APIS IT

Agencija za podršku informacijskim sustavima i informacijskim tehnologijama d.o.o.

Ivan Pozderović, APIS IT d.o.o.
Tomislav Koren, APIS IT d.o.o.
Želimir Pećnik, APIS IT d.o.o.

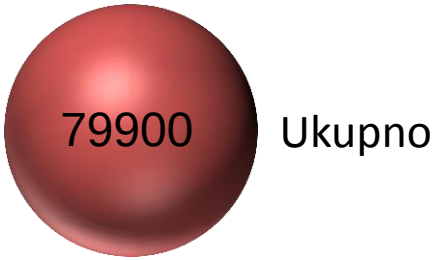
# Prelazak na TLS protokol

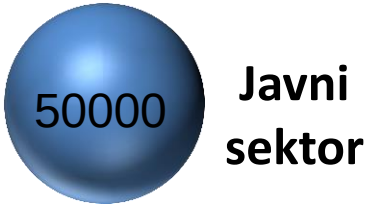
# Sadržaj

- Broj sigurnosnih incidenata 2015.
- SSL/TLS – ranjivosti
- SSL/TLS – općenito
- SSL/TLS – izazovi programske podrške
- SSL/TLS – podrška web preglednika
- Zaključak

# Broj sigurnosnih incidenata 2015.

Verizon Data Breach Investigations Report 2015



Verizon Data Breach Investigations Report 2015

***"About half of the CVEs exploited in 2014 went from publish to pwn in less than a month"***

***„…we can see that the majority of data breaches are attributed to point-of-sale attacks (28.5%), while crimeware (18.8%) and cyber-espionage are tied for the #2 spot."***

# SSL/TLS - ranjivosti

- Poznatije ranjivosti (2009. – 2013.)
  - Insecure TLS Renegotiation (kolovoz 2009.)
  - BEAST – Browser Exploit against SSL/TLS (rujan 2011.)
  - CRIME – Compression Ratio Info-leak Made Easy (rujan 2012.)
  - RC4 napadi (ožujak 2013.)
  - BREACH – Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext (kolovoz 2013.)

# SSL/TLS - ranjivosti

- Poznatije ranjivosti (2014. – 2016.)
  - Heartbleed (travanj 2014.) – izloženo 66% internet prometa
  - POODLE – Padding Oracle On Downgraded Legacy Encryption (listopad 2014.)
  - FREAK – Factoring RSA Export Keys (ožujak 2015.)
  - DROWN – Decrypting RSA with Obsolete and Weakened eNcryption (ožujak 2016.)
  - ? (kolovoz 2017.)

