Zašto vjerovati kriptografskim protokolima?

Ante Đerek

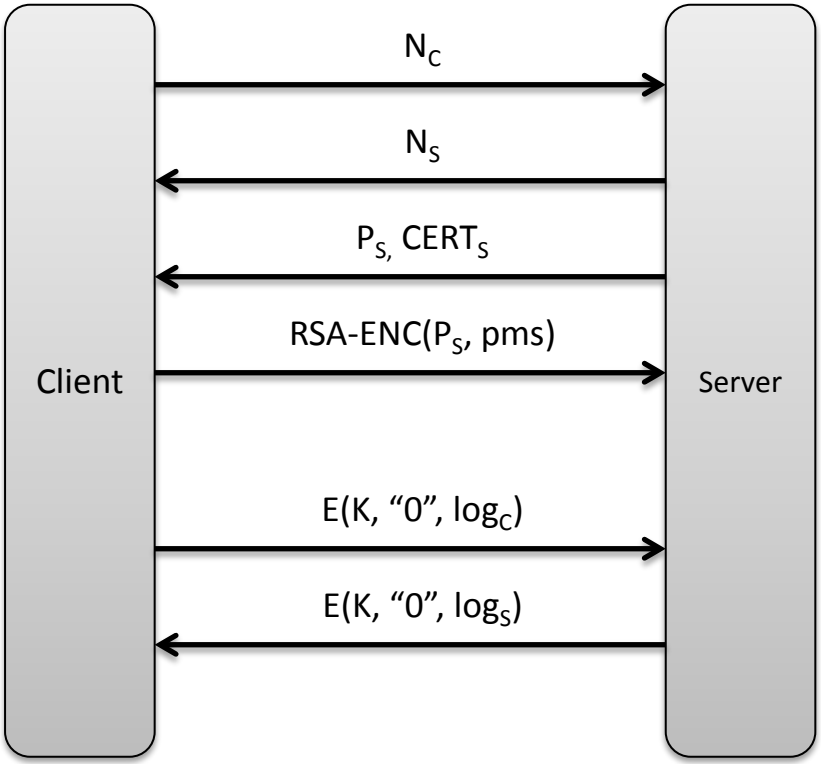
Sveučilište u Zagrebu

Fakultet elektrotehnike i računarstva

NEWFELPRO 2013 2017

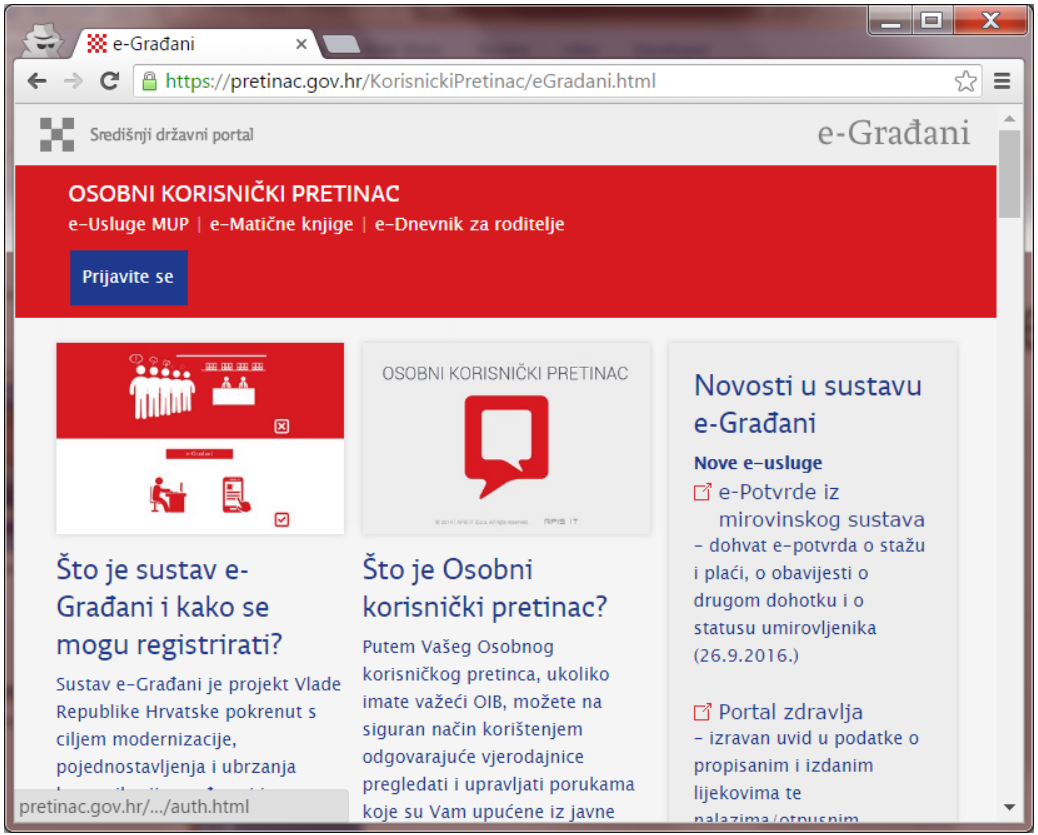

FOX NEWS
CLINTON: CYBER WARFARE WILL BE ONE OF THE BIGGEST CHALLENGES FACING THE NEXT PRESIDENT
1ST PRESIDENTIAL DEBATE
FOX NEWS Channel

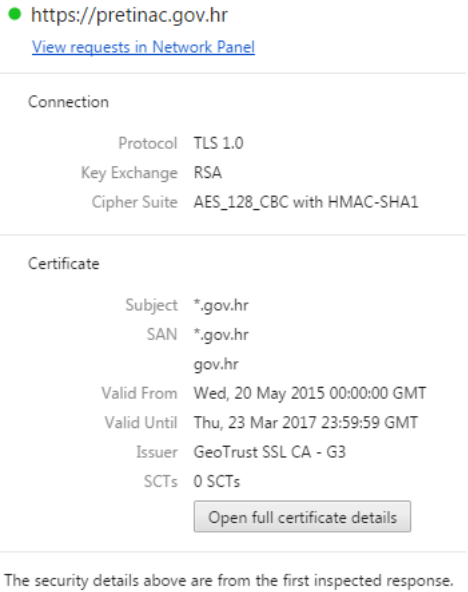
Kriptografski protokol



- Distribuirani program
- Komunikacija putem nesigurnih kanala
- Koristi kriptografiju
- Obavlja kritičnu sigurnosnu funkciju

Transport Layer Security (TLS)





Elektronsko glasovanje

Mislim da je potpuno nevažno tko u Partiji glasa ili kako, već je važno tko će brojati glasove i kako.

Josif Staljin

Medicinski senzori/uređaji

For patients, with discreet mobile display of pump and CGM data

Još puno primjera...

- Wi-Fi, IPSec, Kerberos, Signal, itd.
- Telefonija
- Kreditne kartice
- Ugradbeni sustavi
- Internet of things
- TOR
- ...

Sigurnost kriptografskih protokola

Traženje napada

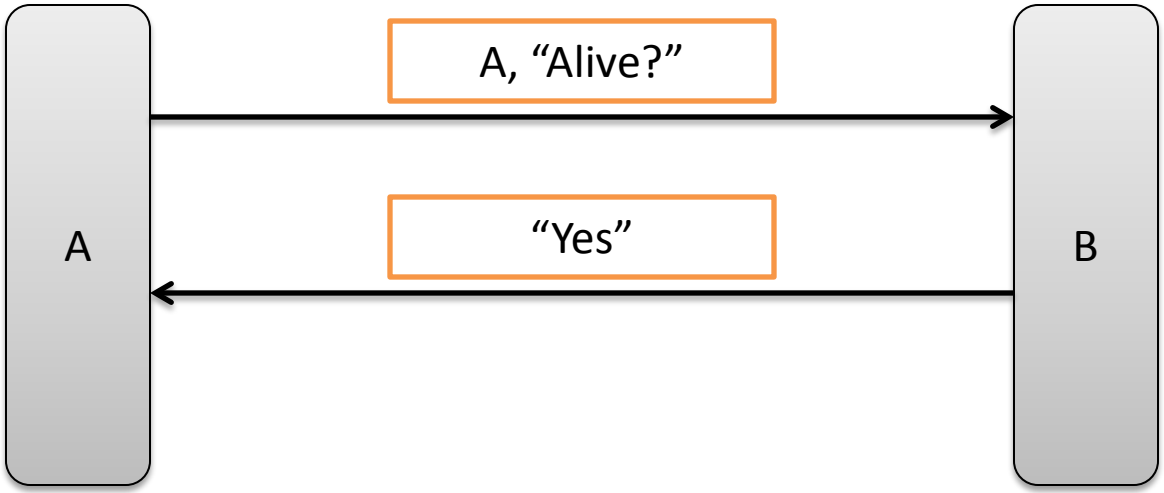
- Napadi na implementaciju
- Napadi na kriptografiju
- Napadi na protokol
- Hibridni napadi
- ...

