

PKI az adathalászat (phishing) ellen?

Dr. Berta István Zsolt <istvan.bertha@microsec.hu>
PhD, MBA, CISA

Microsec Kft.

Milyen támadásról beszélünk?

- Adott egy szervezet, és annak ügyfelei. Nevezzük a szervezetet „bank”-nak.
- Az ügyfelek az Interneten keresztül érzékeny információkat, „utasításokat” küldenek a banknak.
- A bank valahogy meggyőződik az utasítások hitelességéről.
- A támadó célja az, hogy utasítást küldjön a banknak az ügyfelek nevében.
- Ehhez akarja megszerezni a támadó az ügyfelek pl. jelszavait, amelyeket pl. csaló levélben és/vagy csaló weboldalon kér el tőlük.

Mire használható a PKI?

- Aláírás:
 - ❑ saját magánkulcsunkkal kódolunk,
 - ❑ észlelhető, ha az aláírt dokumentumot az aláírást követően megváltoztatták, és később az aláíró kiléte is bizonyítható.
- Titkosítás:
 - ❑ a címzett nyilvános kulcsával kódolunk, a címzett (és csak ő) a saját magánkulcsával visszafejtheti az így kódolt dokumentumot.
- Authentikáció (partner hitelesítés):
 - ❑ saját kilétünket igazoljuk,
 - ❑ véletlen „kihívást” kódolunk a magánkulcsunkkal,
 - ❑ szimmetrikus kulcsokban állapotunk meg, és egy biztonságos csatornát hozhatunk létre.

Gyakran felmerülő PKI alapú megoldások

- Authentikáció
 - ❑ SSL szerver tanúsítványok
 - ❑ Tanúsítvány alapú bejelentkezés (kétfaktoros autentikáció)
- Aláírt levelezés
 - ❑ bank → ügyfél
 - ❑ ügyfél → bank

Vegyük figyelembe: phishing esetén...

- Rengeteg e-mail megy ki,
 - a felhasználók „kis” százaléka dől be,
 - de a csalónak még így is megéri.
-
- NAGY pénz van benne, így
 - a támadó jelentős erőforrásokat befektet.

Webszerverek SSL tanúsítványai

Webszerverek SSL tanúsítványai

- Az ügyfél hozzáfér a webserver SSL tanúsítványához,
- böngészőprogramjával ellenőrzi a tanúsítványt,
- ellenőrzi a tanúsítványban lévő címet,
- a tanúsítványból meghatározza a webserver nyilvános kulcsát,
- a böngésző a nyilvános kulcs alapján SSL kapcsolatot létesít a webserverrel.

Sokan nem tudják, hogy mire jó az SSL

- Sokan azt sem tudják, hogy van veszély.
- Sokan tudják, hogy „lakatot” kell keresni, de az is jó nekik, ha a lakat a weboldalon van.
- Sokan bármilyen (pl. self-signed) tanúsítványt elfogadnak, és azt hiszik, ekkor biztonságban vannak.
- Sokan elvárják, hogy legyen lakat, és a böngésző ne panaszkodjon, és azt hiszik, ekkor biztonságban vannak.

Miért működik a phishing?

- Felhasználóknak weboldalakot mutattak, dönteniük kellett, hogy a weboldal valódi vagy hamis.
- Az ügyes csalások a felhasználók 90%-át megtévesztették. (!)
- Nem találtak összefüggést az elért pontszám és aközött, hogy a felhasználó
 - ❑ hány éves, férfi vagy nő,
 - ❑ mennyire iskolázott,
 - ❑ mennyit webezik hetente,
 - ❑ milyen számítógépes tapasztalattal rendelkezik,
 - ❑ ismeri-e az adott weboldalt.
- „Why Phishing Works”, R. Dhamija, J. D. Tygar, M. Hearst, CHI2006, 2006.

Mit jelent az SSL szerver tanúsítvány?

- A webszerver tanúsítvánnyal a kibocsátó hitelesítés szolgáltató igazolja, hogy a tanúsítványhoz tartozó magánkulcs a tanúsítvány alanyának (a szerver üzemeltetőjének) birtokában van és az alany jogosult a tanúsítványban szereplő domain használatára.
- (Ez akkor igaz, ha a tanúsítvány érvényes.
- A tanúsítvány érvényességét korrektül ellenőriznünk kell.)

Mit NEM jelent az SSL szerver tanúsítvány?

- Nem jelenti azt, hogy a tanúsítvány alanya nem akar becsapni bennünket.
- Nem jelenti azt, hogy a kérdéses webszerver biztonságos.
- Nem jelenti azt, hogy a tanúsítvány alanya valóban az, akiknek mi hisszük.

Az URL sokaknak nem mond semmit

- Az URL akár a támadóé is lehet:
 - ❑ <https://biztonsagosbank.hu>
 - ❑ <https://sunyivagyok.hu>
 - ❑ <https://biztonsagosbank.ru>
- A támadó feltört szerveret is használhat:
 - ❑ <https://koklerbt.hu>
- Feltört szerver wildcard tanúsítvánnyal:
 - ❑ <https://biztonsagosbank.koklerbt.hu>
(és a tanúsítvány a *.koklerbt.hu címre szól)
- Trükkös URL-ek, speciális karakterekkel.

Nézzük meg a tanúsítványt!

- Ha sokat kattintok a Windowsban, előcsalom, hogy:
CN = www.biztonsagosbank.com
E = webmester@biztonsagosbank.com
O = XYZ Ltd.
C = US
- Mint mond ez az átlag felhasználónak?
- Sok weboldal fizetés esetén átirányít egy kifejezetten fizetéssel foglalkozó oldalra. Ekkor egy „vadidegen” céggel kommunikálunk.
- A jelenlévők közül ki szokta ellenőrizni a webszerver tanúsítványok tartalmát?

