Útoky na HTTPS

PV210 - Bezpečnostní analýza síťového provozu

Pavel Čeleda, Radek Krejčí

Ústav výpočetní techniky
Masarykova univerzita
celeda@ics.muni.cz

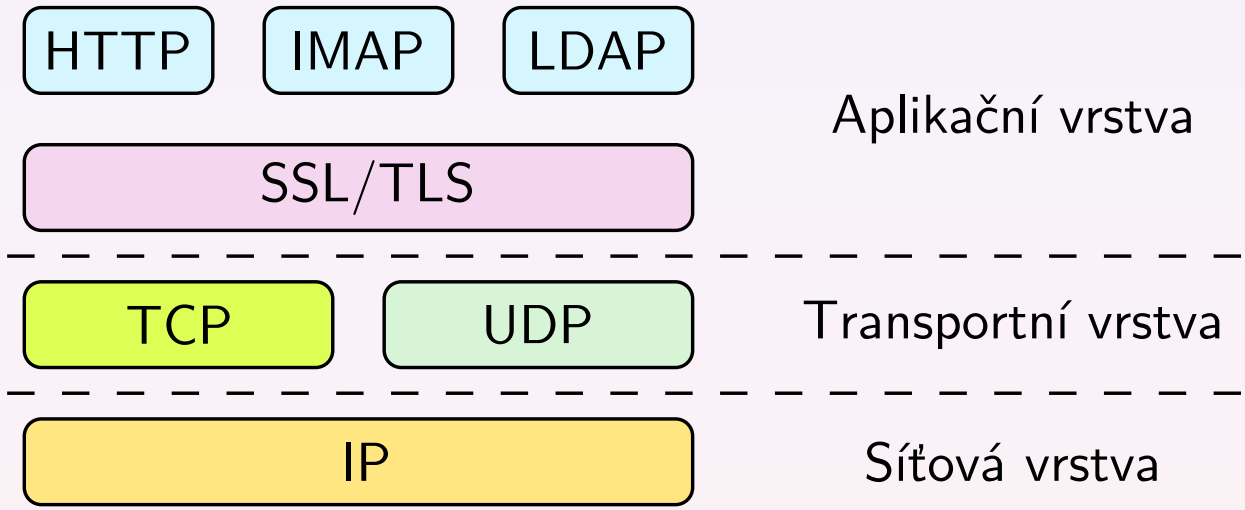
Brno, 5. listopadu 2014

O čem budeme mluvit?

Protokol HTTPS

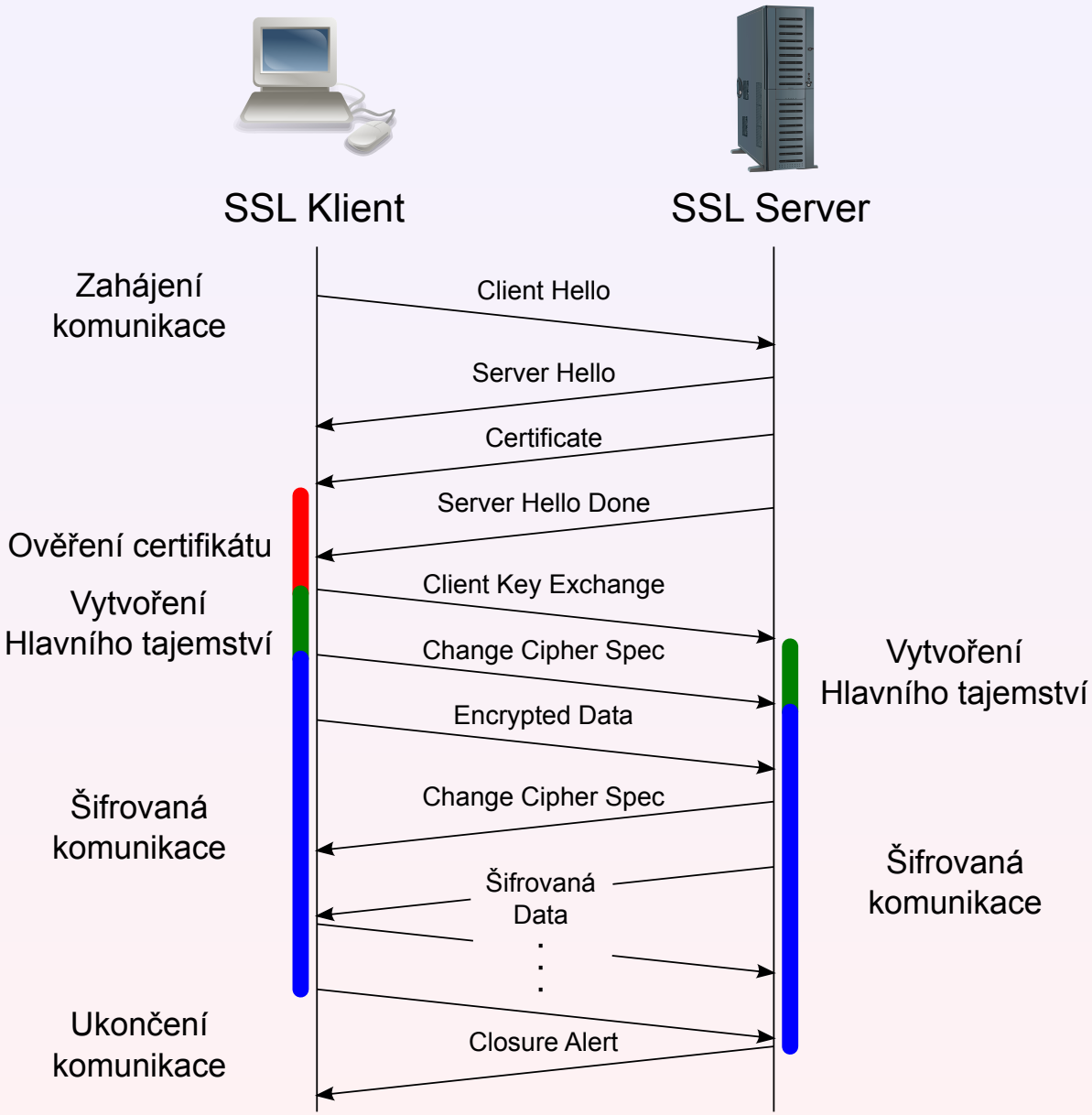
- *Hypertext Transfer Protocol Secure*
- ve skutečnosti dvojice protokolů:

  SSL/TLS + aplikační protokol (HTTP)



- historie protokolů SSL/TLS
  - SSL (*Secure Socket Layer*) – Netscape Communications
  - TLS (*Transport Layer Security*) – IETF (RFC standardy)

Protokol HTTPS



Certifikáty a PKI

Certifikát – Sada identifikačních údajů (norma X.509)

EV Certif. – (Extended Validation) – certifikát s přísnějšími podmínkami vydávání

