

Adatbiztonság II.

Buday Gergely

2010. november 24.

1 Jelszavak

2 Biometria

Jelszavak

- Nyilvánvaló jelszavak: Windows jelszó, bankkártya PIN kódja (Personal Identification Number)
- Nem annyira nyilvánvalók: TAJ szám, anyánk neve
- Példa: AT&T vezeték nélküli szerződés: bárki, aki tudja a nevünket, címünket, telefonszámunkat és a társadalombiztosítási számunk utolsó négy számjegyét, az módosíthatja a szerződést
- Az AT&T elhárít minden felelősséget ami abból adódna, hogy valaki megszerzi ezeket az adatokat
- Az Egyesült Államokban nincs személyi igazolvány

Veszélyek

- "Identity theft" - identitáslopás
- Az USA-ban évente félmillió ember esik ennek áldozatul
- Problémák: gyakran kell használni őket, hogy megjegyezzük
- Kontextus is kell hozzá: a különböző jelszavak ne hassanak egymásra az emlékezetünkben
- Mi van, ha sok olyan honlapon regisztrálunk, amit ritkán használunk?

Azonosítás

- 1. "Valami, amit birtoklunk"
- 2. "valami, amit tudunk"
- 3. "Valami, ami vagyunk"
- 1. garázsajtó elektronikus kulcsa, egy PDA, egy laptop
- 2. jelszó
- 3. ujjlenyomat, íriszminta
- költségek miatt általában a második verziót használjuk

Alkalmazott pszichológia

- Áthágja-e a rendszer biztonságát a felhasználó a jelszó átadásával, véletlenül, szándékosan vagy egy csalás eredményeképp?
- Elég nagy valószínűséggel a helyes jelszót adja-e meg a felhasználó?
- Emlékeznek-e a felhasználók a jelszóra, vagy le kell írniuk, esetleg olyan egyszerű jelszót kell választaniuk, amit a támadó könnyen ki tud találni?

Social Engineering — Szélhámoság

- A jelszó kijátszása
- Felhívom a titkárnőt, hogy a rendszer karbantartója vagyok, és adja meg a jelszavát
- Klasszikus példa: a rendszergazdát felhívja valaki, aki egy menedzser titkárnőjének adja ki magát, valami hihető esetet bemesélve, egyszer vagy kétszer. Ezek után újra hívja, és most egy fontos jelszót kér
- Ilyen esetekre a cégeknek jól megírt biztonsági szabályokra van szükségük

Social Engineering - Sidney-i egyetem

- 336 informatikus hallgatónak kiküldtek egy e-mail-t, hogy adják meg a jelszavukat, mert feltehetően betörtek a rendszerbe, és ez szükséges a jelszó "validálásához"
- 138-an elküldték a jelszót
- Néhányan gyanút fogtak: 30 diák hamis, de valódinak tűnő jelszót adott meg
- Több mint 200 megváltoztatta a jelszavát kérés nélkül
- Nagyon kevés diák jelentette az e-mail-t.

Biztonsági szabály - példa

- "Az adminisztrátor jelszó elég hosszú kell legyen minden gépen ahhoz, hogy ne lehessen megjegyezni"
- "Legalább 16 betűt és számot tartalmazzon, amelyeket a gép választ"
- "Egy borítékba tett papírra kell írni, és abban a szobában tárolni, ahol a gép van"
- "Soha nem szabad telefonon megadni vagy hálózaton keresztül használni"
- "Csak a mondott gép konzoljánál szabad használni"

Problémák a jelszómegadással

- Ha a jelszó hosszú és/vagy nehéz, nehéz lehet helyesen beütni
- Ha sürgős, nagy bajt is okozhat
- Rossz billentyűzetkiosztás - gyakori probléma!

Példa: előre fizetett villanyáram

- Dél-Afrika
- A vevők nem hitelképesek, gyakran még címük sincs
- A lakosság harmada nem tud írni-olvasni
- Fizet, ekkor kap egy húszjegyű számot
- Ez tartalmazza az utasítást: tarifaváltást, elektromos áram vételét, miegyebet
- Az analfabétaság nem jelentett problémát: "mindenki tud telefonálni"
- Az elgépelés probléma volt, de ezt megoldották: az első sorba 3x4, a másodikba 2x4 számjegyet írtak

Emlékezni jelszavakra

- 12 vagy húsz számjegy működik, ha le kell másolni valahonnan
- de nem, ha meg kellene jegyezni
- Egyébként a felhasználók: rövid, könnyen megjegyezhető jelszót választanak, és/vagy leírják a jelszót
- Nem csak számítógép: Franciaországban volt egy szállodalánc, ami teljesen személyzet nélkül működött.
- Bankkártyát használva kapott az ügyfél egy számlát, az azon levő kóddal lehetett bemenni a szobába.
- A fürdőszoba a folyosón volt: ha valaki nem vitte magával a számlát, könnyen elfelejthette a jelszót, és az éjszakát a fürdőszobában volt kénytelen tölteni

A felhasználók képzése

- Vállalati, katonai, és bizonyos mértékben egyetemi közegben ez lehetséges
- Hogyan válasszunk jó jelszót
- Jelezzünk vissza, ha rosszat választ valaki
- Adhatunk nekik véletlen jelszavakat
- A jelszavakat kötelező lehet úgy védeni, mint az adatot, amit védünk (boríték, páncélszekrény)
- A biztonsági őrt körbe lehet küldeni, hogy senki nem hagyott-e jelszót az asztalon
- Tiszta asztal (clean desk) szabály: semmi nem maradhat az asztalon, mikor a munkaidő végén távozik az alkalmazott.

Esettanulmány

- Piros (kontroll) csoport: legalább hat karakter, egy nembetű
- Zöld csoport: találjon ki egy mondatot, és az alapján kreáljon jelszót. "It's 12 noon and I am hungry" -
l'S12&IAH
- Sárga csoport: válasszanak 8 betűt/számot egy eléjük rakott táblázatból, írják le, és 1-2 hét múlva semmisítsék meg a papírt, amint megjegyzték a jelszót

Esettanulmány II.

- A hipotézis az volt, hogy a piros csoport jelszavai könnyebben megfejthetők, mint a zöldéi (mondatból generált jelszavak).
- Szintúgy, hogy a zöld csoportéi könnyebben megfejthetők, mint a sárgáéi.
- És, hogy a sárga / zöld / piros a sorrend a megjegyzés nehézségét illetően
- De a kísérlet nem ezt találta igaznak

Esettanulmány III.

- A piros csoport jelszavainak 30 százaléka visszafejthető volt "cracking" szoftver használatával. Ez a másik két csoportban 10 százalék körüli volt. Tehát a mondatból generált jelszó ugyanolyan hatékony, mint a véletlen.
- Nem volt számottevő különbség a három csoportnál a jelszó-törlési kéréseket illetően
- A megjegyezhetőséget illetően a sárga (véletlen jelszó) csoport számolt be jelentős problémáról, a másik kettőnél nem volt ilyen

Esettanulmány - konklúziók

- Azoknál a felhasználóknál, akik követték az utasításokat, a mondatból generált jelszó a legjobb: könnyű megjegyezni és biztonságos.
- Önmagában az utasítás nem segít: a diákok harmada nem követte a szabályokat.