Korrektül kell ellenőrizni a tanúsítványt

- A böngészők többsége kihagy elemi ellenőrzési lépéseket! Ilyen lépések lehetnek például:
 - ❑ tanúsítványlánc felépítése, egy megbízható root-ig,
 - ❑ visszavonás ellenőrzés a kérdéses tanúsítványra,
 - ❑ visszavonás ellenőrzés a láncra,
 - ❑ visszavonás ellenőrzés a visszavonási információkra
 - ❑ stb.
- Van kontrollunk afelett, hogy mely root-okat fogadunk el megbízhatónak?
- Alkalmazások alapértelmezett tanúsítványtárai...
- Csak annyira vagyunk biztonságban, mint amekkora biztonságot a leggyengébb „megbízható” root nyújt.

Merre van kiút?

- A böngészők sok segítséget nyújthatnak
 - ❑ a tanúsítványokban lévő, „fontos” információk kiemelésében,
 - ❑ a megbízható root-ok kiválogatásában,
 - ❑ a tanúsítványok korrekt ellenőrzésében,
 - ❑ és egyéb, nem PKI védekezési módszerekkel.
- Extended validation (EV) tanúsítványok ?

Tanúsítvány alapú bejelentkezés (kétfaktoros autentikáció)

Tanúsítvány alapú bejelentkezés

- A felhasználó továbbra is ellenőrzi a webszerver SSL tanúsítványát
- A felhasználó bejelentkezéskor nem (csak) felhasználónevet és jelszót ír be, hanem kliens SSL tanúsítványt (is) használ. (A szerver ezt ellenőrzi stb.)
- A támadó nem tudja ellopni a jelszavát (mert nincs jelszó), vagy nem elég, ha ellopja a jelszót.
- A felhasználó tanúsítványához tartozó magánkulcs jó, ha chipkártyán van.

Mit tehet a támadó?

- Közbeékelődéses támadás (man in the middle)
 - ❑ A felhasználó a támadóval beszélget,
 - ❑ a támadó továbbítja a felhasználó üzeneteit a banknak, és viszont.
 - ❑ A támadó néha lecseréli az üzeneteket.
 - ❑ Ez esetben nem sokat jelent.
- Trójai programot telepít a felhasználó gépére
 - ❑ ha a felhasználó belép,
 - ❑ a trójai a felhasználó session-jét kihasználva küld üzenetet, a felhasználó nevében.

Tanúsítvány alapú bejelentkezés?

- A támadónak stratégiát kell váltania.
- Meg is teszi...

Aláírt levelezés, bank → ügyfél

Hogyan?

- Példa: A bank aláírtan csak aláírt levelet küld az ügyfeleinek. A csaló nem ismeri a bank tanúsítványához tartozó magánkulcsot, így nem tudja aláírni a csaló leveleket. Ezért a csaló nem tudja megtéveszteni a címzetteket.

Aláírt levelezés, bank → ügyfél ?

- A banknak tudatosítania kell az ügyfeleiben, hogy tőle kizárólag aláírt levelek jöhetnek.
- Ez ugyanaz a probléma, mint az, hogy a bank soha nem kéri el az ügyfél PIN kódját. Ezt sem könnyű tudatosítani az ügyféllel.
- A tanúsítvány és az alany összetartozásával kapcsolatos problémák itt is felmerülnek.
- Aláírás és aláírás között nagy különbség lehet.
- Itt még kevésbé kiforrottak az eszközök.

Ez sem egyszerű...

- A „csak aláírt levelet fogadok el” nem megoldás.
 - A csalónak is lehet aláírása.
 - Feltört gépek problémája...
-
- Gipsz Jakab és baráti köre számára ez lehet, hogy ma megoldást jelent, de globálisan és hosszú távon nem.

Aláírt levelezés, ügyfél → bank

Hogyan?

- Példa: A bank kizárólag aláírt levelet fogad el az ügyféltől. A támadónak alá kell íratnia valamit az ügyféllel. Ha az ügyfél hajlandó aláírni, amit a támadó kér, akkor megérdemli.

Felvetülő kérdések

- Célszerű chipkártyán tárolni a felhasználó magánkulcsát.
- Hogy dönti el a bank, hogy ki készítette az aláírást? (Nem triviális, de léteznek megoldások.)
- Aláírás $\leftrightarrow$ Authentikáció
- Feltört gépek?
- Kevesen használják...

Összegzés

Összegzés

- Gyakran hallani, hogy:
 - ❑ „Nincs tanúsítványod, ezért nem vagy biztonságos!”
 - ❑ „Vegyél tanúsítványt, mert akkor biztonságban leszel!”... ez nem ilyen egyszerű.
- A PKI számos nagyon jó eszközt kínál, ezek – megfelelő feltételek mellett, más eszközökkel együtt – van, amire jól használhatóak.
- A phishing üzeneteknek kevesen dőlnek be, de a támadónak így is megéri. Drasztikus csökkentés PKI-val?
- A PKI nagyon jó eszköztárat kínál...
- ... de egy nem technológia problémára ne a technológiától várjuk a megoldást.



További info

- <http://www.berta.hu>
- http://www.e-szigno.hu/?lap=tudasbazis_webszerver
- <http://www.e-szigno.hu/?lap=tudasbazis>
- http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf
- http://www.schneier.com/blog/archives/2005/03/the_failure_of.html
- <http://www.schneier.com/crypto-gram-0303.html#3>

PKI az adathalászat (phishing) ellen?

Dr. Berta István Zsolt <istvan.bertha@microsec.hu>
PhD, MBA, CISA

Microsec Kft.