Verifikacija svojstava

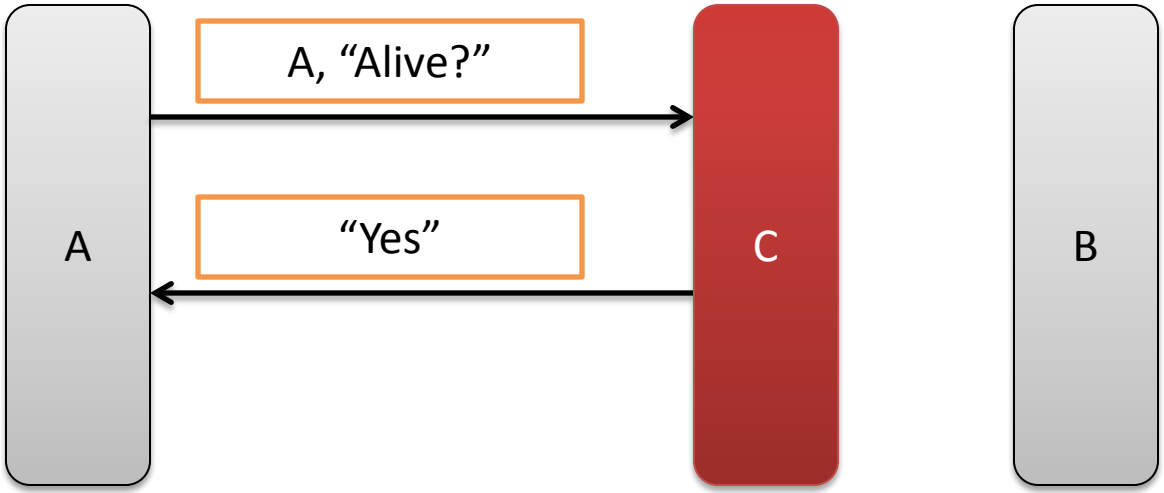
- Za sve moguće konfiguracije protokola
- Za sve moguće napadače
- U svim mogučim slučajevima
- Moraju biti zadovoljena sva željena svojstva

Neuspješno traženje napada != Verifikacija

Je li Bob živ? – Protokol 1



Je li Bob živ? – Napad 1

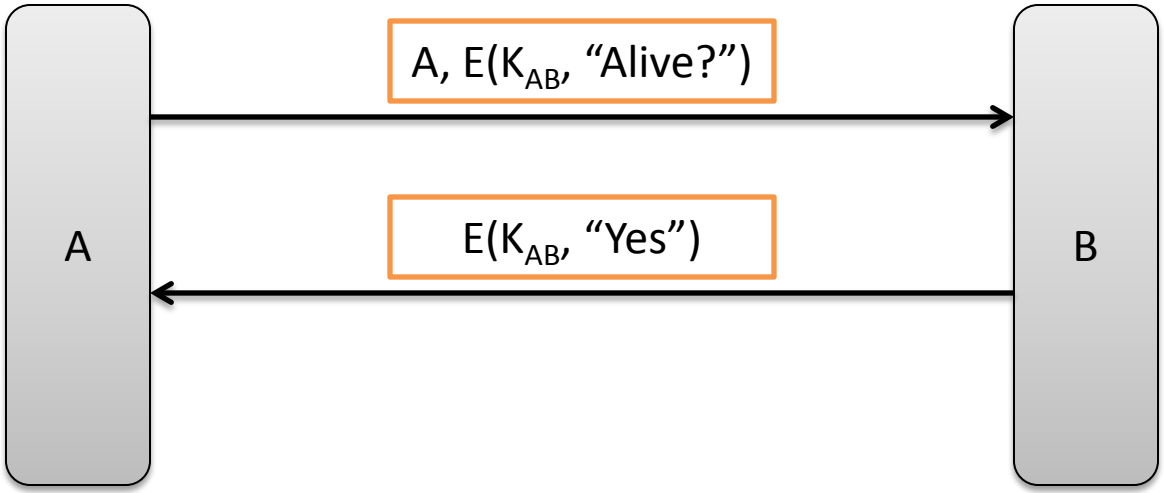


Kriptografija: Simetrična autentificirana enkripcija

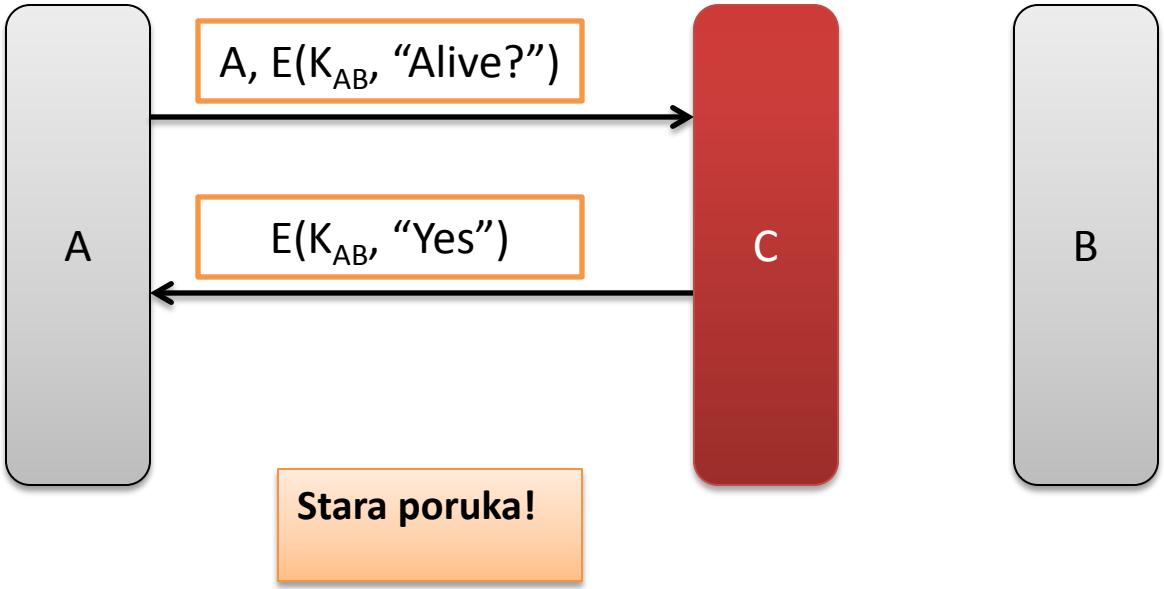
$E(K_{AB}, m)$

- Svojstva (neformalno):
  - *Povjerljivost :* Poruku kriptiranu s ključem K_{AB} može dekriptirati samo onaj tko ima ključ K_{AB}
  - *Autentifikacija:* Poruku kriptiranu s ključem K_{AB} mogao je kriptirati samo onaj tko ima ključ K_{AB}
  - *Integritet*: Ako se poruka uspješno dekriptira onda nije izmijenjena