# SSL/TLS - ranjivosti

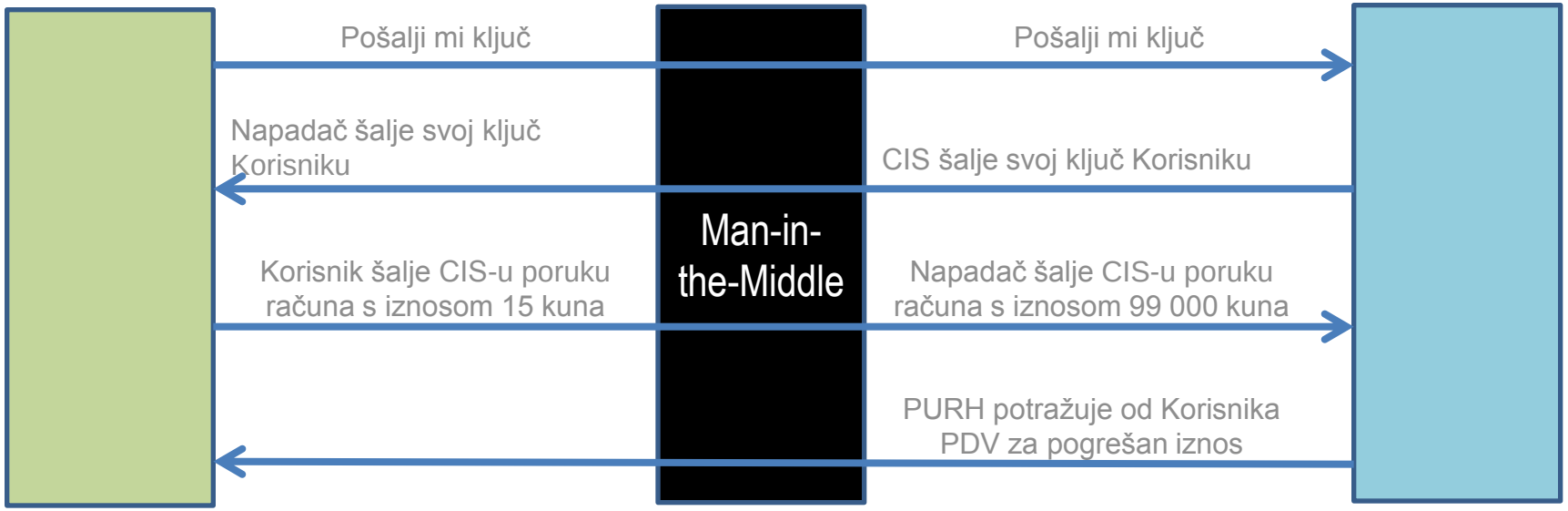
- POODLE - Padding Oracle On Downgraded Legacy Encryption
  - *Man-in-the-middle* napad, označio kraj korištenja SSLv3
  - Bodo Möller, Thai Duong and Krzysztof Kotowicz – Google Security Team (2014.)
  - relativno jednostavno iskorištavanje ranjivosti (*the POODLE vulnerability is real*)
  - Koristi ranjivost SSL 3.0 (1996. godina) i TLS 1.0 (1999. godina) protokola

# Primjer Man-in-the-Middle napada

**Korisnik fiskalizacije**

**Napadač**

**CIS PURH**



# SSL/TLS - općenito

*The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP), is the TLS Record Protocol.*

Izvor: T. Dierks, TLS Protocol, Version 1.2 (Kolovoz 2008)

# SSL/TLS - općenito

- Kriptografski protokoli
  - omogućavaju sigurnu komunikaciju putem računalne mreže
- Široka primjena
  - koriste se u: web preglednicima, e-mailu, *instant-messaging* klijentima, VoIP-u
- Osnovne značajke
  - enkripcija podataka (AES, RC4) putem unikatnih simetričnih ključeva
  - provjera integriteta (SHA-1, SHA-2) putem *hash* funkcija
  - provjera identiteta (RSA, DSA) putem asimetričnih ključeva (javni i privatni)

# SSL/TLS – izazovi programske podrške

- Programi koji koriste .Net Framework
  - inačice 3.5 i 4.0 podržavaju samo TLS v1.0
  - inačica 4.5 podržava TLS v1.2
  - problem sa Windows Vista/Windows Server 2008 i starijim sustavima – podrška samo za .Net inačicu 4
- Programi koji koriste OpenSSL
  - npr. cURL (*cross-platform* alat)
  - OpenSSL podržava TLS v1.2 od inačice 1.0.1 (ožujak 2012.)
- Programi koji koriste *custom* rješenja
  - razmotriti mogućnost korištenja neovisnih biblioteka

# SSL/TLS – podrška web stranica

| Protocol version | Website support | Security |
|---|---|---|
| SSL 2.0 | 7.0% (±0.0%) | Insecure |
| SSL 3.0 | 24.4% (±0.0%) | Insecure |
| TLS 1.0 | 97.8% (±0.0%) | Depends on cipher and client mitigations |
| TLS 1.1 | 74.0% (±0.0%) | Depends on cipher and client mitigations |
| TLS 1.2 | 76.4% (+0.1%) | Depends on cipher and client mitigations |

Izvor: Wikipedia, srpanj 2016.