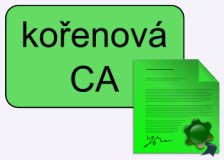
CA – Certifikační Autorita

PKI – Public Key Infrastructure

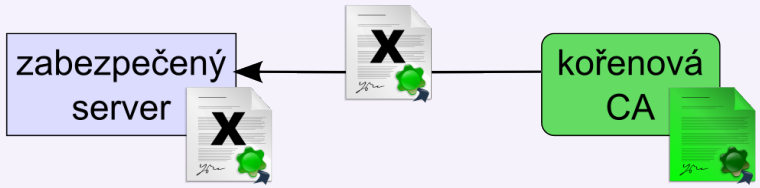
Ověření certifikátu

1. Kolikátého je dnes?
2. Znám tě?
3. Umíš se podepsat?
4. Jak se jmenuješ?

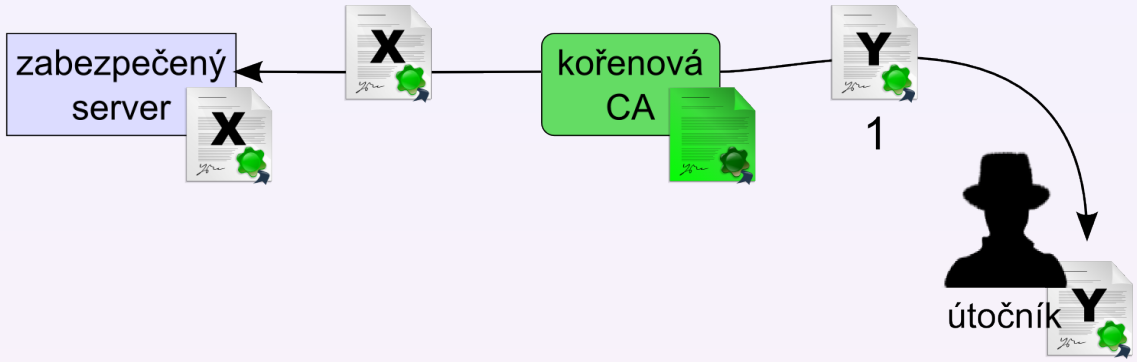
Kolizní součty MD5



Kolizní součty MD5

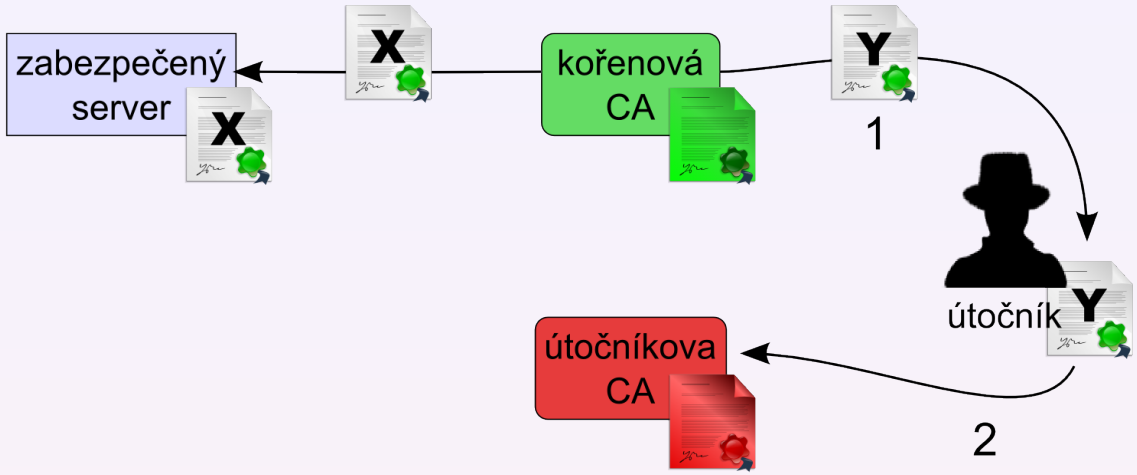


Kolizní součty MD5



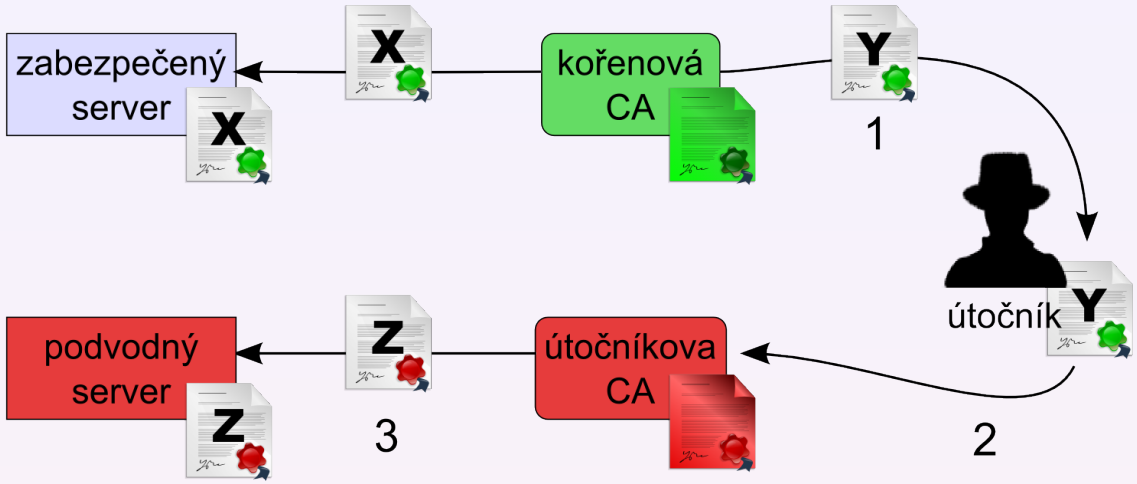
1. Vydání certifikátu útočníkovu serveru

Kolizní součty MD5



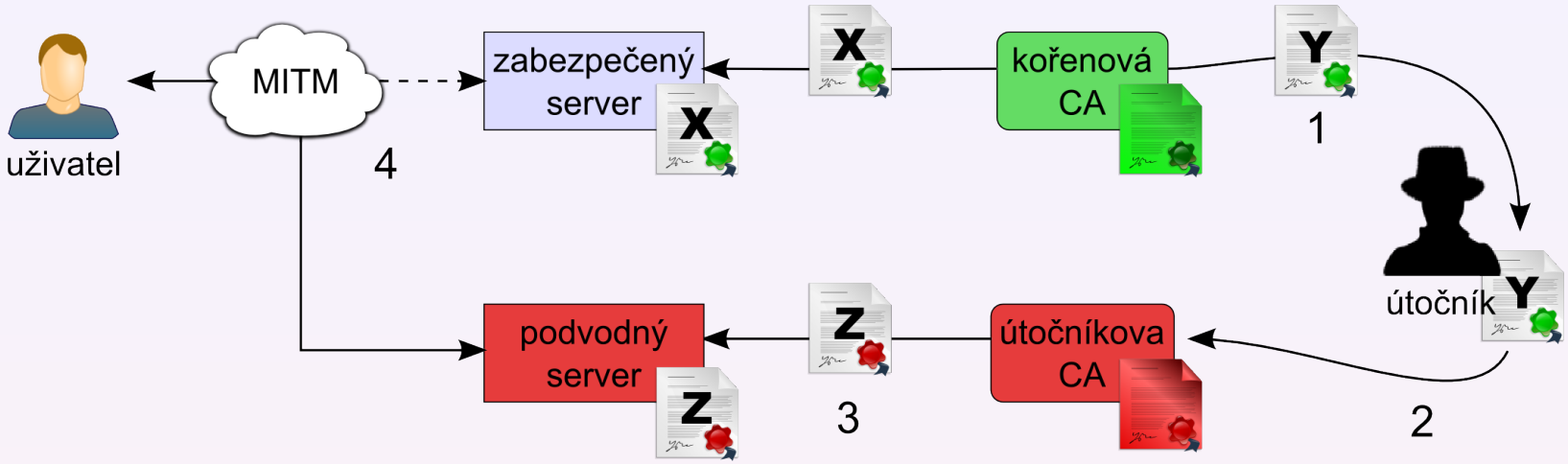
1. Vydání certifikátu útočníkovu serveru
2. Kolizí MD5 vytvořený certifikát CA útočníka

Kolizní součty MD5



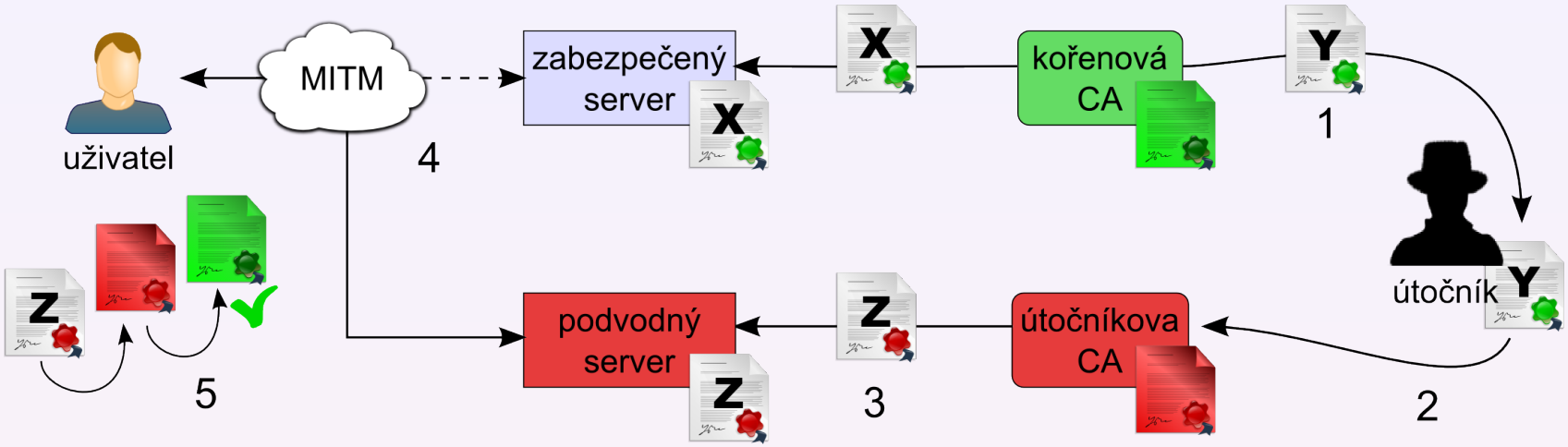
1. Vydání certifikátu útočníkovu serveru
2. Kolizí MD5 vytvořený certifikát CA útočníka
3. CA útočníka vydává certifikáty serverům

