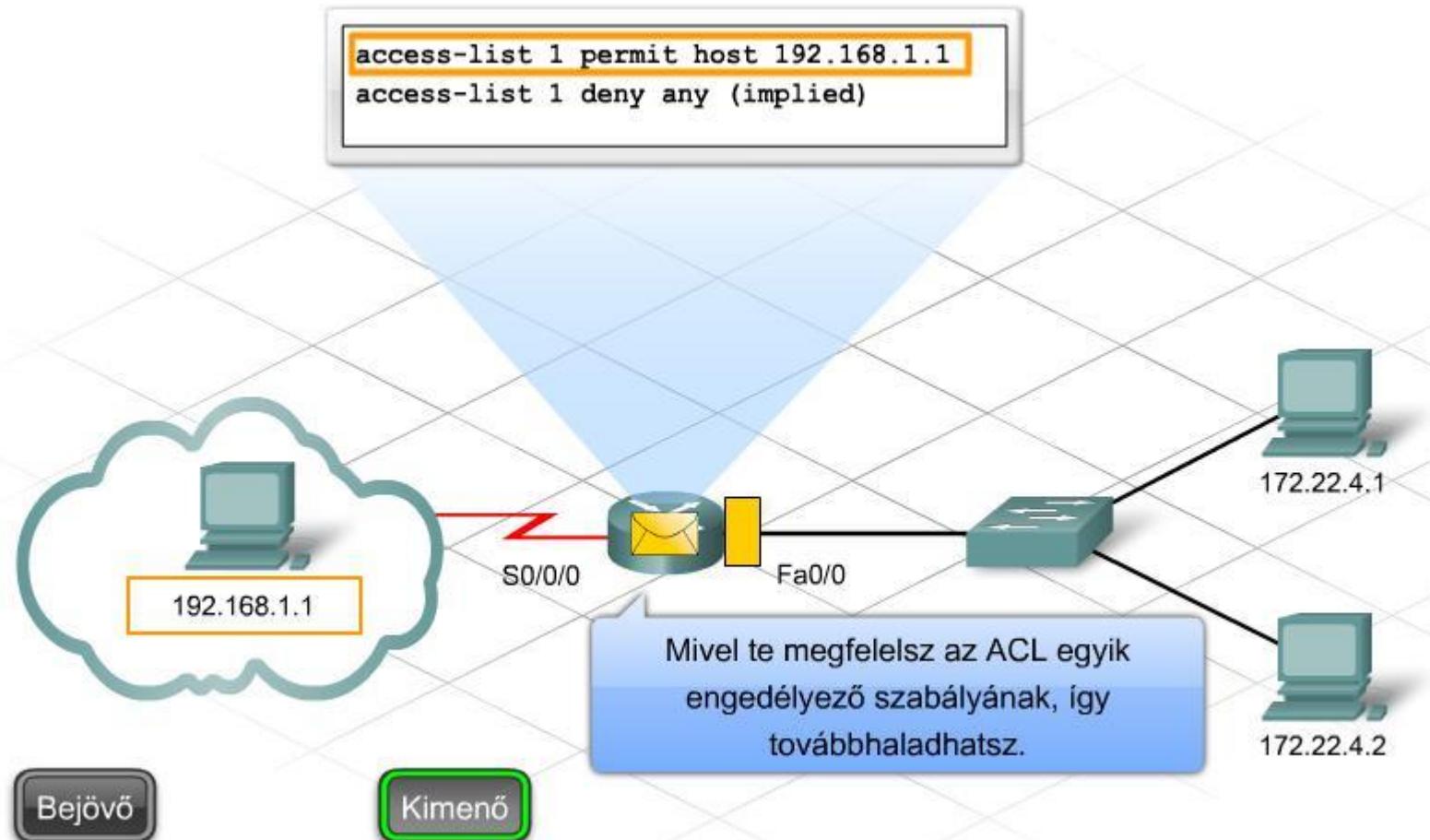
ACL-ek hatása

- A forgalomirányító interfészkekhez protokollonként és irányonként egy-egy ACL adható meg.
- Az interfészhez hozzárendelt ACL-ek végrehajtása késlelteti a forgalmat.
- Akár egyetlen hosszú ACL is észrevehető hatással lehet a forgalomirányító teljesítményére.

Bemenő forgalom



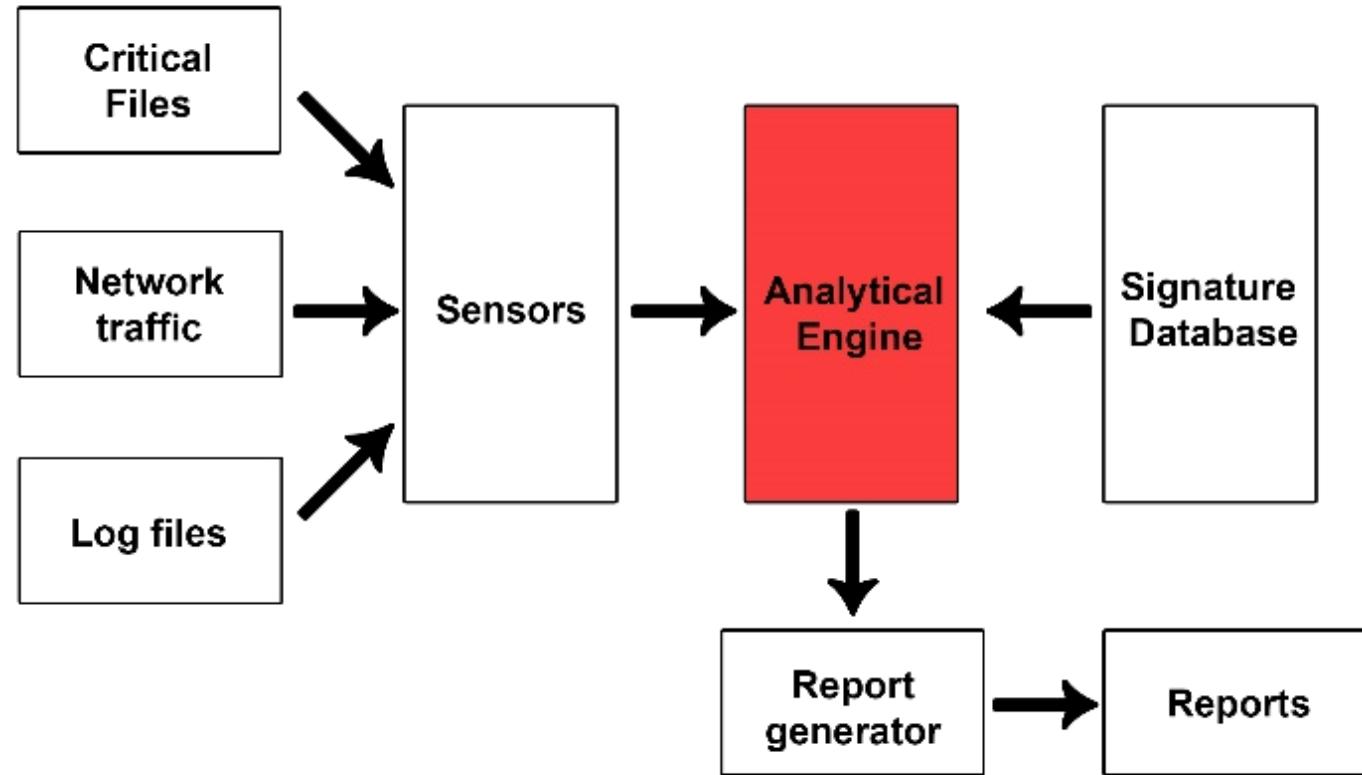
Kimenő forgalom



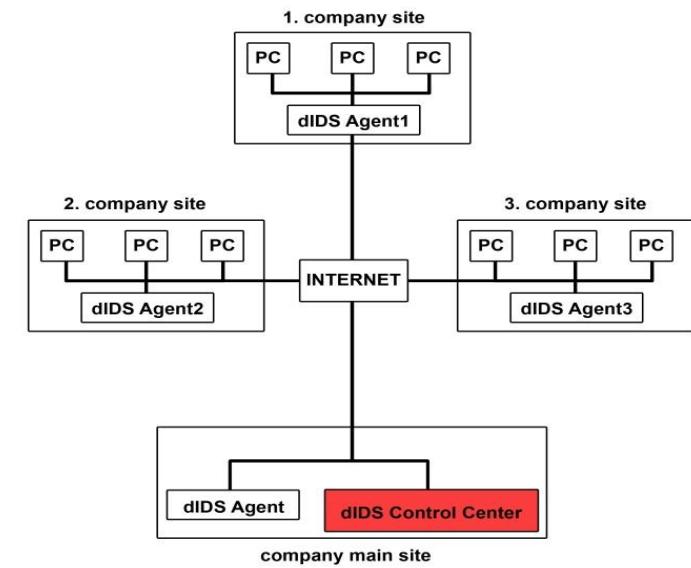
