Paweł Pokrywka, Ispara.pl

Podsłuchiwanie szyfrowanych połączeń – niezauważalny atak na sesje SSL

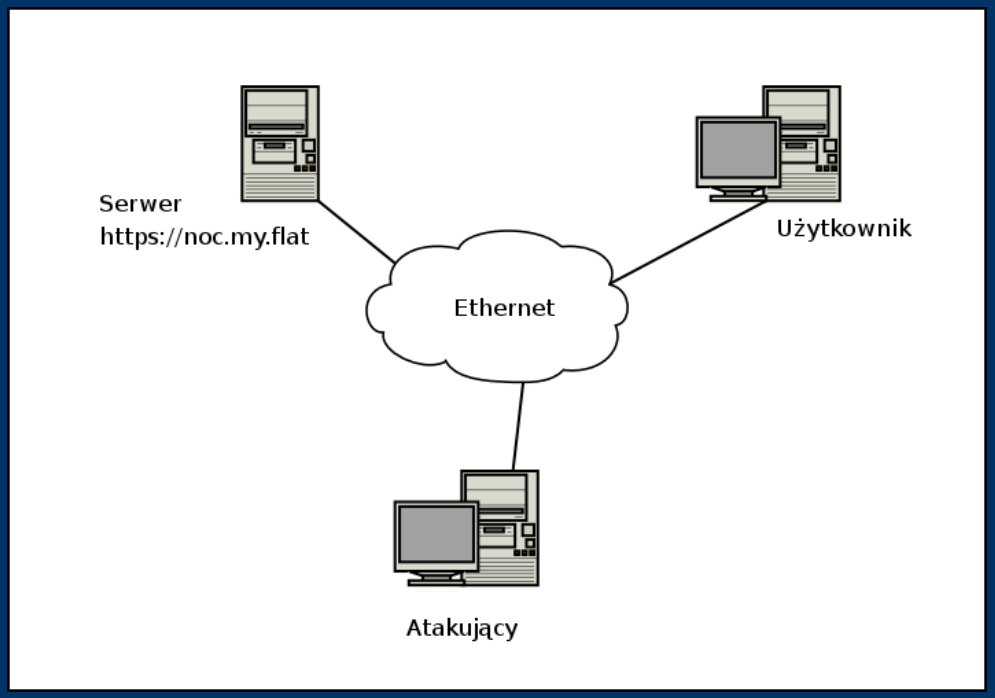
Plan prezentacji

- Co to jest SSL?
- Demonstracja ataku.
- Na czym polega atak?
- Jak się zabezpieczyć?

Co to jest SSL?

- Wikipedia: “SSL (ang. Secure Sockets Layer) - protokół, w swojej pierwotnej wersji zaprojektowany przez firmę Netscape Communications Corporation zapewniający poufność i integralność transmisji danych oraz zapewnienie uwierzytelnienia, opierający się na szyfrach asymetrycznych oraz tzw. certyfikatach standardu X.509.”

Topologia sieci



- Hosty wirtualne (qemu):
  - Serwer
  - Atakujący
- Host fizyczny
  - Użytkownik

- Wszystkie hosty znajdują się w jednej sieci
  - brctl addbr br0
  - brctl addif br0 tap0 tap1
  - 192.168.100.0/24

Instalacja serwera https

- Stworzenie certyfikatu
- Certyfikat typu Self Signed
  - nie trzeba płacić CA
  - technicznie takie samo bezpieczeństwo