Kolizní součty MD5



1. Vydání certifikátu útočníkovu serveru
2. Kolizí MD5 vytvořený certifikát CA útočníka
3. CA útočníka vydává certifikáty serverům
4. MITM útok a přesměrování na podvodný server

Kolizní součty MD5



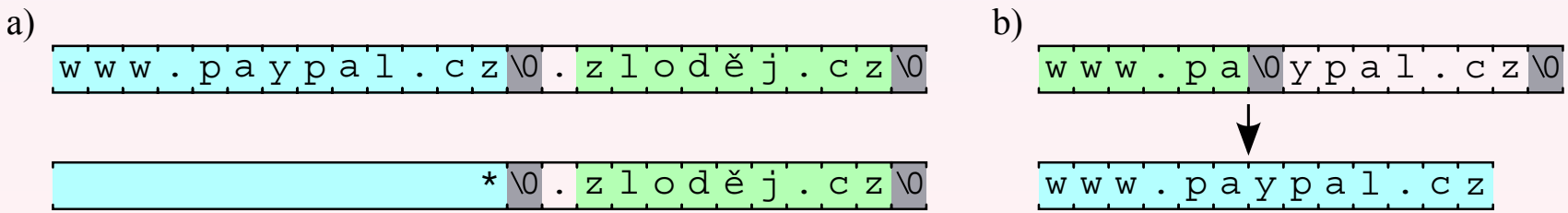
1. Vydání certifikátu útočníkovu serveru
2. Kolizí MD5 vytvořený certifikát CA útočníka
3. CA útočníka vydává certifikáty serverům
4. MITM útok a přesměrování na podvodný server
5. Přenos důvěrnosti a platná kontrola certifikátu

Null-prefix certifikáty

- Útok využívá chyby v implementaci ověřování certifikátu.

Postup

1. Žádost útočníka o certifikát pro doménu
   `www.paypal.cz\0.zlodej.cz`
2. MITM útok a přesměrování oběti na útočníkův server vydávající se za `www.paypal.cz`
3. Klient ověřuje certifikát
   (vydaný pro `www.paypal.cz\0.zlodej.cz`)
4. Certifikát souhlasí



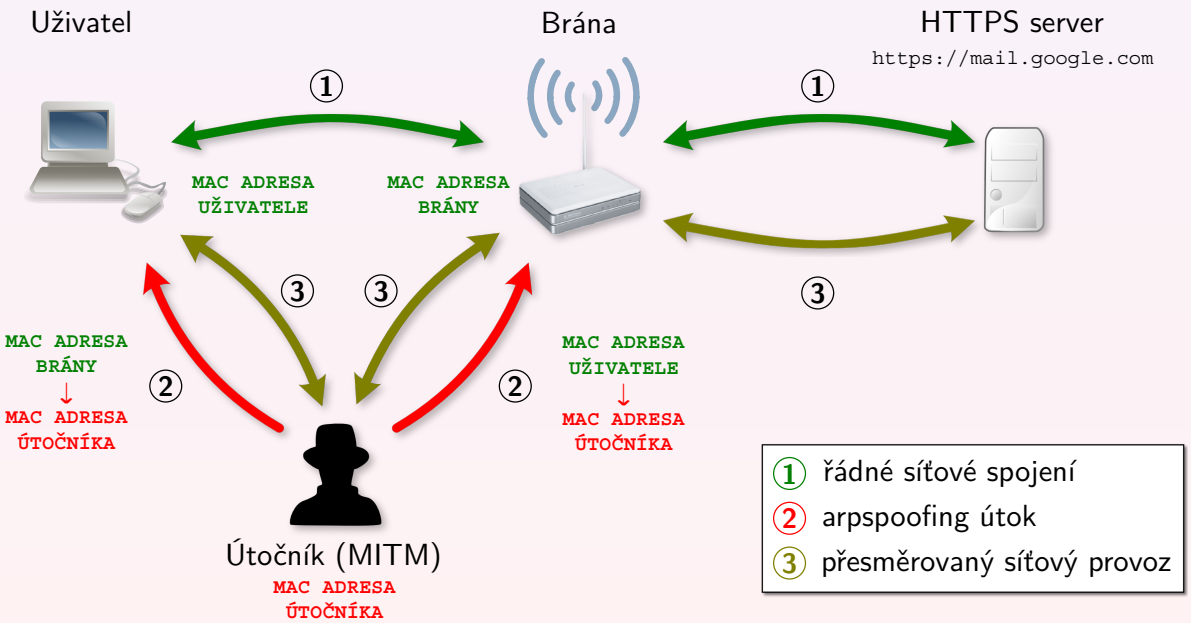
Odposlech HTTPS

MITM

- ARP spoofing, (DNS spoofing)
- ovládnutí aktivního prvku sítě (Chuck Norris botnet)
- nástroj *sslsniff* (`http://www.thoughtcrime.org/software/sslsniff`)

Útočník v roli MITM může

- pomocí privátního klíče serveru dešifrovat komunikaci
- přerušit komunikaci oběti a vystupovat jako koncový server