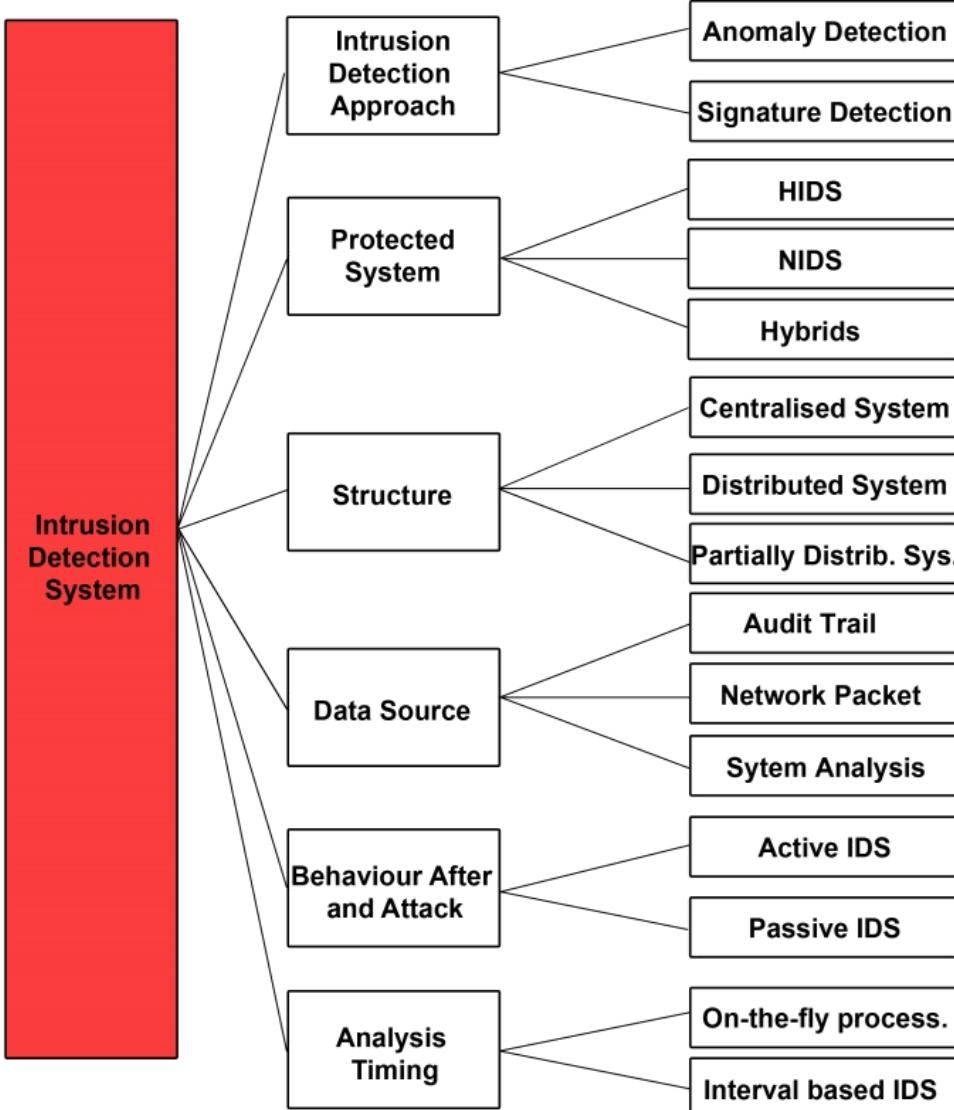
Behatolás érzékelő rendszerek

Intrusion Detection System (IDS)