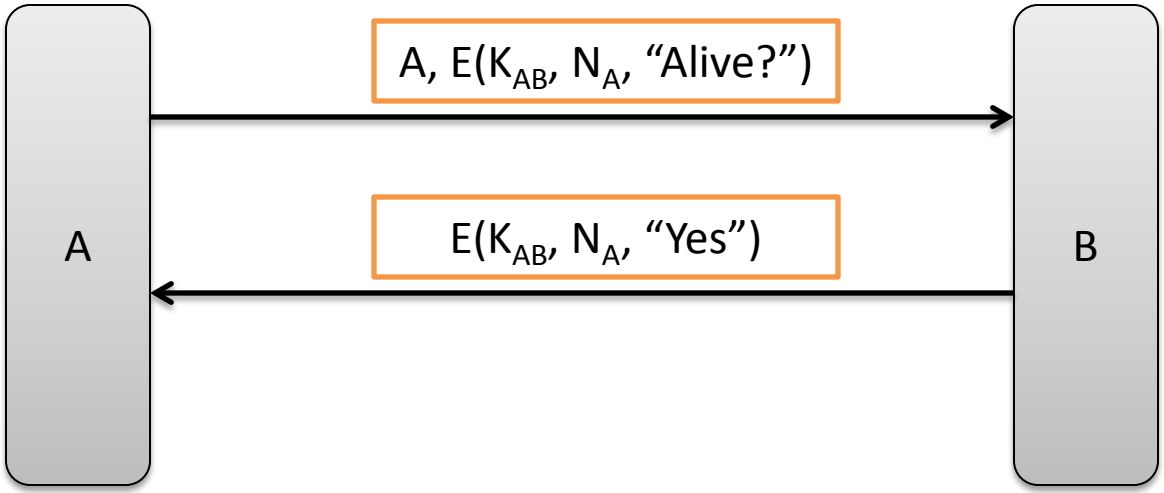
Je li Bob živ? – Protokol 2



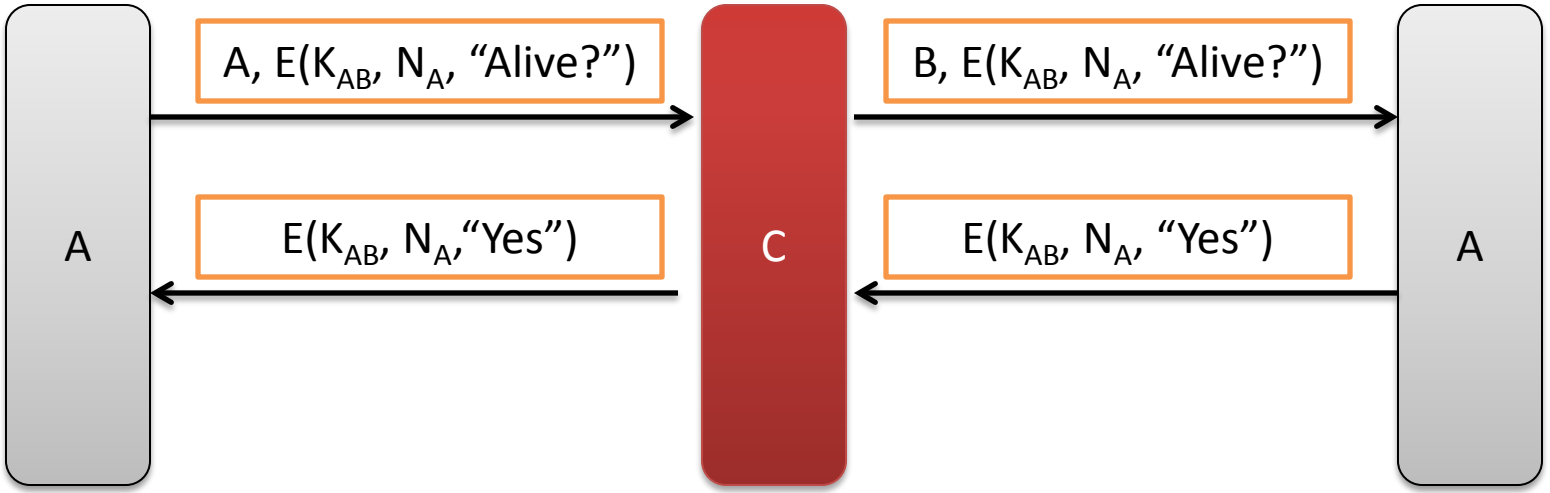
Je li Bob živ? – Napad 2 (*Replay*)



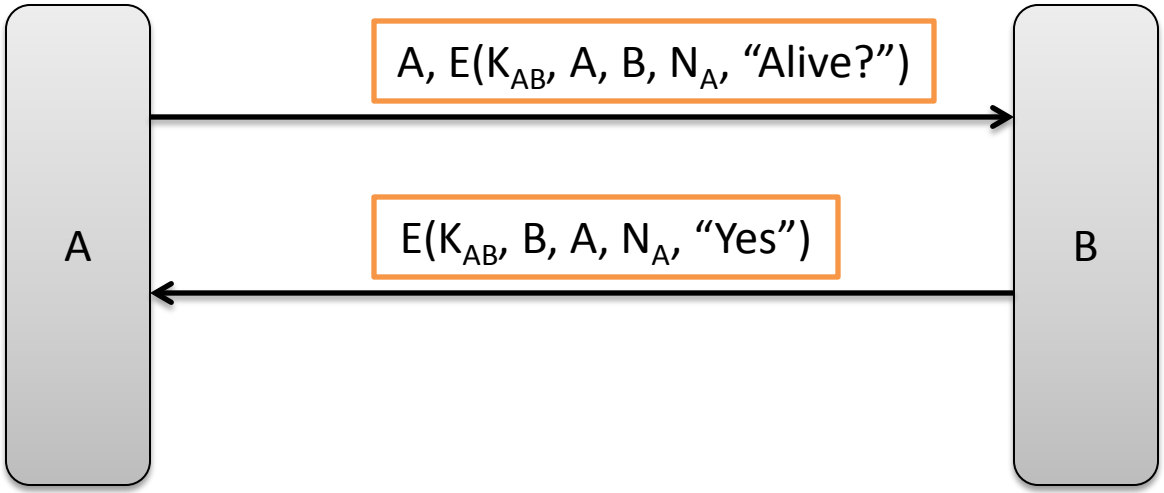
Je li Bob živ? – Protokol 3



Je li Bob živ? – Napad 3 (*Reflection*)



Je li Bob živ? – Protokol 4



Autentificirana razmjena ključeva

- *Cilj*: A i B žele razmijeniti tajni ključ te se (jednostrano ili obostrano) autentificirati
  - Ako A završi protokol, čini se sa B, onda
    - B je završio protokol, čini se sa A
    - A i B su izračunali isti ključ K
    - Ključ K je tajan
    - Pod pretpostavkom da je B pošten
- *Pretpostavka*: Postoji infrastruktura javnih ključeva (PKI)

Kriptografija: Asimetrična enkripcija

$E(P_A, m)$

- Svojstva (neformalno):
  - *Povjerljivost:* Poruku kriptiranu sa *javnim* ključem P_A može dekriptirati samo onaj tko ima odgovarajući *privatni* ključ S_A

Kriptografija: Digitalni potpis i certifikat

$Sig(S_A, m)$

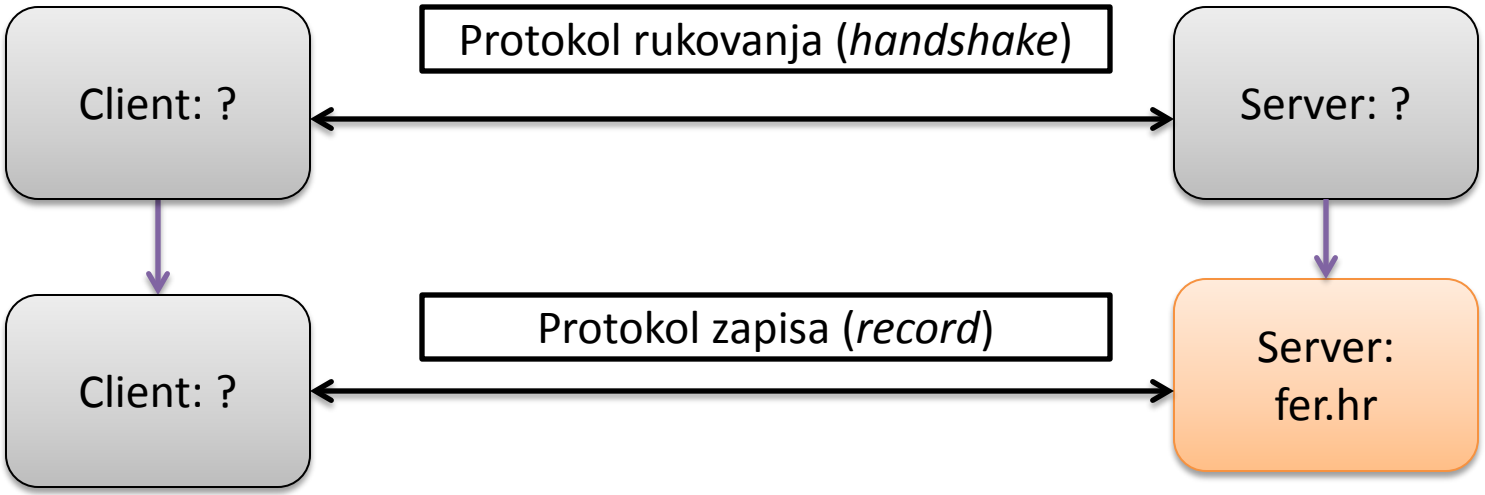
$CERT_A = Sig(S_{Auth}, P_A)$

- Svojstva (neformalno):
  - *Integritet:* Ako verifikacija potpisa uspije onda poruka nije promijenjena
  - *Autentifikacija:* Potpis koji se verificira javnim ključem P_A može generirati samo onaj tko ima odgovarajući *privatni* ključ S_A
- Certifikat:
  - Digitalni potpis javnog ključa od strane autoriteta kojemu se vjeruje
  - Povezuje javni ključ sa identitetom (“Fakultet elektrotehnike i računarstva”, www.fer.hr)

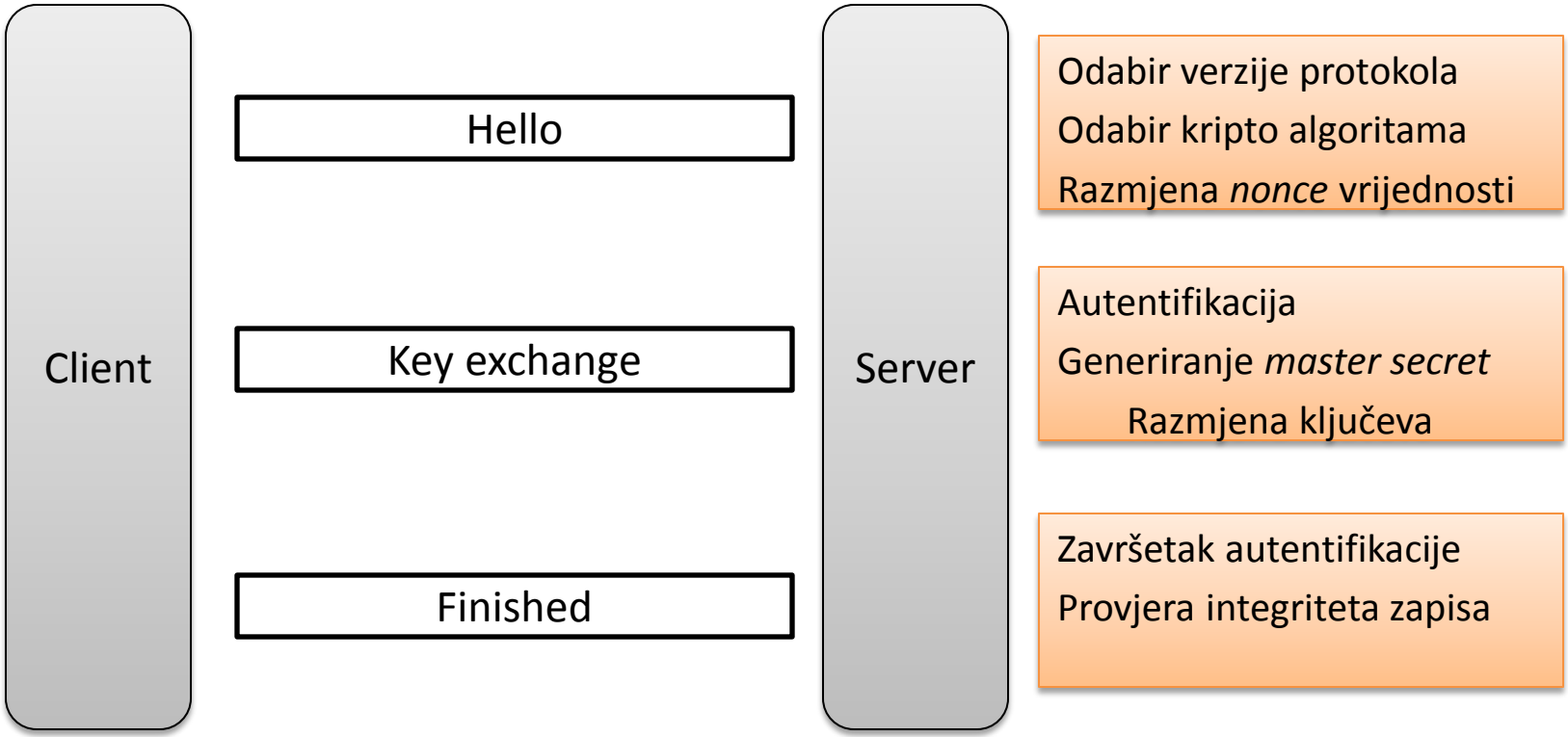
Transport Layer Security

- *Cilj*: Uspostava sigurnog komunikacijskog kanala
- *Primjene:* HTTPS, e-Mail, VPN, VoIP, ...
- *Implementacije:* OpenSSL, GnuTLS, JSSE, SChannel, ...
- 20 godina proširenja, napada, popravaka i dokaza sigurnosti
  - Napad na implementaciju: HeardBleed (2014)
  - Napad na kriptografiju: PKCS #1 padding (Bleichenbacher 1998)
  - Napad na protokol: 3Shake (2014)