SSL Strip

Uživatel

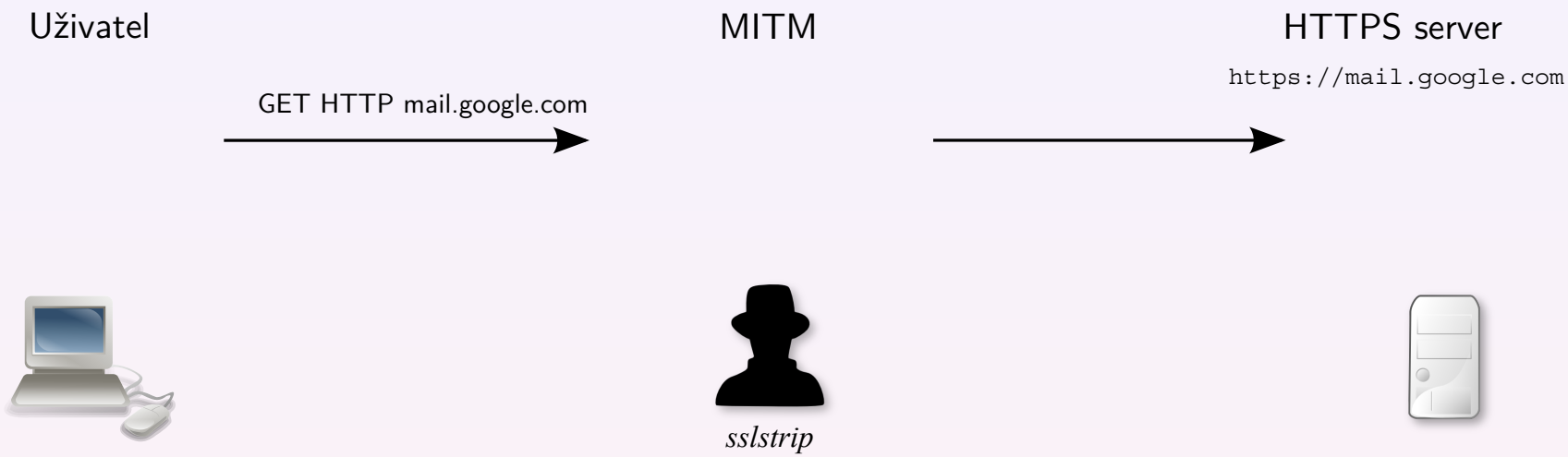
MITM

HTTPS server

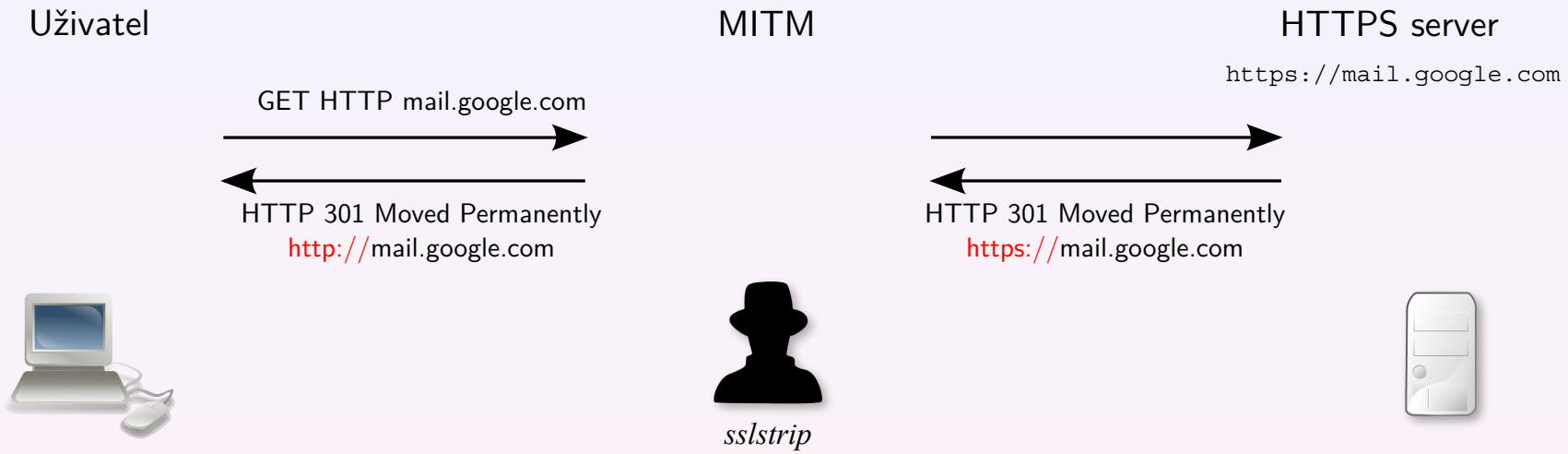
`https://mail.google.com`

sslstrip

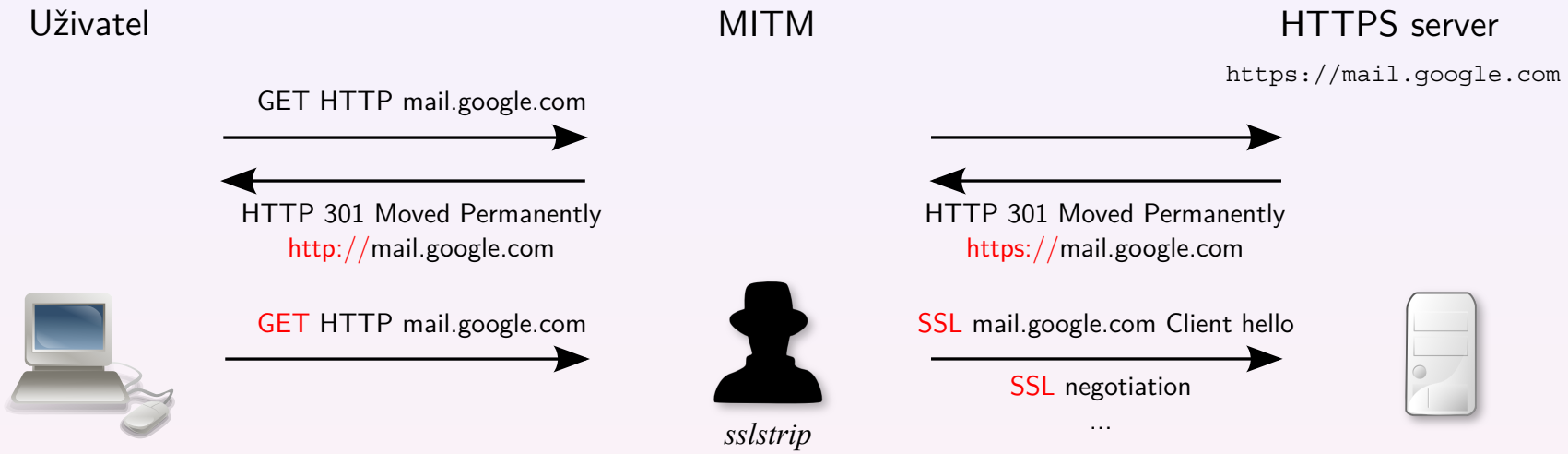
SSL Strip


Uživatel
MITM
HTTPS server
https://mail.google.com
GET HTTP mail.google.com
sslstrip

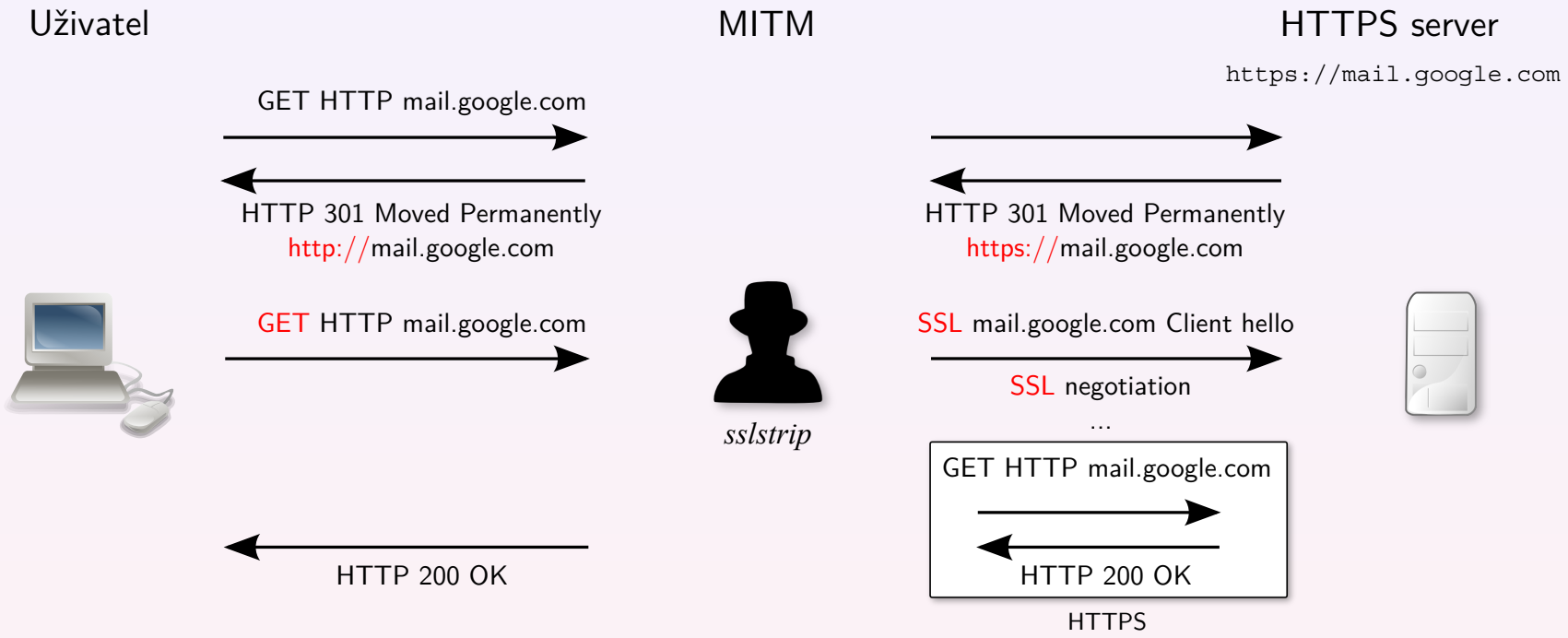
SSL Strip


Uživatel
MITM
HTTPS server
https://mail.google.com
GET HTTP mail.google.com
HTTP 301 Moved Permanently
http://mail.google.com
HTTP 301 Moved Permanently
https://mail.google.com
sslstrip

SSL Strip


Uživatel
MITM
HTTPS server
https://mail.google.com
GET HTTP mail.google.com
HTTP 301 Moved Permanently
http://mail.google.com
GET HTTP mail.google.com
SSL mail.google.com Client hello
SSL negotiation
...
sslstrip

SSL Strip


Uživatel
MITM
HTTPS server
https://mail.google.com
GET HTTP mail.google.com
HTTP 301 Moved Permanently
http://mail.google.com
HTTP 301 Moved Permanently
https://mail.google.com
GET HTTP mail.google.com
SSL mail.google.com Client hello
SSL negotiation
...
sslstrip
GET HTTP mail.google.com
HTTP 200 OK
HTTP 200 OK
HTTPS

Zranitelnost renegociace SSL/TLS spojení I

renegociace = znovuvyjednání parametrů SSL/TLS spojení

- Problém je přímo v (nejasné) specifikaci protokolu.
- Řeší RFC 5746 – TLS Renegotiation Indication Extension.
- Původně jen přidávání vlastních dat do požadavků klienta, ale bez možností získat výsledek.

