Jen správně nasazené HTTPS je bezpečné

Petr Krčmář

12. listopadu 2015

Prezentace už teď na webu

www.petrkrcmar.cz

Proč nasazovat HTTPS?

- HTTPS není jen pro banky a mail
- autenticita přenášených dat
- odposlech je považován za útok (RFC 7258)
- pozměňování přenosů, supercookies, malware
- ochrana osobních údajů
- zabránění únosu session cookie
- možnost nasazení HTTP/2 – výkon

ROOT.CZ vpsFree.cz

Proč nasazovat HTTPS?

- HTTPS není jen pro banky a mail
- autenticita přenášených dat
- odposlech je považován za útok (RFC 7258)
- pozměňování přenosů, supercookies, malware
- ochrana osobních údajů
- zabránění únosu session cookie
- možnost nasazení HTTP/2 – výkon
- SSH je normální, proč používat telnet?

Transport Layer Security

- TLS je nový název pro SSL
  změna názvu kvůli sporům s Netscape
  TLS 1.0 je vlastně SSL 3.1
- rychle se vyvíjí – bezpečnější varianty
  současná verze je TLS 1.2, vyvíjí se 1.3
- bezpečný tunel pro přenos dat
- zajišťuje šifrování a autentizaci
- používá asymetrickou i symetrickou kryptografii
- autentizace asymetrická, šifrování symetrické
- používá infrastrukturu veřejného klíče (PKI)

Nasadit vs. nasadit dobře

> „To je past vedle pasti…“
>
> — Luboš při opravě Lakatoše

- volba aktuálních protokolů
- volba bezpečných šifer
- generování klíčů
- získání certifikátu
- správná konfigurace
  (posílání celé cesty)
- stálé aktualizace – situace se rychle vyvíjí
- a další špeky…

Verze SSL/TLS

- SSL 1.0 – nikdy nevydána veřejně, nebezpečná
- SSL 2.0 – zastaralá od roku 2011, RFC 6176
- SSL 3.0 – zastaralá od června 2015, RFC 7568
- TLS 1.0 – od ledna 1999, pozor downgrade na SSL
- TLS 1.1 – od dubna 2006
- TLS 1.2 – od srpna 2008, ruší kompatibilitu se SSL
- TLS 1.3 (draft) – odstraní spoustu zastaralých standardů

Známé útoky na protokoly

- Renegotiation attack – přidání plaintextu na začátek komunikace
- Heartbleed – implementační chyba, vylákání dat z paměti (klíčů)
- BEAST – dešifrování zprávy v SSLv3 a TLSv1.0
- POODLE – dešifrování zprávy v SSLv3 a TLSv1.0
- CRIME – dešifrování obsahu stránky při zapnuté kompresi TLS
- FREAK – vyjednání přechodu na slabé 512bitové klíče
- Logjam – vyjednání přechodu na slabou sadu veřejných DH parametrů
- a další...

Známé slabiny šifer

- RC4 – dlouhodobě slabá, prohlížeče zakázaly
- 3DES – nebezpečná, součástí TLS 1.2
- IDEA – nebezpečná, odstraněna z TLS 1.2
- DES – nebezpečná, odstraněna z TLS 1.2
- RC2 – nebezpečná, odstraněna z TLS 1.1
- a další...

Jak správně

- kombinace několika problematických algoritmů: výměna klíčů, autentizace, blokové šifry, hashování
- výsledek: nikdo tomu nerozumí, stálé změny
- bezpečnost vs. kompatibilita s klienty
- použijte doporučení BetterCrypto.org

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+ \
\aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:! \
\eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256 \
\-SHA:CAMELLIA128-SHA:AES128-SHA';
```

Generování DH parametrů

- pro Diffie–Hellman key exchange
- forward secrecy – bezpečnost do budoucna
- klíče se nedají zjistit ani po dešifrování handshake
- Logjam umožňuje nasazení slabých předgenerovaných parametrů
- nutné vypnout a vygenerovat vlastní 2048bitové
- poté vložit do konfigurace serveru
- info a test na weakdh.org

```
openssl dhparam -out dhparams.pem 2048
```

Správné nasazení certifikátů

- tři druhy certifikátů: DV, OV, EV
  - DV: manipulace doménou
  - OV: + právo zastupovat organizaci
  - EV: + detailní prověření organizace a lidí
- tisíce delegovaných autorit
- existence DV ničí princip PKI
- privátní klíč, certifikát, cesta(!)
- pozor na mixed content

Content-Security-Policy: upgrade-insecure-requests

Princip PKI

- kořenový certifikát → mezilehlý → serverový certifikát
- cest může být více (cross-signing)
- mezilehlých certifikátů může být víc
- vydává se na základě CSR
  použije se jen veřejný klíč
- autorita ověří (různé) a vystaví cert
- certifikát obsahuje podrobnosti:
  - platnost (od do)
  - název subjektu (doména)
  - alternativní názvy
  - omezení certifikátu
  - veřejný klíč
  - podpis autority…

Kde vzít a nekrást? (certifikát)

- vygenerovat vlastní – nedůvěryhodný
- koupit – ceny od ~200 Kč
- pořídit zadarmo
  - StartSSL – nekomerční, jedno jméno
  - WoSign – jedno jméno (další za dva dolary)
- Let’s Encrypt – zdarma a automaticky

Downgrade attack to HTTP

- pořád existují vektory útoků
- řeší HTTP hlavičky HSTS a HPKP
- nejobvyklejší downgrade na HTTP
  - většina lidí píše „facebook.com“ – přesměrování
  - HTTP Strict Transport Security (HSTS)
    tady se musí šifrovat – není cesty zpět (Wiki v Rusku)
  - není to pro každého(!)
- nebo náhrada jinou autoritou
  - HTTP Public Key Pinning (HPKP)
    v cestě musí být tento certifikát nebo záložní klíč
  - „chtěné“ MitM útoky neprojdou – antiviry
- obojí má preloaded variantu v prohlížečích
- DANE bohužel není v prohlížečích

ROOT.CZ vpsFree.cz

Čím to otestovat?

- SSL Labs Test – velmi podrobný test
- SSL Decoder – vypíše všechny detaily o certifikátech
- Symantec CryptoReport – protokoly, chyby, díry
- GeoCerts SSL Checker – ukazuje řetězec
- COMODO SSL Analyzer – a ještě jeden
- gcr-viewer v balíčku gnome-keyring

```
openssl s_client -showcerts -connect www.root.cz:443 < \
/dev/null | openssl x509 -outform DER > cert.der
```

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz