Webes biztonság

IT Biztonság Témalaboratórium 2017 ősz

Közérdekű

Magamról

- Hegedűs Tamás vendégelőadó
- Korábbi műegyetemi hallgató
- A CrySys Student Core és a !SpamAndHex magyar hackercsapat tagja
- Neptunhoz és adminisztratív rendszerekhez nem férek hozzá

A tananyag webes részéről bátran kérdezzetek engem, piazzan keresztül elértek. Az előadást Molnár Gábor “Web Application Security” anyagából tartjuk.

Közérdekű

A Web Security laboralkalmak programja

- Október 2.: előadás
- Október 9.: Avatao feladatok, vezetett gyakorlat
- Október 16.: önálló Avatao feladatmegoldás

Miért beszélünk a webes biztonságról?

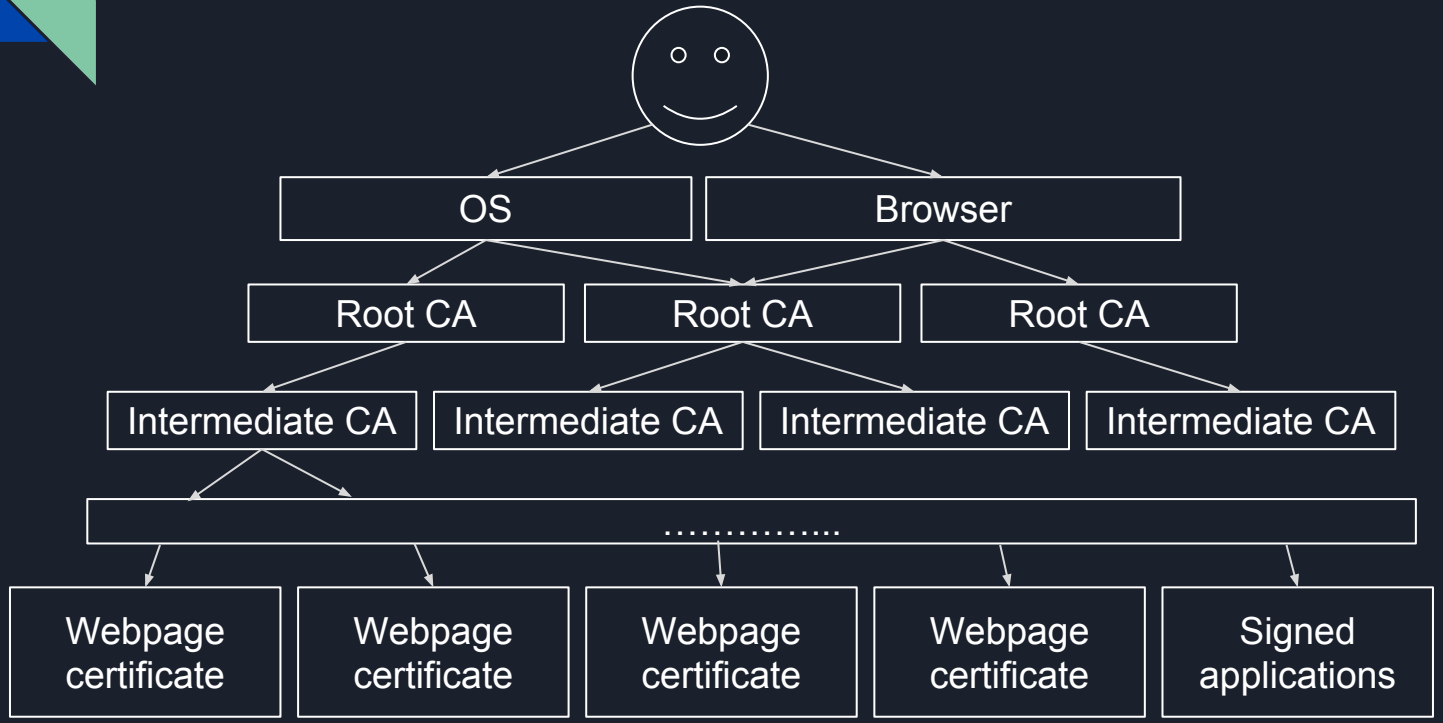
- Az eredeti világhálót egyetemek közötti kommunikációra tervezték, nem készültek rosszindulatú felhasználókra
- Az internet széleskörű elterjedésével párhuzamosan próbálják befoltozni a biztonsági réseket mind az szoftverfejlesztő cégek, mind a globális szabványosító szervezetek
- Következmény #1: folyamatosan válnak elérhetővé jobb és jobb best practicek
- Következmény #2: régi webes alkalmazások amiket nem tartanak karban gyakran sebezhetőek
- Következmény #3: A “secure by default” elv nem teljesülhet a visszamenőleges kompatibilitás miatt
- Következmény #4: Sok új webes alkalmazás eleve sérülékenyen készül
- Következmény #5: Emberek millliárdjai használnak sebezhető szolgáltatásokat nap mint nap

Kiegészítés: Web Application Security HTTP/S Proxies

Windows: Fiddler

Linux: mitmproxy

PKI - Public Key Infrastructure



PKI - Public Key Infrastructure

- OS: Windows, OSX, Android, Ubuntu - mindnek van saját “certificate store”-ja
- Böngésző: Chrome, Safari, Firefox, Edge - többnyire az OS tanusítványait használják, de lehet saját storejuk is
- Root CA: GeoTrust Global, VeriSign, etc… - páncélszekrényben őrzött privát kulcsok
- Intermediate CA: Google, Symantec, etc... - tőlük lehet saját certificatet venni, gyakrabban veszik elő a privát kulcsaikat
- … több szintnyi Intermediate CA is lehet, egy cégnek több aláírókulcsa is lehet, így kisebb a kár ha valamelyik kulcsot ellopják
- Website vagy aláírt program tanusítványa, további aláírásra nem alkalmas, de az eredetiség a láncolaton keresztül ellenőrizhető egészen a legfelső szintig