Zranitelnost renegociace SSL/TLS spojení II

SSL Klient

útočník

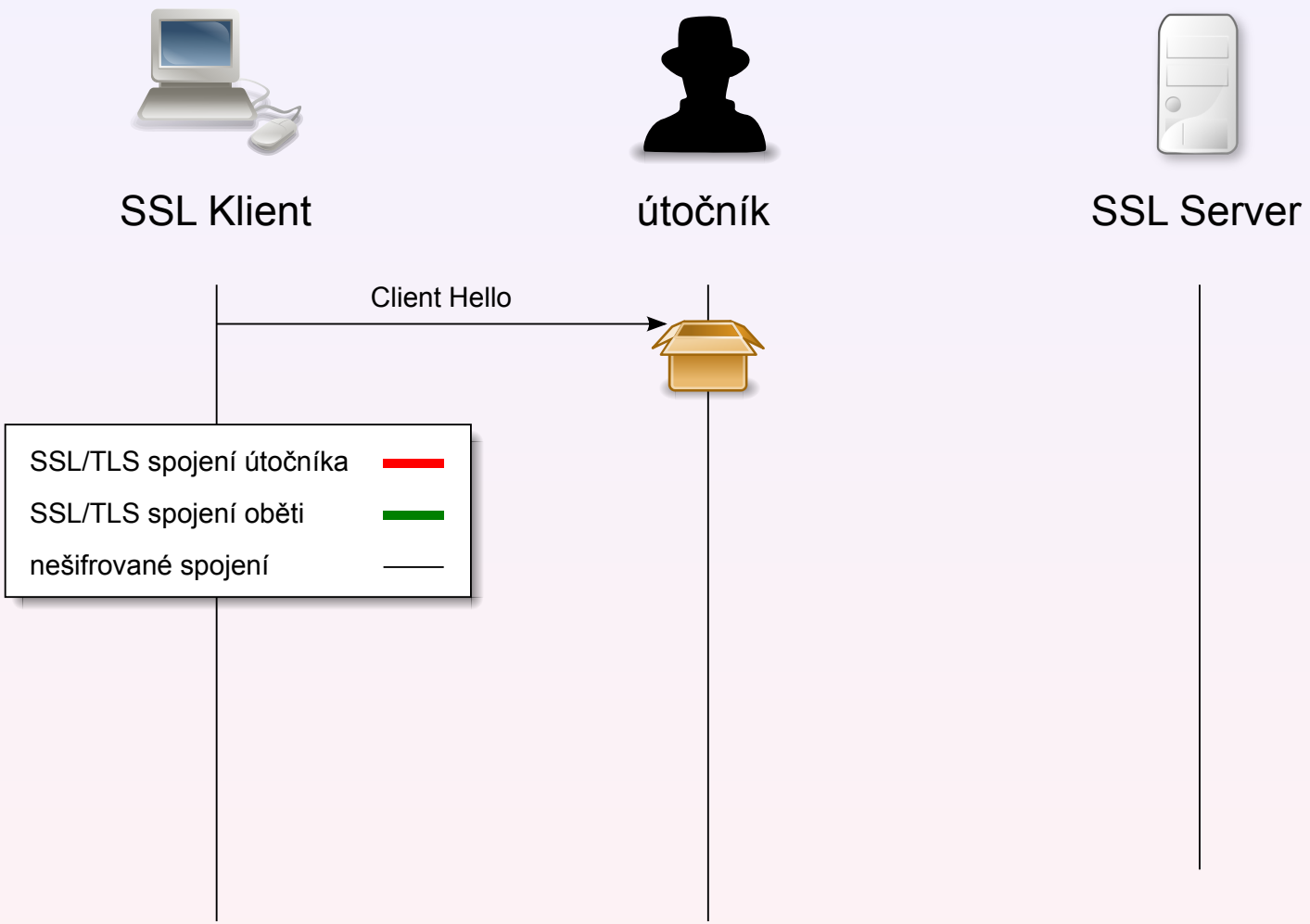
SSL Server

SSL/TLS spojení útočníka

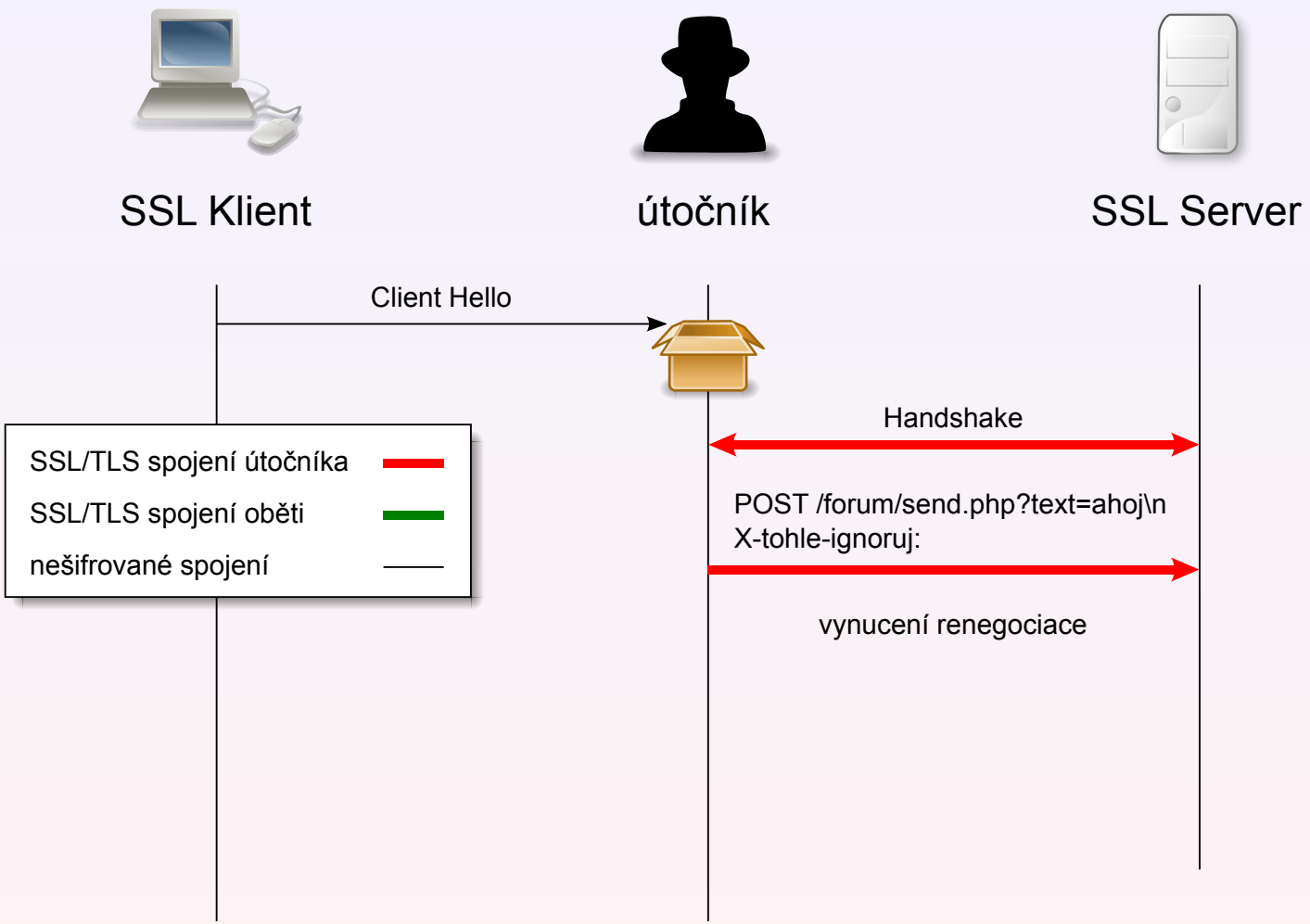
SSL/TLS spojení oběti

nešifrované spojení

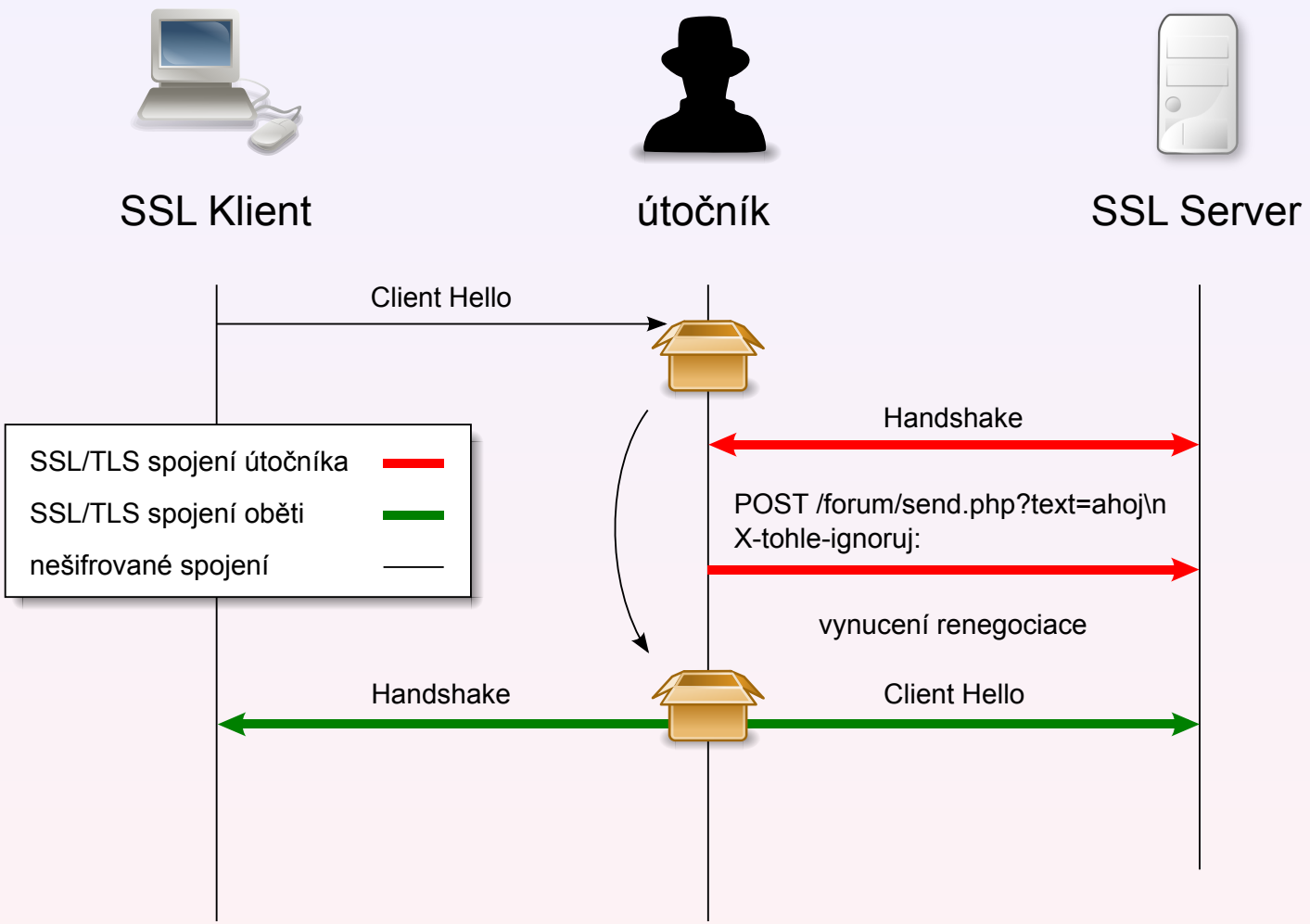