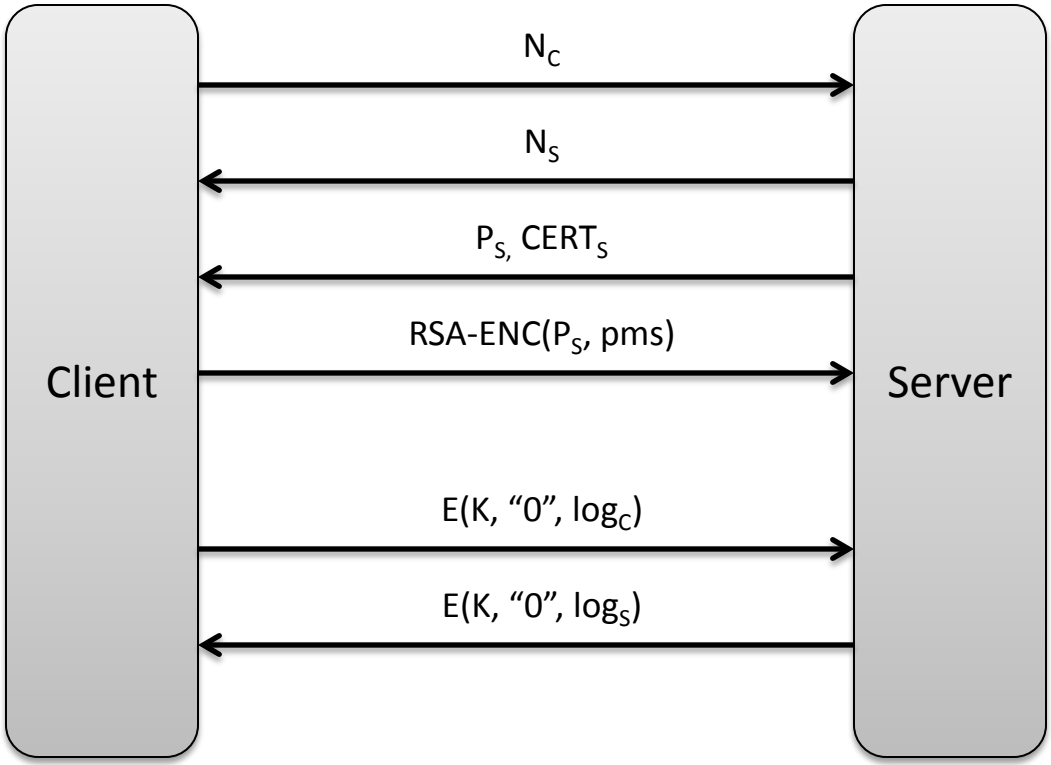
Faze TLS protokola



TLS rukovanje



TLS rukovanje – pojednostavljena RSA verzija



Razmjena *nonce* vrijednosti

Klijent bira *pre-master secret*

master secret i svi ključevi generirani od pms, N_C, N_S

Autentificirana enkripcija

log vrijednosti dobivene hashiranjem cijelokupnog transkripta uključujući ms

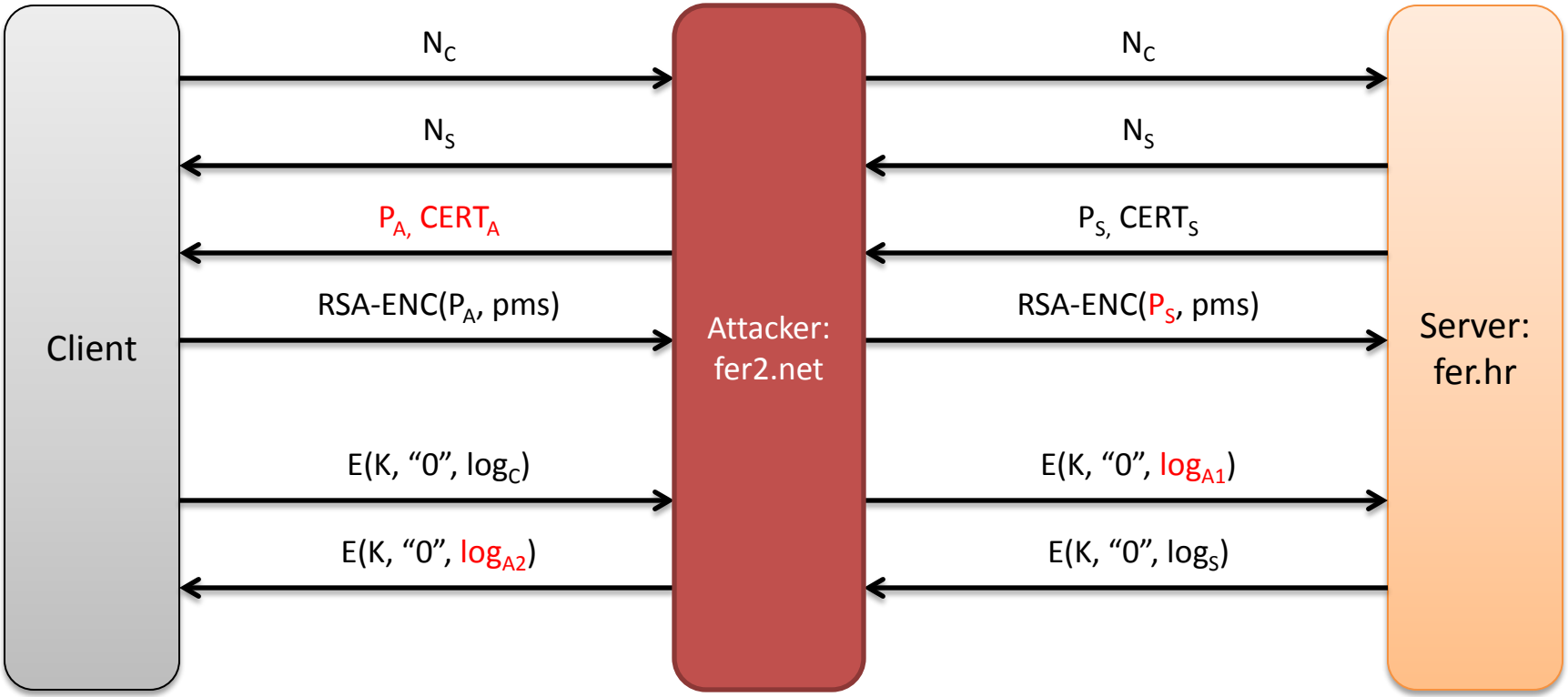
Puno varijanti i mogućnosti

- Verzije protokola: SSL 2, SSL 3, TLS 1.0, TLS 1.1, ...
- Kriptografski algoritmi: RC5, 3DES, AES, ...
- Razmjena ključeva: RSA, DH, ECDH, PSK, ...
- Optimizacije i dodatne mogućnosti
  - Autentifikacija klijenta
  - Ponovno rukovanje
  - Nastavak sjednice
  - ...
- Proširenja
- Mehanizmi neuspjeha

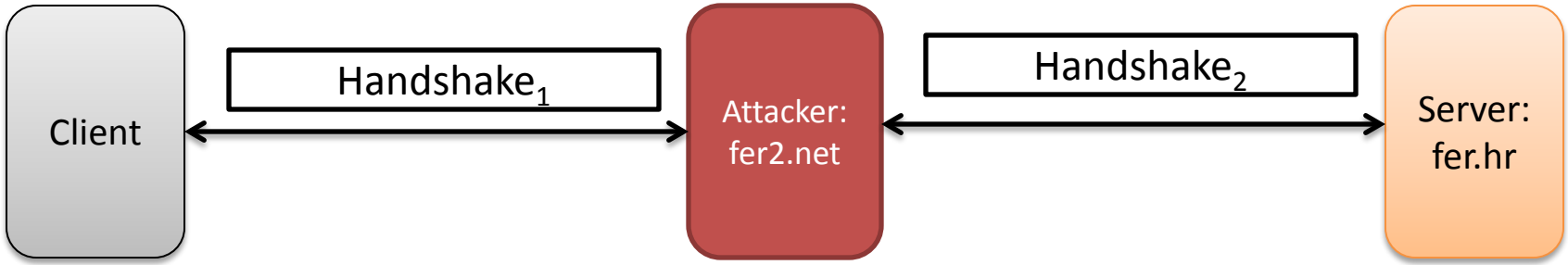
Primjer napada – 3Shake

- Napad proizlazi iz nepoželjene interakcije različitih modula u protokolu
- Ovdje smo pojednostavili priču
  - Bhargavan et al., *Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over, TLS* 2014

Prvi “napad” (*unknown key-share attack*)

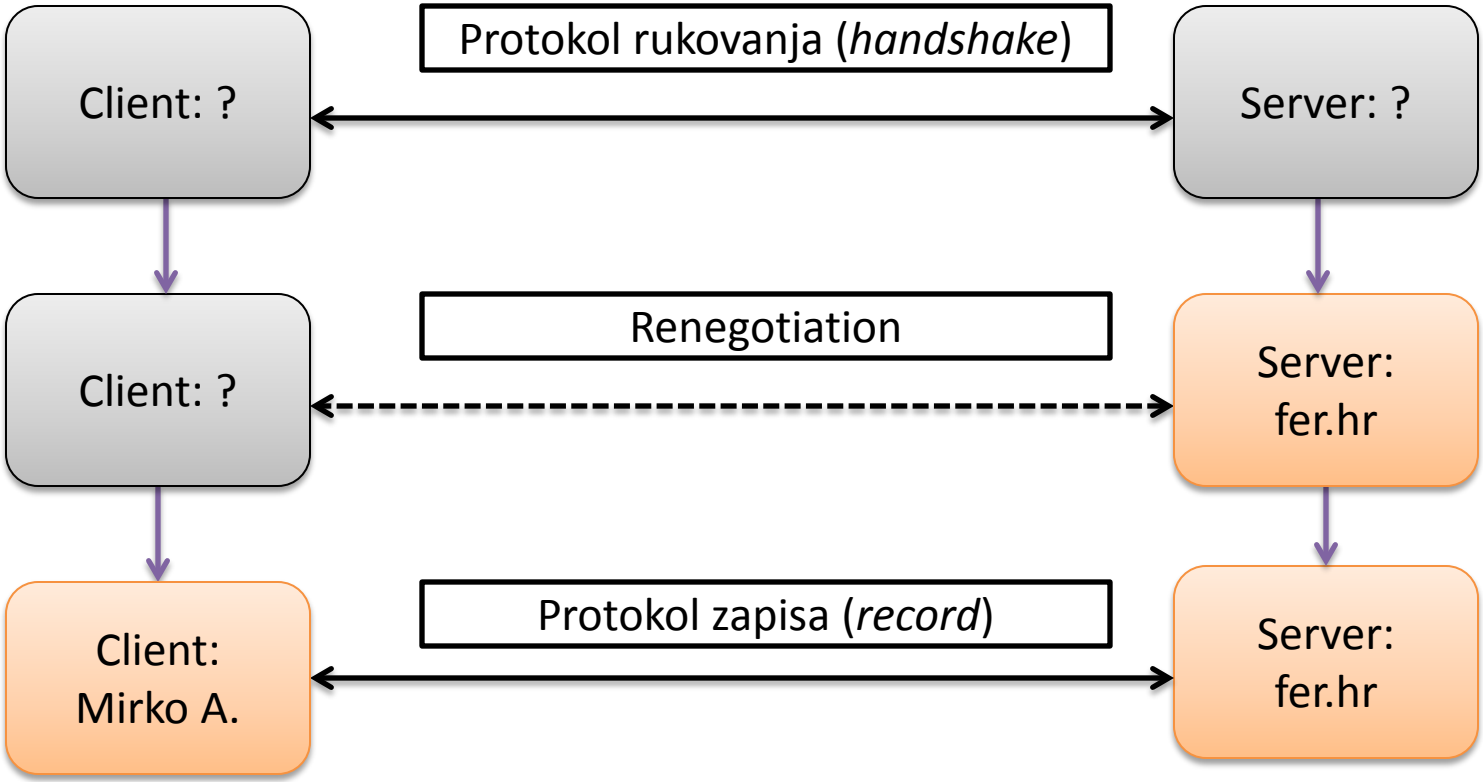


Ništa strašno?