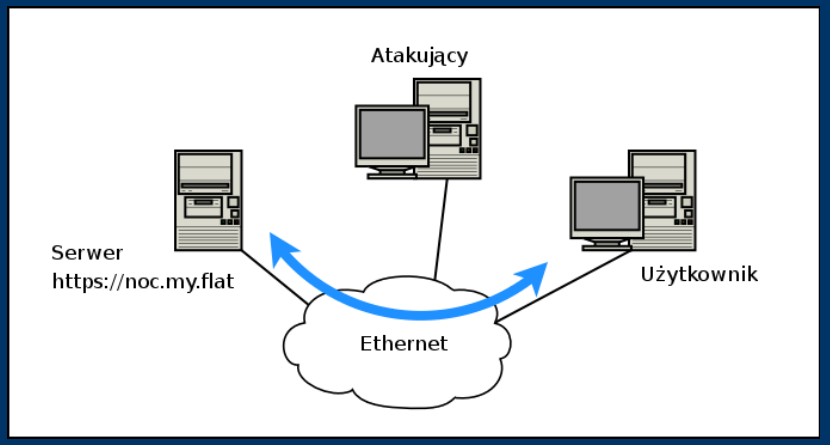
Instalacja certyfikatu w przeglądarce

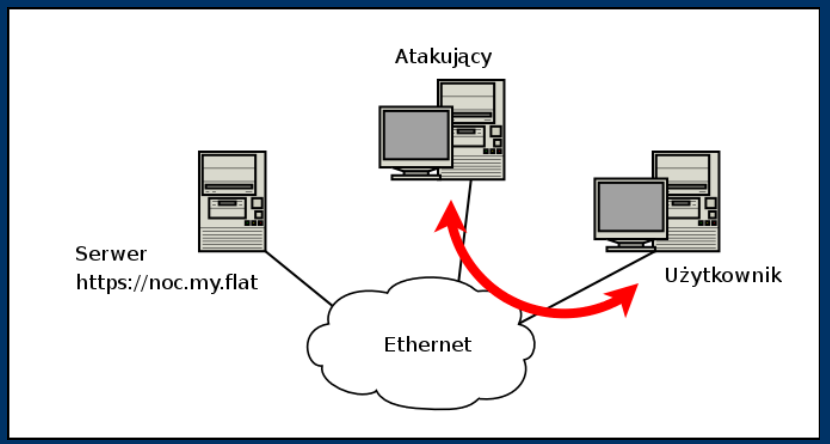
- Wygoda
  - nie trzeba za każdym razem akceptować połączenia
- Bezpieczeństwo
  - nikt nie przechwyci sesji (?)
- Jeśli pojawi się ostrzeżenie to oznacza, że ktoś próbuje przejąć sesję

Atak MitM

- Fałszywy serwer https
- Fałszywa strona logowania
- ARP Spoofing
- REDIRECT
- tail -f access_log

- Certyfikat!





Certyfikat = klucz pub. + podpis CA

- Klucz publiczny
  - wraz z kluczem prywatnym pozwalają ustalić symetryczny klucz sesji
- Podpis CA
  - klucz publiczny został zatwierdzony
- CA
  - lista zaufanych wbudowana w przeglądarki

International
Russian Language and Culture Courses

CERTIFICATE

This is to certify that Mr. Loosli Marco Harald

citizen of Switzerland

has taken Intensive course at

the Philological Faculty
of the Moscow State University
named after M. V. Lomonosov

in Low Intermediate Russian

from March 22, 2003 till April 4, 2003

40

City of Moscow 3 April, 2003

Registration number 2003-009

MOSCOW STATE UNIVERSITY named after M.V. LOMONOSOV
PHILOLOGICAL FACULTY

Ataki

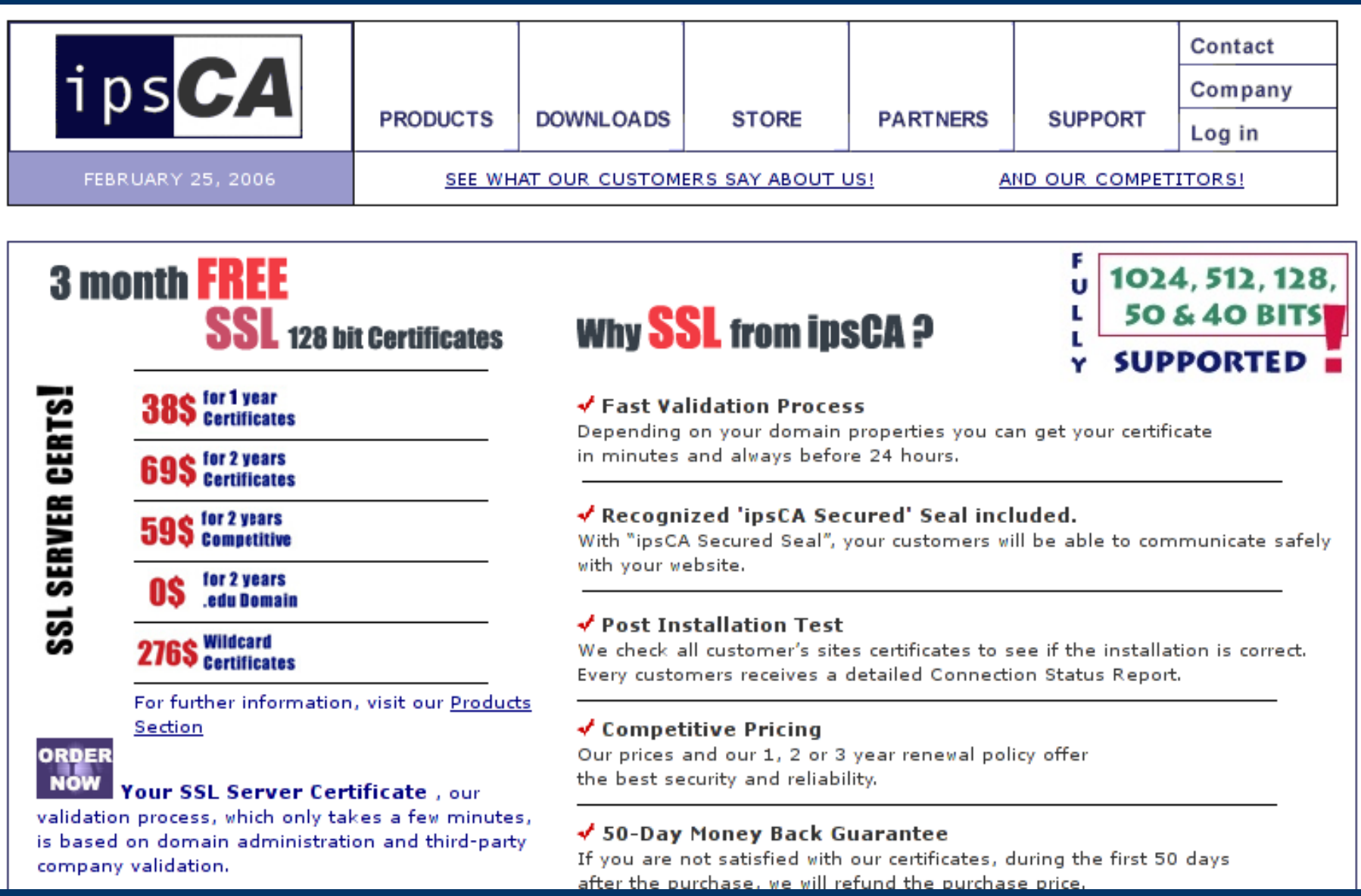
- Obniżenie jakości szyfrowania
- Wyłączenie szyfrowania
- Phishing
- Błędy implementacyjne
  - np. MSIE
- Inne?