# SSL/TLS – podrška web preglednika

| Web preglednik | SSL 3.0 | TLS 1.0 | TLS 1.1 | TLS 1.2 | POODLE | BEAST | FREAK |
|---|---|---|---|---|---|---|---|
| Internet Explorer 10 | DA + | DA | DA - | DA - | DA | M | M |
| Internet Explorer 11 | DA - | DA | DA | DA | M | M | M |
| Google Chrome 48-49 | NE | DA | DA | DA | NE | NE | M |
| Google Chrome 50-51 | NE | DA | DA | DA | NE | NE | M |
| Mozilla Firefox 44-48 | NE | DA | DA | DA | NE | NE | NE |
| Mozilla Firefox 49 | NE | DA | DA | DA | NE | NE | NE |

+ Enabled by default - Disabled by default M Mitigacija

# Zaključak

- Zaštitni mehanizmi i protokoli evoluiraju s vremenom
  - jedna značajna ranjivost je otkrivena godišnje u prosjeku
  - SSL v3 nadogradio SSL v2 – 1996.
  - TLS v1.0 nadogradio SSL v3 – 1999.
  - TLS v1.1 nadogradio TLS v1.0 – 2006.
  - TLS v1.2 nadogradio TLS v1.1 – 2008.
  - TLS v1.3 će nadogradit TLS v1.2 – u pripremi

# Zaključak

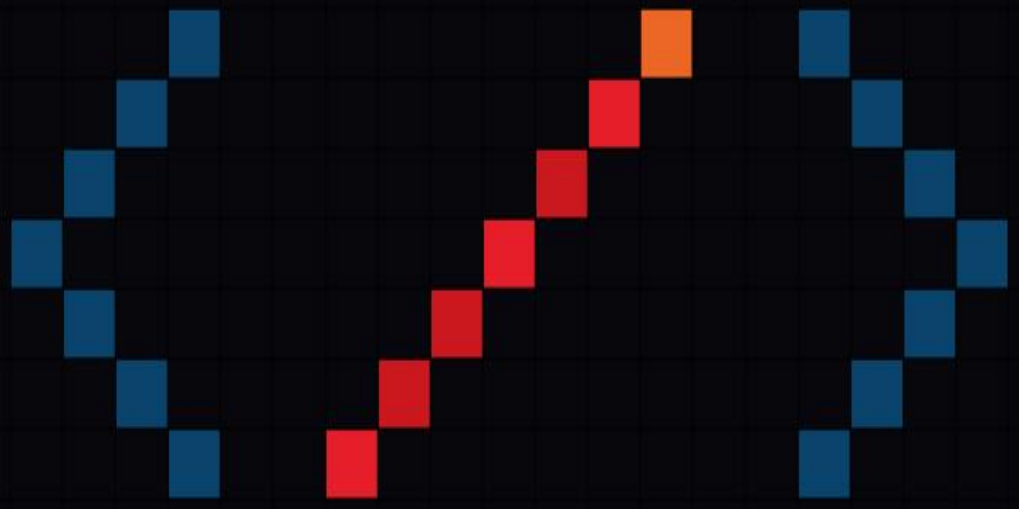
- Nije moguće napraviti trajno rješenje bez rizika
  - rizik se povećava s vremenom, napretkom tehnologije i otkrivanjem sigurnosnih propusta (kako u implementaciji, tako i u samim protokolima)
- Ranjivosti SSL/TLS protokola su prepoznate diljem tržišta
  - npr., PCI DSS v3.1 standard zahtijeva korištenje minimalno TLS_v1.1 (od 30. lipnja 2016.)
  - APIS IT mora pratiti standarde i dobre prakse, kako bi osigurali siguran pristup svojim korisnicima
- Preporuka je koristiti **TLS v1.2** ili TLS v1.1

# Zaključak

**Ukidanje podrške za SSL v3 i TLS v1.0 na CIS-u Porezne uprave**

**TESTNA OKOLINA – 1. rujna 2016.**

**PRODUKCIJSKA OKOLINA – 9. siječnja 2017.**



# Hvala na pažnji

www.apis–it.hr