Zranitelnost renegociace SSL/TLS spojení II



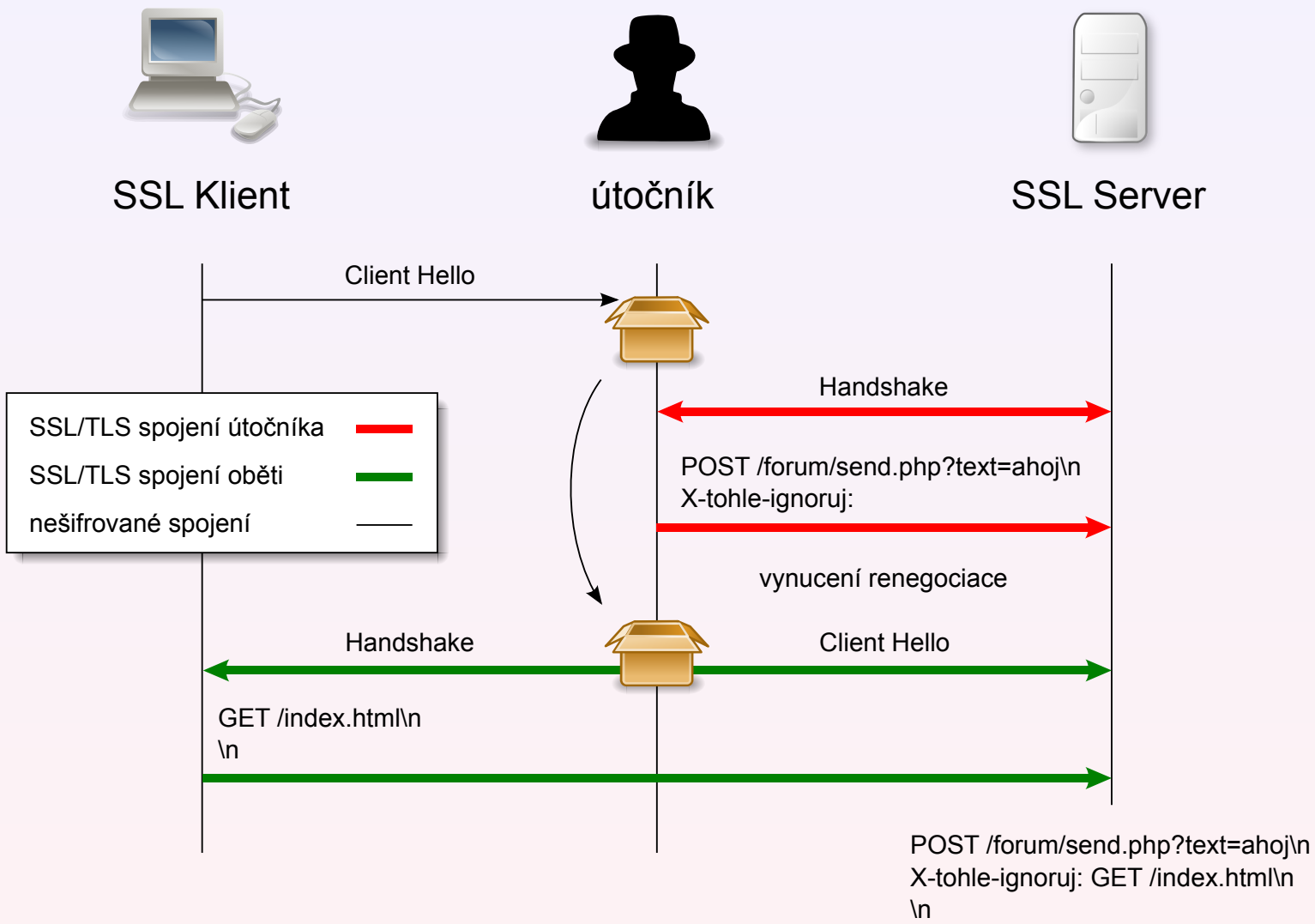
Zranitelnost renegociace SSL/TLS spojení II



Zranitelnost renegociace SSL/TLS spojení II



Zranitelnost renegociace SSL/TLS spojení II



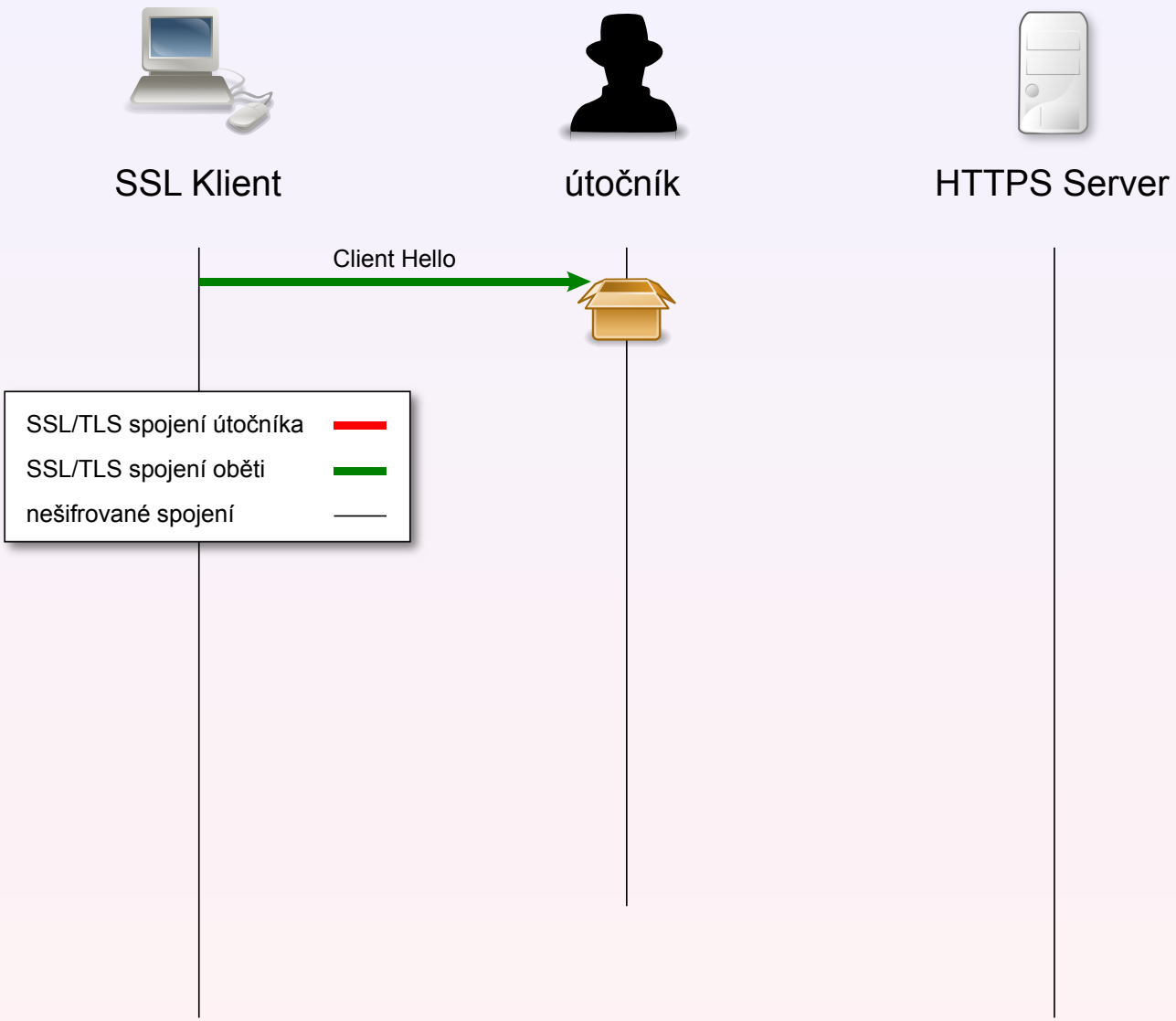
Zranitelnost renegociace SSL/TLS spojení III