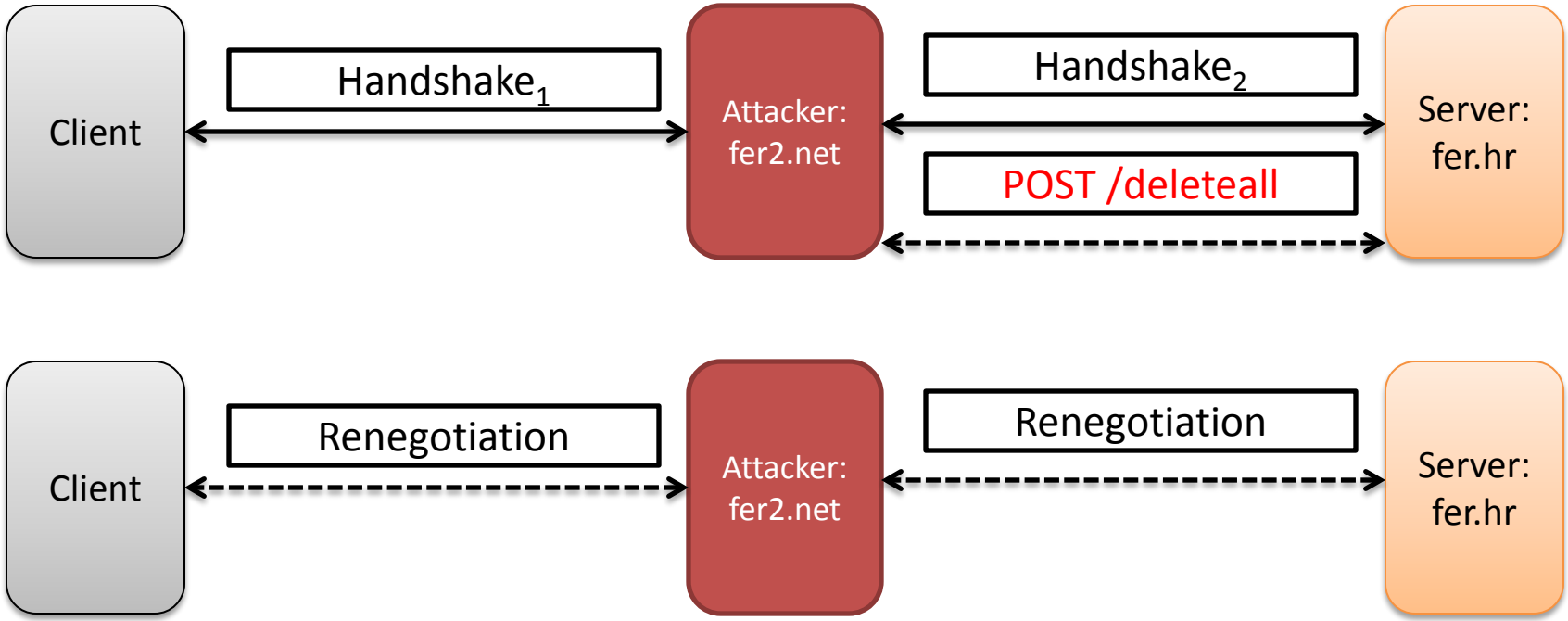


- Klijent uspostavi sigurni kanal sa napadačem na fer2.net
- Napadač uspostavi sigurni kanal sa fer.hr
- *Pre-master secret* pa tako i svi ostali ključevi su **jednaki**!

Ponovno rukovanje (*renegotiation*)



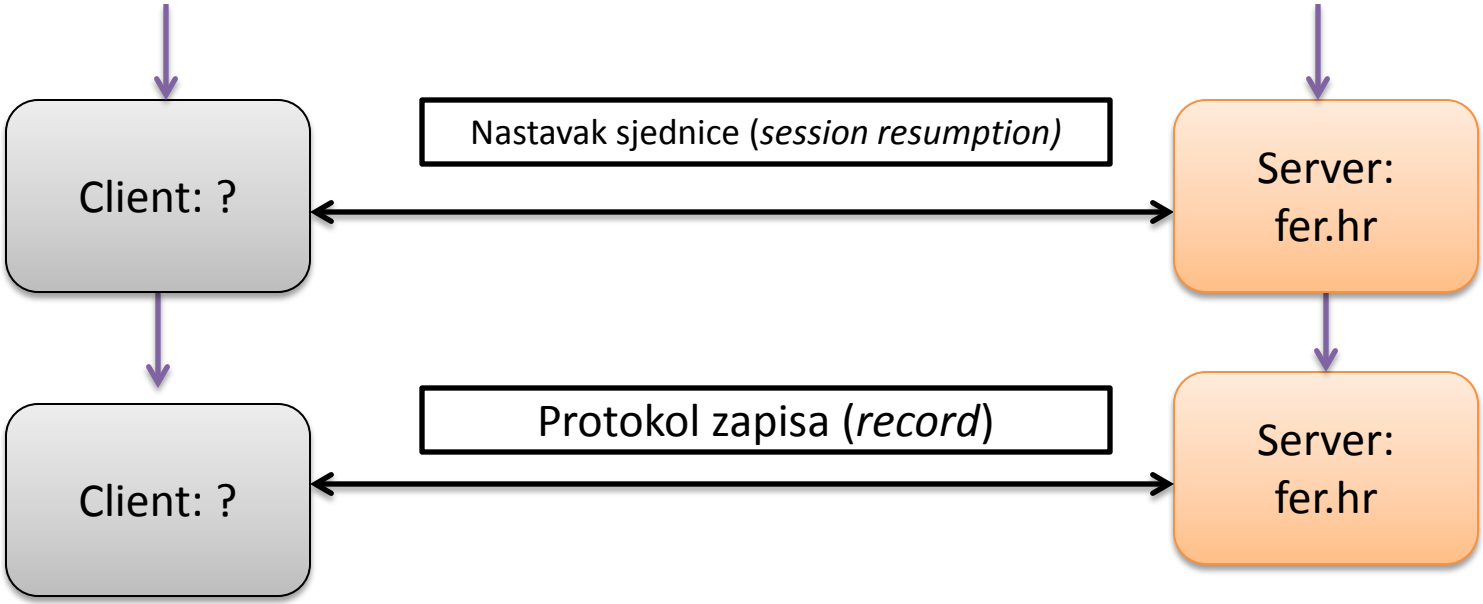
TLS renegotiation napad [Ray, Dispensa 2009]



Popravak

- Zadnja poruka rukovanja mora biti uključena u protokol za ponovno rukovanje
  - ClientFinished = E(K, “0”, $\log_C$)

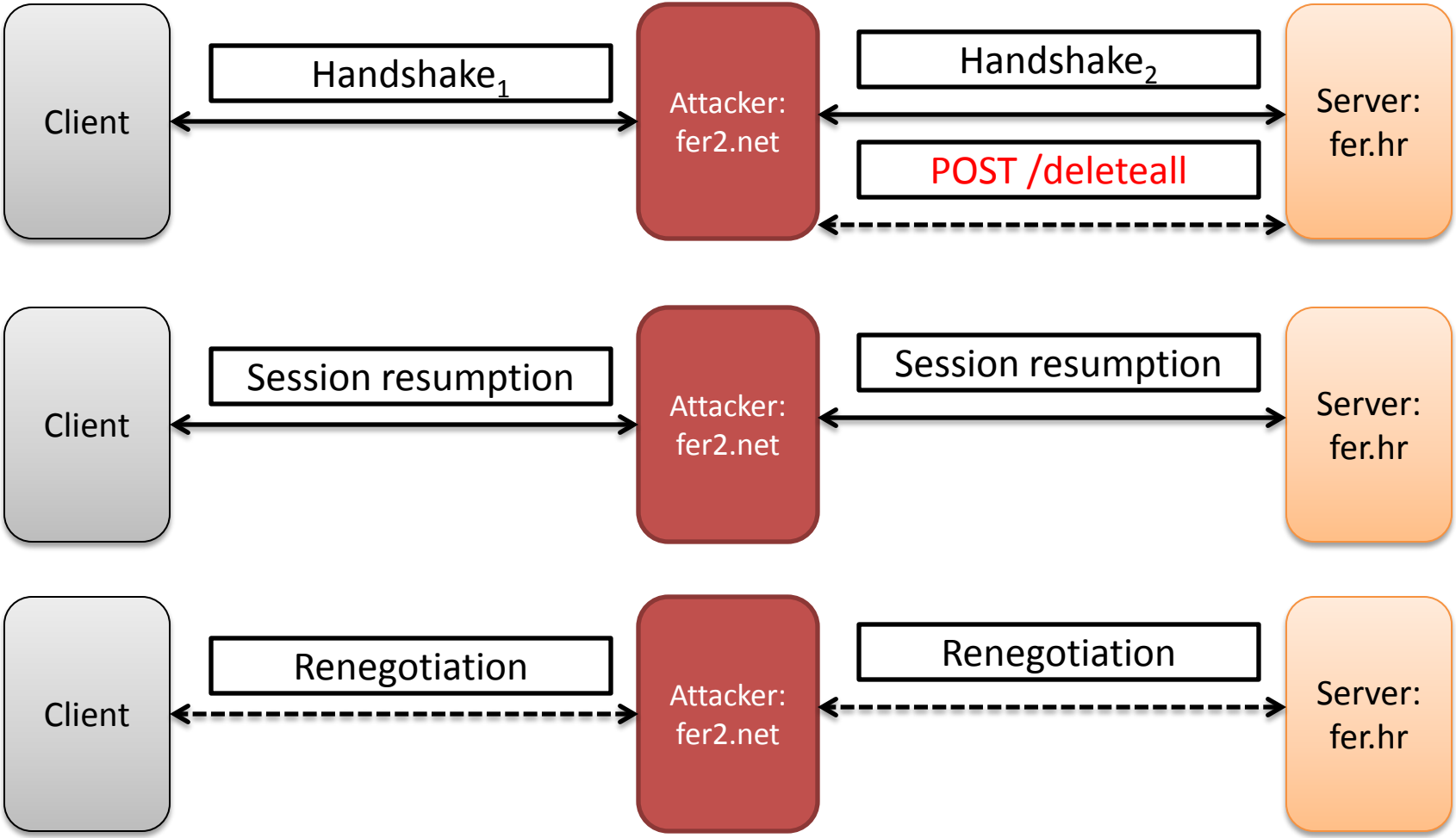
Nastavak sjednice (*session resumption*)



