# Bezpečnost

Lenka Kosková Třísková, NTI TUL

22. března 2013

# Technologie

- Symetrické vs. asymetrické šifry (dnes kombinace)
- HTTPS
  - Funguje nad HTTP
  - Šifrování s pomocí SSL nebo TLS
  - Šifrování chrání před odposlechem
  - Výměna klíčů jiným kanálem před útokem typu MIM
  - SSL labs: `https://www.ssllabs.com`
- Demo: SSL Labs pro STAG

# SSL

- Jen protokol, nezávislý na volbě šifrovacích algoritmů
- Umožňuje více spojení
- Volba algoritmů na začátku relace
- Dvě úrovně protokolů (SSL handshake, SSL Record protokol)
- SSL record protocol: spojení šifrovaná rychlou sym. šifrou
- Cipher suite: definice as. algoritmů pro autentizaci, klíč pro hanshake, definice sym. protokolů pro record protokol
- Při detekci chyby mohou pokračovat ostatní spojení, nelze navázat nová.

# Certifikáty a autority

- Certifikát = ověření totožnosti (serveru)
- Sdílení důvěry: certifikát vydá a podepíše certifikační autorita (CA)
- CA dbá o svou důvěryhodnost (nepodepíše podvrženou identitu)
- Klíče CA jsou instalovány v prohlížeči a slouží k ověření přijatých certifikátů
- Placené certifikáty - např. pro komunikaci se státem (v ČR garance MV, zákon o el. podpisu)
- Demo: Seznam CA na MV ČR

# HTTP autentizace

- Standardní součást protokolu HTTP
- Vyskakuje samostatné přihlašovací okno (nelze měnit)
- Dána vlastnostmi webového serveru
- V naprosté většině použití nekóduje hesla
- Nevýhoda: nelze odhlásit uživatele, relace nevyprší

# HTTP Autentizace - httpd (apache)

- Soubor .htaccess (konfigurace) a .htpasswd (hesla)
- Hesla generuje příkaz htpasswd, ukládá kódovaná do souboru
- V souboru .htaccess direktivy AuthUserFile, AuthName, AuthGroupFile, AuthType

# Vlastní formulář a sessions

- Formulář pro přihlášení
- Obsluha s pomocí session proměnné
- Odhlášení - zrušení session
- Dočasné přihlášení: vyprší časové razítko v session (čas posledního přístupu k serveru)
- S JavaScriptem na straně klienta lze heslo posílat kódované
- Demo: Session pro STAG

# Certifikát na straně klienta

- Typicky banky, armáda, apod.
- Certifikát klienta by měl být chráněný před zápisem (klíčenka)
- Uživatelsky náročné, problém ochrany certifikátu

# Další metody autentizace

- SMS: Unikátní kód pro danou operaci zaslaný přes SMS (předpokládáme bezpečný kanál)
- OTP: Jednorázová hesla generovaná kalkulačkou na straně klienta
- Předgenerovaná OTP: Klient dostane seznam již vygenerovaných OTP, která postupně spotřebuje
- Skutečná asymetrická komunikace (na serveru veřejný klíč klienta)

# OpenID

- Snahou je sjednodit přihlašování do více různorodých aplikací do jednoho ID
- Unikátní URL spolu s heslem
- Uživatel si nárokuje přístup k určité digitální identitě
- Metoda ověření identity je dána poskytovatelm OpenID
- Google (používá e-mail, ne url), PayPal, Seznam

# Solení hesel

- VŽDY ukládáme heslo kódované
- Samotný otisk málo (slovníky a rainbow tables)
- Nutné změnit hash hesla
  - Voláme: hash(heslo+sůl), získáme jiný otisk pro stejné heslo
  - Sůl: číslo, uživatelské jméno, cokoliv - cílem je změnit hash
  - Dobré proti útoku s rainbow tables - nefungují
  - Ukradenou tabulku otisků hesel nejde použít pro jinou službu
  - Každý uživatel má svou sůl - potom nenajdeme uživatele se stejným heslem

# Uživatelský vstup

- Formulářová pole (rovnou útočný kód)
- URL požadavku (podstrčená proměnná, řetězec pro zásobník serveru)
- Cookies (ukradená session)
- Hlavičky (útok na proměnnou)

# Cross site scripting (XSS)

- Problém neošetřených speciálních znaků ve vstupním poli formuláře
- Nebezpečné i vkládání URL, částí skriptů či šablon
- Útok proběhne podstrčením JavaScriptu s kódem nebo podstrčením odkazu na sever útočníka
- V PHP funkce `htmlspecialchars`
- `http://php.vrana.cz/cross-site-scripting-poradne.php`
- `htmlpurifier.org`: PHP knihovna
- Demo: Článek ze zdrojáku
- Demo: HTMLPURIFIER
- Demo: Kosek.cz - neinicializovaná proměnná