SSL Klient

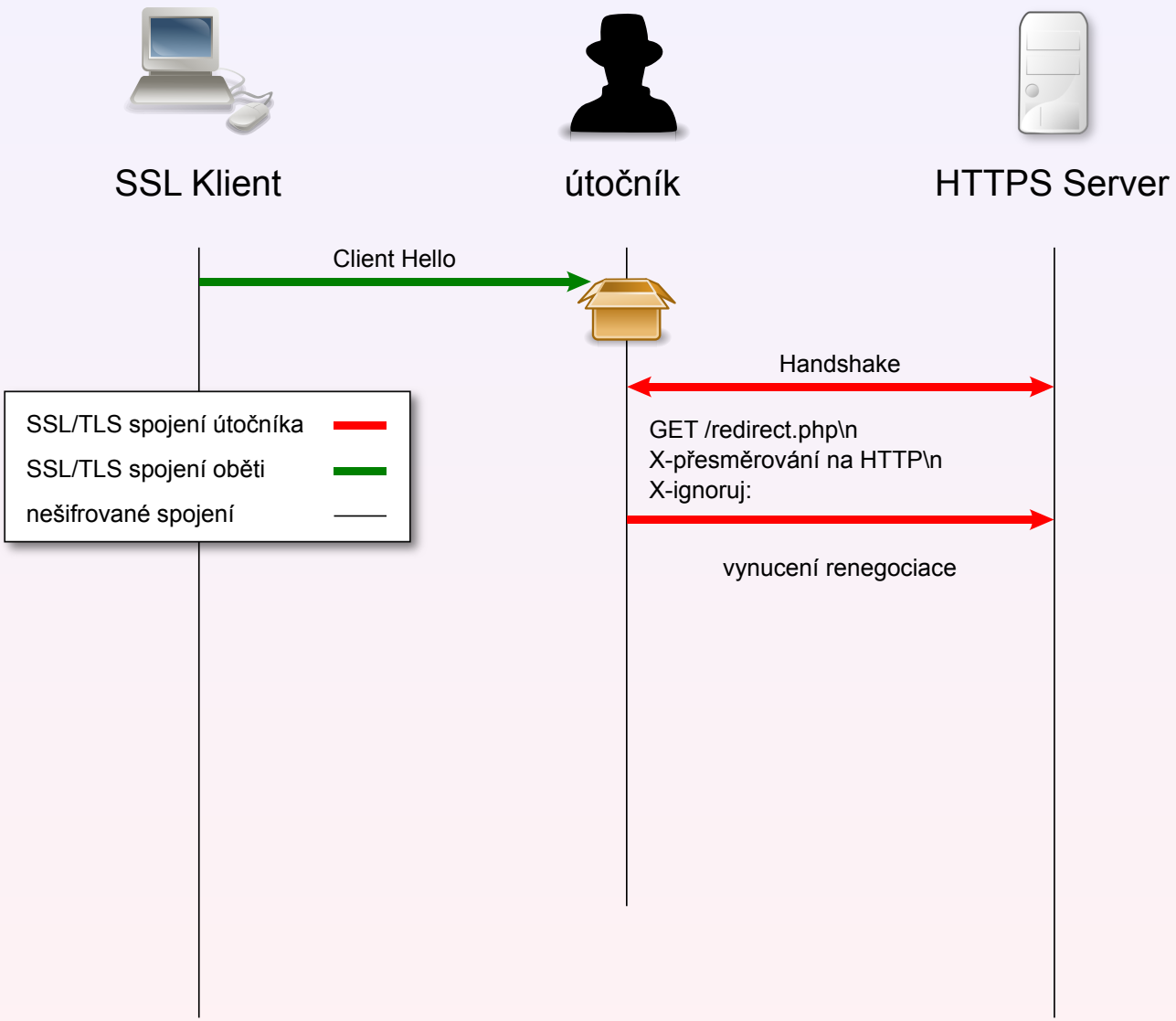
útočník

HTTPS Server

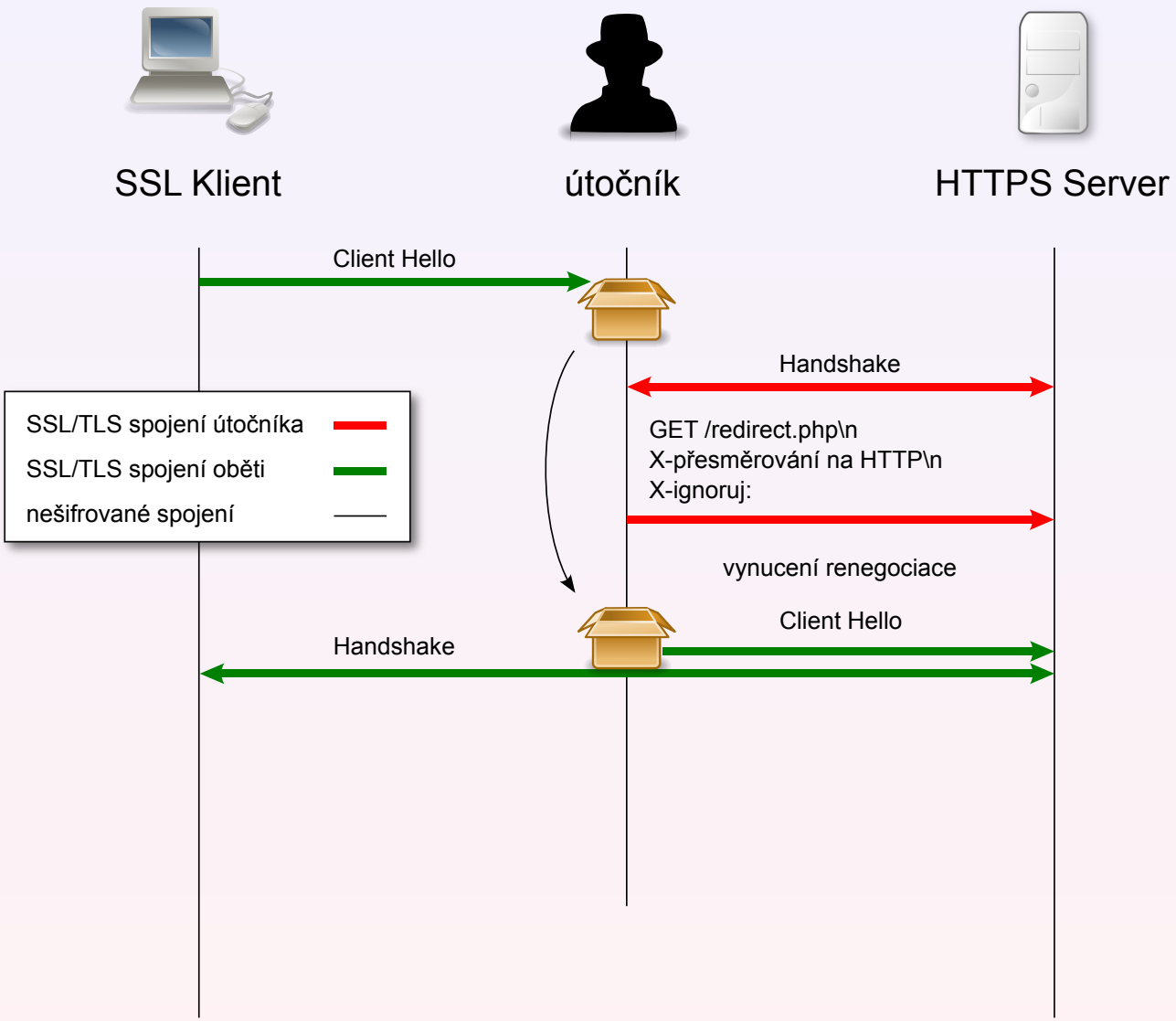
Zranitelnost renegociace SSL/TLS spojení III