IDS



http://gocslaszlo.hu/kutatas/G_J_Survey_on_Intrusion_TEAM_2015.pdf



Types of IDS systems

IDS

- **Aktív IDS**

A behatolás megelőző rendszerként (Intrusion Prevention System – IPS) ismert aktív IDS emberi beavatkozás igénye nélkül, automatikusan blokkolja a gyanúsnak vélt rendszer-hozzáférési kísérleteket. Az IPS-t a hálózat határain kell elhelyezetni, aminek következtében maga az IPS is érzékennyé válik a támadásokra. Még az is megtörténhet, hogy saját tevékenységét véli illetéktelen behatolásnak. Az IPS megfelelő konfiguráció hiányában könnyen tilthatja a rendszer használatára felhatalmazott felhasználókat és alkalmazásokat is. Az IPS típusú megoldás érzékenyebb egy memória túlterhelést irányzó támadásra (Denial of Service – DOS) mint egy passzív IDS. A DOS támadás különböző hálózati címekről indít kérelmeket a rendszer felé egészen addig, amíg a rendszer memória puffere túl nem terhelődik. Az IPS ugyan képes ennek kivédésére, viszont mellékhatásként letilthatja az adott portot, vagy akár a teljes hálózati forgalmat is.

- **Passzív IDS**

A passzív IDS nem képes automatikus válaszlépésekre, csak a háttérben működve vizsgál, és támadásgyanús esetben riasztja a rendszergazdát. Előnye, hogy mivel csak passzív megfigyelő a hálózatban, ezért nem válik támadás célpontjává, és az a veszély sem fenyegeti, hogy saját tevékenységét érzékelje támadásként. Hátránya, hogy mire a rendszergazda az megkapja értesítést, elemzi azt, majd döntést hoz a válaszlépésről, addigra nagy valószínűséggel a támadás már lezajlott.

IDS

- **Hálózati behatolást jelző rendszer (Network intrusion detection system - NIDS)**

Egy NIDS általában egy hálózati megfigyelő eszközt tartalmaz, ami mögött egy hálózati interfész kártya dolgozik. Ez az IDS típus a hálózat egy szegmensében vagy annak határa mentén helyezkedik el, és vizsgálja a hálózati forgalmat. Képes egy, vagy akár több rendszert és eszközt is megfigyelni a hálózaton belül, és védeni a hálózatot a támadások ellen.

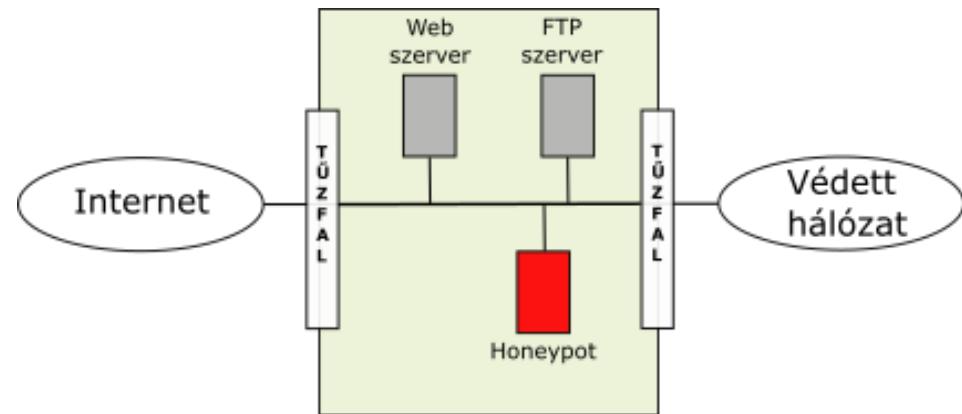
- **Host Intrusion Detection System – HIDS**

A HIDS egy önálló számítógép megfigyelésére szolgál. Telepíteni és konfigurálni kell az adott gépre. A HIDS-nek szüksége van kisebb, beleépített vizsgáló mechanizmusokra, amelyek az adott rendszer napló fájljaiból szerzik be a szükséges információt a behatolási kísérletek elleni fellépéshez. Képes a rendszert fenyegető hálózati és fizikai támadások jelzésére és kivédésére is egyaránt.