Demonstracja

Skąd się biorą certyfikaty?

- Weryfikacja
  - dowód tożsamości
  - dokumenty firmy
  - ...
  - prawa do domeny (whois)
- Tanie/darmowe certyfikaty
  - tylko prawa do domeny (whois)
- Jak odróżnić tani/darmowy certyfikat?
- **Jak zweryfikować prawo do domeny wewnętrznej?**

IPSCA


ipsCA
PRODUCTS
DOWNLOADS
STORE
PARTNERS
SUPPORT
Contact
Company
Log in
FEBRUARY 25, 2006
SEE WHAT OUR CUSTOMERS SAY ABOUT US!
AND OUR COMPETITORS!
3 month FREE
SSL 128 bit Certificates
SSL SERVER CERTS!
38$ for 1 year Certificates
69$ for 2 years Certificates
59$ for 2 years Competitive
0$ for 2 years .edu Domain
276$ Wildcard Certificates
For further information, visit our Products Section
ORDER NOW
Your SSL Server Certificate , our validation process, which only takes a few minutes, is based on domain administration and third-party company validation.
Why SSL from ipsCA ?
FULLY
1024, 512, 128, 50 & 40 BITS
SUPPORTED
Fast Validation Process
Depending on your domain properties you can get your certificate in minutes and always before 24 hours.
Recognized 'ipsCA Secured' Seal included.
With "ipsCA Secured Seal", your customers will be able to communicate safely with your website.
Post Installation Test
We check all customer's sites certificates to see if the installation is correct. Every customers receives a detailed Connection Status Report.
Competitive Pricing
Our prices and our 1, 2 or 3 year renewal policy offer the best security and reliability.
50-Day Money Back Guarantee
If you are not satisfied with our certificates, during the first 50 days after the purchase, we will refund the purchase price.

IPSCA

- “Please make sure that the COMMON NAME (CN) in your CSR is the Fully-Qualified Domain Name (example: www.ips.es) of your OWN Server, .If it is an intranet server, use the network name of your server.”
- Niezweryfikowane certyfikaty nie są nic warte
- Cały system SSL jest tak silny jak najsłabsze ogniwo
- Certyfikat noc.my.flat

Zabezpieczenia

- Wewnętrzne domeny
  - lepiej: wewnetrzna.zewnetrzna.pl
  - uwaga na HOWTO
- Zmiana certyfikatu podczas sesji – ostrzeżenie
  - instalacja nowego certyfikatu
- Usunięcie IPSCA z listy CA w przeglądarce

- Zagrożenie: niskie

Dziękuję za uwagę.

Paweł Pokrywka,
Ispara.pl