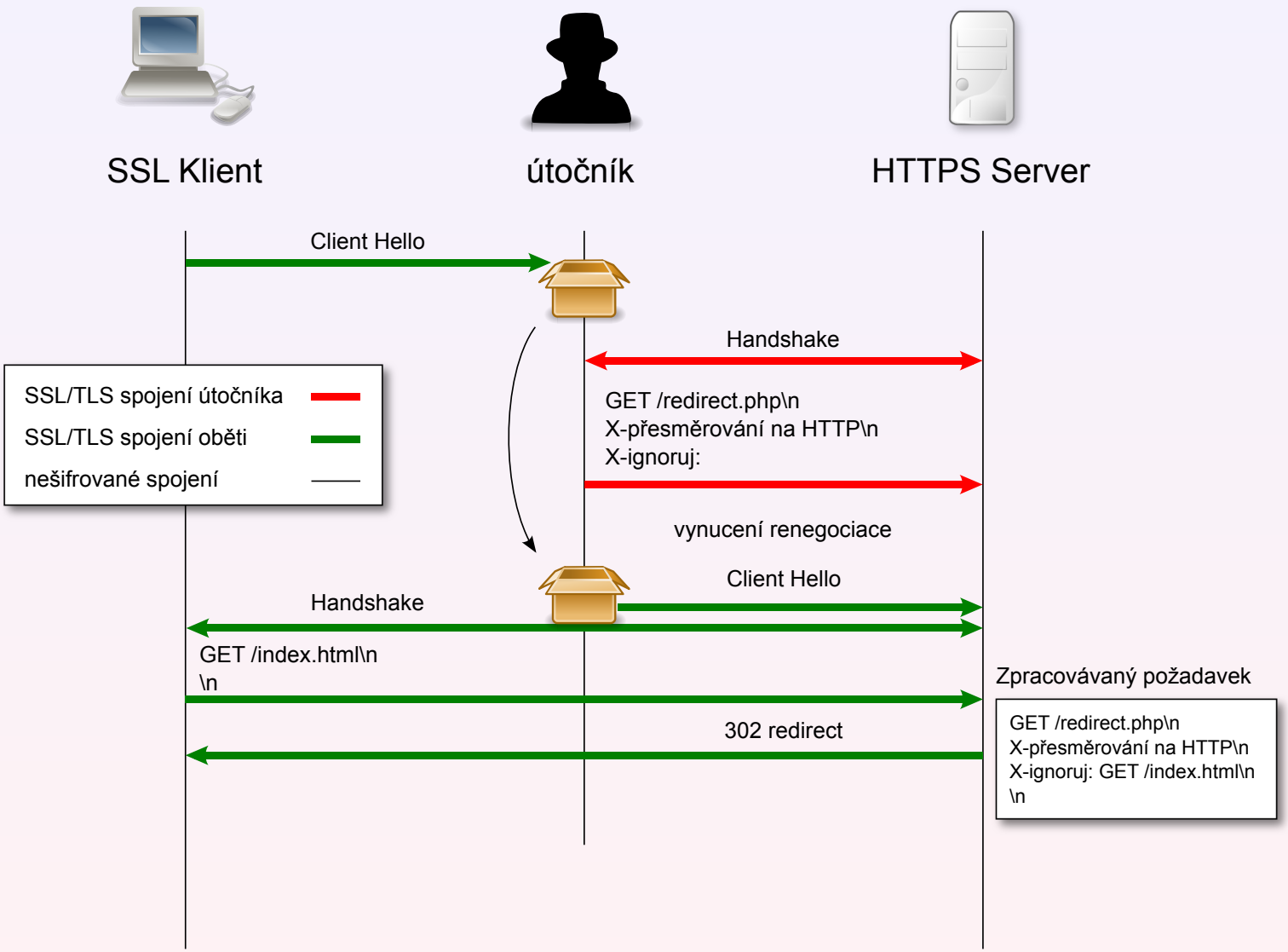
Zranitelnost renegociace SSL/TLS spojení III



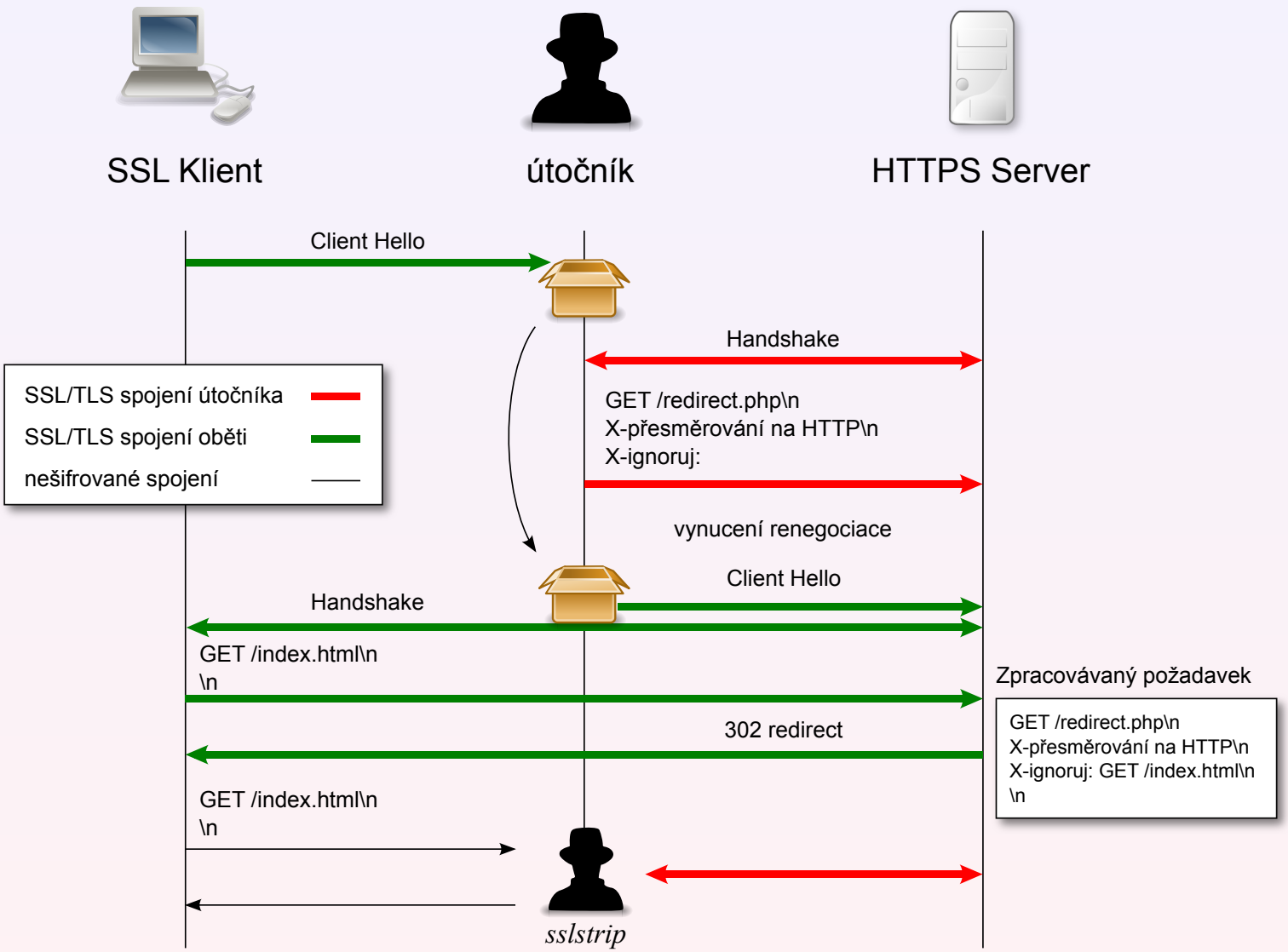
Zranitelnost renegociace SSL/TLS spojení III



Zranitelnost renegociace SSL/TLS spojení III



Zranitelnost renegociace SSL/TLS spojení III



Závěr

- Při útocích se jen vyjímečně jedná o chybu v protokolu SSL/TLS.
- Využívají se chyby v implementaci protokolu nebo zranitelnosti způsobené chybným používáním protokolu.
- Z hlediska obrany je nejdůležitější, ale zároveň nejobtížnější osvěta uživatelů.

Děkuji za pozornost.

Dotazy?