CSALIK A HÁLÓZATON

Honeypot

- Egy olyan információs rendszer (erőforrás), mely értéke az erőforrás engedély nélküli felhasználásában rejlik.
- Csaliként használunk olyan számítógépes rendszereket, hogy hackereket, kárt okozó embereket vagy szoftvereket tudjunk beazonosítani.
- Csak szimulálnak működő rendszereket
- Nincs normális funkciójuk, tehát minden tevékenység ami kapcsolatba van velük az támadási kísérlet.



Honeypot

- Csak a támadásokat naplózza – könnyű feldolgozás
- Támadások, betörések érzékelésére és nyomon követésére
- Kutatási célokra: új támadási módszerek, eszközök felderítésére, statisztikák készítésére
- Wormok és spamek elleni védekezésre

Honeypot – alacsony kölcsönhatású

- Az alacsony kölcsönhatású honeypot nem egy önálló gép (virtuális gép), hanem csak egy emulátor program, ami egy operációs rendszer szolgáltatásait utánozza.
- Előnyös tulajdonsága, hogy egyszerű telepítés és konfigurálás jellemzi. Az emulált szolgáltatással minimális a kockázat.
- Ezen megoldás nagy előnye, hogy a támadó nem szerzi meg az irányítást az operációs rendszer fölött, mivel az csak emulált.
- A támadó csak korlátozott mennyiségű információt szerez, főként tranzakciós adatokat, néhány kisebb kölcsönhatást gyűjt.
- Ezeket leginkább a vállalati rendszerekben, termelési iparágakban használják.

Honeypot – magas kölcsönhatású

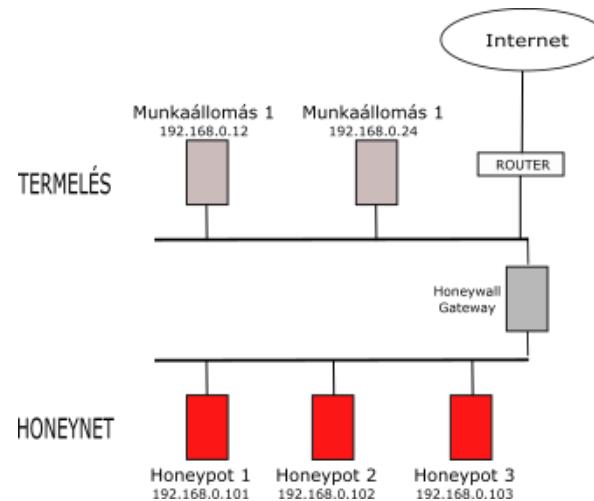
- A magas kölcsönhatású honeypotok nem emulált, hanem valós operációs rendszert és szolgáltatásokat futtatnak.
- Az ilyen típusú honeypotok mögé tűzfalat kell helyezni a kockázatok csökkentése érdekében.
- Telepítésük és karbantartásuk nehézkes, de hatalmas mennyiségű információt tudnak nyújtani a hackerek viselkedéseiről, motivációiról.
- Ezeket leginkább kutatásokhoz használják.

Honeynet

A honeynet több számítógépből álló hálózat, ami a honeypotokéval megegyező funkciókkal rendelkezik.

Ha egy hálózaton konfigurálunk egy honeypotot, amelyen csaliként több ismert szolgáltatást futtatunk vagy emulálunk egyszerre, a támadó számára gyanús lehet, hogy egy sebezhető szervert több módon is meg tud támadni.

Ennek elkerülése érdekében érdemes egy hálózaton több honeypotot tartalmazó honeynet-et kialakítani, ahol a különböző szolgáltatások más és más honeypoton futnak.



Honeyfarm

Azon vállalatoknál, melyek telephelyei földrajzilag távol esnek egymástól, problémát okozhat, hogy ezen az egyes telephelyeken telepített honeynet-ek túl sok erőforrást igényelnek, és az üzemeltetéshez is külön adminisztratív személyzet szükséges.

Ebben az esetben egy honeyfarm megvalósítása jelenti a megoldást. Működésének lényege, hogy egy központi helyre kell telepíteni egy csali hálózatot (honeynet), a telephelyekre pedig egy-egy honeypot-t, melyeknek az a szerepe, hogy a gyanús tevékenységeket azonnal átirányítja az adatokat a központi honeynet-re.