Radi efikasnosti ne koristi kriptografiju javnog ključa

Razmjena novih *nonce* vrijednosti, pozivanje na stari pms

ClientFinished poruka sada ne ovisi o certifikatima


Client
Handshake1
Attacker:
fer2.net
Handshake2
Server:
fer.hr
POST /deleteall
Client
Session resumption
Attacker:
fer2.net
Session resumption
Server:
fer.hr
Client
Renegotiation
Attacker:
fer2.net
Renegotiation
Server:
fer.hr

Napad u stvarnom svijetu?

- *Proof of concept: https://mitls.org/pages/attacks/3SHAKE*
- Potrebno je da oba servera
  - Podržavaju ponovno rukovanje
  - Koriste iste klijentske certifikate
- Napad postoji već dugo godina, otkriven formalnom analizom

Verifikacija kriptografskih protokola

Formalne metode: *matematički modeli kompleksnih sistema*

$$Auth_{Resp} : true[\mathbf{Resp}(\mathrm{B})]_{\mathrm{T}} \left(\Rightarrow \left(\begin{array}{c} \mathrm{Honest}(\mathtt{idA}^{[\mathrm{T}]}) \wedge \mathtt{idA}^{[\mathrm{T}]} \neq \mathrm{B} \\ \exists \mathrm{T}' : \ \mathrm{T}'.pname = \mathtt{idA}^{[\mathrm{T}]} \\ \wedge \mathrm{Send}(\mathrm{T}', \mathtt{enca}^{[\mathrm{T}]}) \lhd \mathrm{Receive}(\mathrm{T}, \mathtt{enca}^{[\mathrm{T}]}) \\ \wedge \mathrm{Receive}(\mathrm{T}, \mathtt{enca}^{[\mathrm{T}]}) \lhd \mathrm{Send}(\mathrm{T}, \mathtt{encb}^{[\mathrm{T}]}) \end{array} \right) \right)$$

Formalni dokazi: *Garancije koje se mogu algoritamski provjeriti*

Modeliranje sigurnosnih protokola

- Potrebno je modelirati:
  - Izvođenje protokola
  - Kriptografiju
  - Napadača
  - Sigurnosna svojstva

Dvije škole modeliranja protokola

	Simbolički model [NS78,DY84,…]	Model teorije složenosti [GM84, ...]
Izvršavanje protokola	*Simboličko*: Poruke koje se razmjenjuju u protokolu su termovi	*Konkretno*: Poruke su nizovi bitova
Kriptografija	*Savršena*: Enkripcija od “m” je “E(k, m)”	*Stvarna:* Kriptografske pretpostavke sigurnosti poput IND-CPA
Napadač	*Fiksni skup akcija*: Slanje poznate poruke, primanje poruke, dekripcija sa poznatim ključem ...	*Samo ograničenje na efikasnost*: Bilo koji vjerojatnosni polinomijalni Turingov stroj
Sigurnosna svojstva	*Idealizirana:* Poruka je tajna ako napadač ne posjeduje term koji odgovara poruci	*Precizna*: Poruka je tajna ako napadač nema nikakvo parcijalno znanje o bitovima poruke

Prednosti i mane

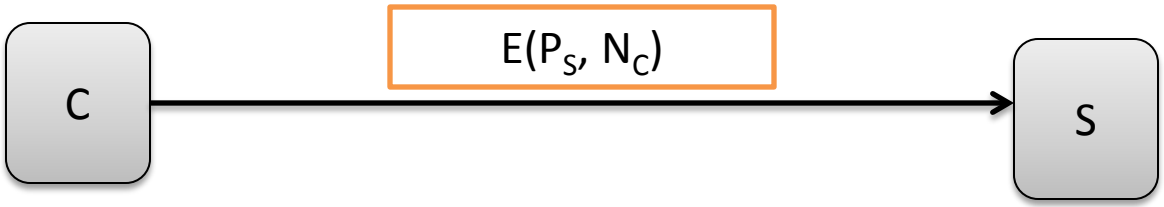
- Simbolični model:
  - idealizirani protokol, ne nalazi sve napade
  - lakša analiza, mnoštvo alata
- Model teorije složenosti:
  - protokol koji je bliže stvarnome
  - zahtjevna analiza

Primjeri formalnih modela podržanih alatima

- Tamarin http://www.infsec.ethz.ch/research/software/tamarin.html
  - Alat za automatsku analizu protokola u simboličkom modelu
  - Razvijen na ETH Zurich (Simon Meier, Benedikt Schmidt, et al.)
  - Trenutnu se koristi za formalnu analizu prilikom razvoja TLS 1.3 standarda (Cas Cremers et al., University of Oxford)
- miTLS http://www.mitls.org/
  - Projekt koji implementira TLS protokol verificirano siguran u modelu teorije složenosti
  - Suradnja INRIA i Microsoft
  - Napisan u F* - funkcijski programski jezik namijenjen verifikaciji

	Tamarin
Izvršavanje protokola	*Multiset-rewriting*: Stanje je skup terma, stanje se mijenja pravilima koja određeni skup terma u multiskupu zamijenjuje nekim drugim
Kriptografija	Enkripcija od “m” je “E(k, m)”, teorije jednakosti izražavaju svojstva poput “D(k, E(k, m))” = “m”
Napadač	Eksplicitno definirane akcije, čitanje poruka sa mreže, slanje poruka, dekripcija sa poznatim ključevima itd.
Sigurnosna svojstva	Izražena u fragmentu logike prvog reda sa kvantifikacijom nad porukama i vremenskim točkama te teorijama jednakosti Ručno ili automatsko dokazivanje pretraživanjem stanja unazad

Tamarin: Primjer definiranja akcija u protokolu




```
// Start a new thread executing the client role, choosing the server
// non-deterministically.

rule Client_1:
           [
                      Fr(~nC) // choose fresh key ,
                      !Pk($S, pkS) // lookup public-key of server
           ]
           -->
           [
                      Client_1( $S, ~nC ) // Store server and key for next step of thread ,
                      Out( aenc(~nC, pkS) ) // Send the encrypted session key to the server
           ]
```

Tamarin: Primjer definiranja sigurnosnog svojstva

```
lemma Client_session_key_secrecy:
  " /* It cannot be that a  */
    not(
      Ex S k #i #j.
        /* client has set up a session key 'k' with a server'S' */
        SessKeyC(S, k) @ #i
        /* and the adversary knows 'k' */
      & K(k) @ #j
        /* without having performed a long-term key reveal on 'S'. */
      & not(Ex #r. LtkReveal(S) @ r)
    )
  "
```

Tamarin: Dokazivanje svojstava

- Ispravnost formule se svodi na zadovoljivost negacije
- Constraint solving: iscrpno pretraživanje neekvivalentnih scenarija koji zadovoljavaju negaciju
  - Ili protuprimjer
  - Ili dokaz ispravnosti
  - Ili beskonačna petlja (Općenito neodlučiv problem)
- Najbolji rezultati: Poluautomatsko dokazivanje

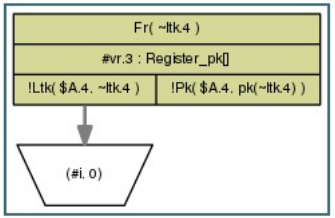
Proof scripts

```
theory FirstExample begin

Message theory

Multiset rewriting rules (8)

Untyped case distinctions (10 cases, all chains solved)

Typed case distinctions (10 cases, all chains solved)

lemma Client_session_key_secrecy:
  all-traces
  "¬(∃ S k #i #j.
          ((SessKeyC( S, k ) @ #i) ∧ (K( k ) @ #j)) ∧
          (¬(∃ #r. LtkReveal( S ) @ #r)))"
by sorry

lemma Client_auth:
  all-traces
  "∀ S k #i.
         (SessKeyC( S, k ) @ #i) ⇒
         ((∃ #a. AnswerRequest( S, k ) @ #a) ∨
          (∃ #r. (LtkReveal( S ) @ #r) ∧ (#r < #i)))"
by sorry

lemma Client_auth_injective:
  all-traces
  "∀ S k #i.
         (SessKeyC( S, k ) @ #i) ⇒
         ((∃ #a.
            (AnswerRequest( S, k ) @ #a) ∧
            (∀ #j. (SessKeyC( S, k ) @ #j) ⇒ (#i = #j))) ∨
          (∃ #r. (LtkReveal( S ) @ #r) ∧ (#r < #i)))"
by sorry

lemma Client_session_key_honest_setup:
  exists-trace
  "∃ S k #i.
         (SessKeyC( S, k ) @ #i) ∧ (¬(∃ #r. LtkReveal( S ) @
#r))"
by sorry

end
```

Untyped case distinctions

Sources of "!Ltk(t.1, t.2) ▶₀ #i" (1 cases)

Source 1 of 1 / named "Register_pk"



"!Ltk(t.1, t.2) ▶₀ #i"

last: none

formulas:

equations:
  subst:
    $A.4 <~ {t.1}
    ~ltk.4 <~ {t.2}
  conj:

lemmas:

allowed cases: untyped

solved formulas:

unsolved goals:

solved goals:
  !Ltk($A.4, ~ltk.4) ▶₀ #i // nr: 0" (useful2)"

Sources of "!Pk(t.1, t.2) ▶₀ #i" (1 cases)

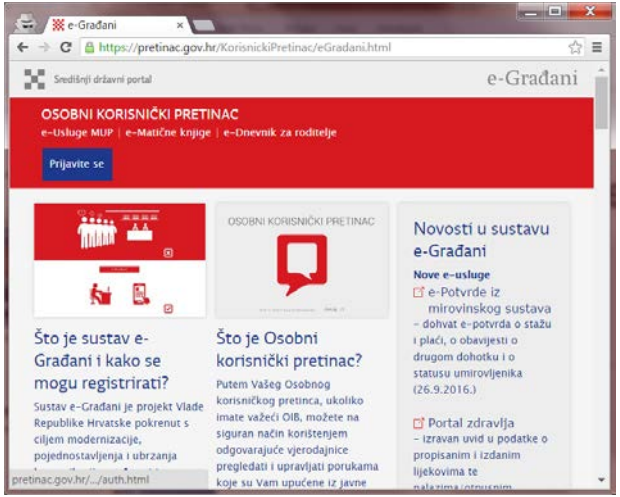
Source 1 of 1 / named "Register_pk"

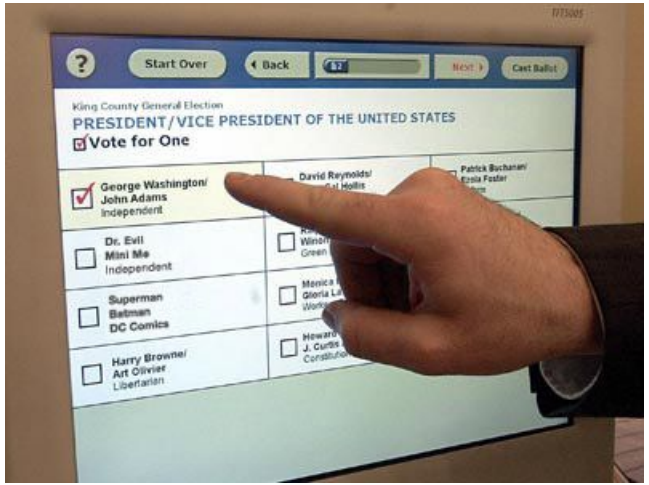
Neki rezultati [Meier et al. 2013]

	Protocol	Security property	Result	Time [s]	Details in
1.	KAS1	KI with Key Compromise Impersonation	proof	0.7	[13]
2.	NAXOS	eCK	proof	4.4	[13]
3.	STS-MAC	KI, adversary can register arbitrary public keys	attack	4.6	[13]
4.	STS-MAC-fix1	KI, adversary can register arbitrary public keys	proof	9.2	[13]
5.	STS-MAC-fix2	KI, adversary can register arbitrary public keys	proof	1.8	[13]
6.	TS1-2004	KI	attack	0.3	[13]
7.	TS2-2004	KI with weak Perfect Forward Secrecy	attack	0.5	[13]
8.	TS3-2004	KI with weak Perfect Forward Secrecy	non-termination	-	[13]
9.	UM	Perfect Forward Secrecy	attack	1.5	[13]
10.	TLS handshake	secrecy, injective agreement	proof	2.3	[10]
11.	TESLA 1	data authenticity	proof	4.4	[10]
12.	TESLA 2 (lossless)	data authenticity	proof	16.4	[10]
13.	Keyserver	keys are secret or revoked	proof	0.1	[10]
14.	Security Device	exclusivity (left or right)	proof	0.4	[10]
15.	Contract signing protocol	exclusivity (abort or resolve)	proof	0.8	[10]
16.	Envelope (no reboot)	denied access implies secrecy	proof	32.7	[10]
17.	SIGJOUX (tripartite)	Perfect Forward Secrecy	proof	102.9	[14]
18.	SIGJOUX (tripartite)	Perfect Forward Secrecy, ephemeral-key reveal	attack	111.5	[14]
19.	RYY (ID-based)	Perfect Forward Secrecy	proof	10.3	[14]
20.	RYY (ID-based)	Perfect Forward Secrecy, ephemeral-key reveal	attack	10.5	[14]
21.	YubiKey (multiset)	injective authentication	proof	19.3	[7]
22.	YubiHSM (multiset)	injective authentication	proof	7.6	[7]

Table 1. Selected results of the automated analysis of case studies included in the public TAMARIN repository. Here, KI denotes key independence.

Zaključak


e-Građani
https://pretinac.gov.hr/KorisnickiPretinac/eGradani.html
Središnji državni portal
e-Građani
OSOBNI KORISNIČKI PRETINAC
e-Usluge MUP | e-Matične knjige | e-Dnevnik za roditelje
Prijavite se
OSOBNI KORISNIČKI PRETINAC
Novosti u sustavu e-Građani
Nove e-usluge
e-Potvrde iz mirovinskog sustava – dohvat e-potvrda o stažu i plaći, o obavijesti o drugom dohotku i o statusu umirovljenika (26.9.2016.)
Portal zdravlja – izravan uvid u podatke o propisanim i izdanim lijekovima te
Što je sustav e-Građani i kako se mogu registrirati?
Sustav e-Građani je projekt Vlade Republike Hrvatske pokrenut s ciljem modernizacije, pojednostavljenja i ubrzanja
Što je Osobni korisnički pretinac?
Putem Vašeg Osobnog korisničkog pretinca, ukoliko imate važeći OIB, možete na siguran način korištenjem odgovarajuće vjerodajnice pregledati i upravljati porukama koje su Vam upućene iz javne
pretinac.gov.hr/.../auth.html


Start Over
Back
Next
Cast Ballot
King County General Election
PRESIDENT/VICE PRESIDENT OF THE UNITED STATES
Vote for One
George Washington/ John Adams Independent
David Reynolds/
Patrick Buchanan/
Dr. Evil Mini Me Independent
Superman Batman DC Comics
Harry Browne/ Art Olivier Libertarian

Hvala!

Zašto vjerovati kriptografskim protokolima?

NEWFELPRO 2013 2017

FER