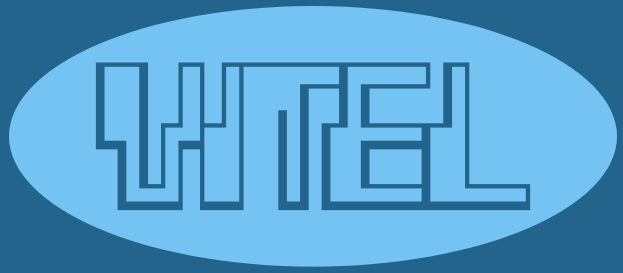


Varnost v telekomunikacijah in kako jo zagotoviti

Sašo Tomažič

Saso.tomazic@fe.uni-lj.si

Fakulteta za elektrotehniko
Tržaška 25, Ljubljana

Pomen TK v informacijski družbi

PP:
pojasnilo
pojm

- V informacijski družbi postaja informacija najpomembnejša tržna dobrina.
- Pomembno je da je prava informacija pravočasno na pravem mestu.
- To omogočajo telekomunikacijski sistemi, ki zato predstavljajo infrastrukturo informacijske družbe.
- Vse večja povezanost in odprtost informacijskih sistemov omogoča tudi različne zlorabe.
- Vedno pomembnejši vidik načrtovanja TK sistemov je zato njihova varnost.
- Vendar:
  Kaj razumemo pod pojmom varnost v telekomunikacijah?

Varnost

- Pojem varnost je zelo širok.
- V različnih kontekstih ima pojem lahko različen pomen: varnost v prometu, varnost pri delu, varna spolnost, varne telekomunikacije, ...
- Pojem je tudi subjektiven: kar je varno za nekoga je morda nevarno nekomu drugemu.
- Uporaba varnega GSM aparata med vožnjo avtomobila utegne biti zelo nevarna.

Varnost v TK

- V telekomunikacijah gre za prenos različnih sporočil. Ta sporočila so lahko sistemska ali uporabniška.
- Ko govorimo o varnosti v telekomunikacijah imamo v mislih predvsem **celovitost telekomunikacijskih sporočil**. Primernejša pojema bi bil zato lahko **zaščita** ali **varovanje** telekomunikacijskih sporočil.
- V določenih primerih bi temu lahko dodali: zanesljivost, dostopnost, odpornost proti motenju, odpornost proti detekciji, ...

Celovitost sporočil

Pod pojmom celovitost razumemo:

- zasebnost (vsebina sporočila je dostopna samo upravičenemu uporabniku),
- verodostojnost (sporočilo ni bilo spremenjeno, namerno ali nenamerno) in
- avtentičnost (nedvomno je znana identiteta izvora, tega kasneje tudi ni mogoče zanikati).

Zagotavljanje celovitosti

- Vsi vidiki celovitosti so enako pomembni.
- V e-bančništvu sta npr. verodostojnost in avtentičnost celo pomembnejši od zasebnosti.
- Celovitost lahko zagotavljamo na različne načine (nedostopnost prenosne poti, terminalne opreme, zanesljive prenosne poti, ...)
- Vse vidike celovitosti je mogoče zagotoviti z ustrezno uporabo šifrirnih postopkov.

Zagotavljanje celovitosti

Zavedati se moramo

- da telekomunikacijski sistem sam po sebi ne more zagotavljati celovitosti informacijskega sistema, ki ta sistem uporablja,
- da je mogoče zagotoviti popolno celovitost le z uporabo šifrirnih postopkov na končnih točkah komunikacije (end to end) in to le za uporabniška sporočila in
- da za nekatera sistemska sporočila ni mogoče zagotoviti vseh vidikov celovitosti.

Šifrirni postopki

- Šifrirni postopek preslika razumljivo sporočilo (čistopis) v nerazumljivo sporočilo (šifropis).
- Obratna preslikava (dešifriranje) je mogoča le, če poznamo neko skrivno informacijo (tajni ključ).
- Varnost postopka naj temelji na tajnosti ključa in ne na tajnosti postopka (ni upoštevano v GSM)
- Glede na vrsto ključev ločimo:
  - simetrične šifrirne postopke in
  - asimetrične šifrirne postopke.

Simetrični postopki

- Za šifriranje in dešifriranje se uporablja isti ključ.
- Ključ predstavlja skupno skrivnost, ki jo morajo poznati vsi udeleženci komunikacije.
- Ključ si morajo udeleženci pred komunikacijo izmenjati na nek varen način.
- Ločimo bločne in pretočne šifrirne postopke.

Asimetrični postopki

- Imamo par ključev: ključ za šifriranje in ključ za dešifriranje.
- Tajen mora biti le ključ za dešifriranje. Imenujemo ga tudi privatni ključ.
- Ključ za šifriranje je lahko splošno poznan. Imenujemo ga tudi javni ključ.
- Postopki so zasnovani na enosmerni funikciji s stranskim vhodom (one way trap dor function).

Enosmerna funkcija

šifriranje

tajni ključ

odpira stranska vrata

(dešifriranje)

javni ključ

Varnost šifrirnih postopkov

Cilji kriptoanalize

- dešifrirati sporočilo,
- odkriti tajni ključ,
- odkriti šibkost šifrirnega postopka

Vrste napadov

- zgolj na osnovi šifropisa,
- na osnovi para čistopis-šifropis
- na osnovi izbranih parov čistopis-šifropis

Varnost šifrirnih postopkov

- Teoretična varnost
  - Dešifriranje teoretično ni mogoče ne glede na vložen čas in sredstva.
  - Teoretično varen postopek je sprotno šifriranje z enkratno uporabo ključa.
- Praktična varnost
  - Dešifriranje ni mogoče v omejenem času z omejenimi sredstvi.
  - Varnost je odvisna od postopka in od dolžine ključa.
  - Pomen dolžine ključa je različen pri simetričnih in asimetričnih postopkih.

Vpliv dolžine ključa

- Če simetrični šifrirni postopek nima šibkosti, je edini možni napad preizkušanje vseh možnih ključev.
- Za preizkušanje vseh 128 bitnih ključev bi potrebovali 10 miljard miljard tisočletij, če bi vsako sekuddo preizkusili miljardo ključev.
- Pri asimetričnih postopkih zadošča da iz javnega ključa izračunamo tajnega.
- Pri RSA je zato potrebna faktorizacija produkta dveh praštevil.
- Varnost je torej odvisna od trenutnega stankja na področju faktorizacije. 128 bitnemu simetričnemu ključu trenutno ustreza 2048 bitni RSA ključ.

Protokoli

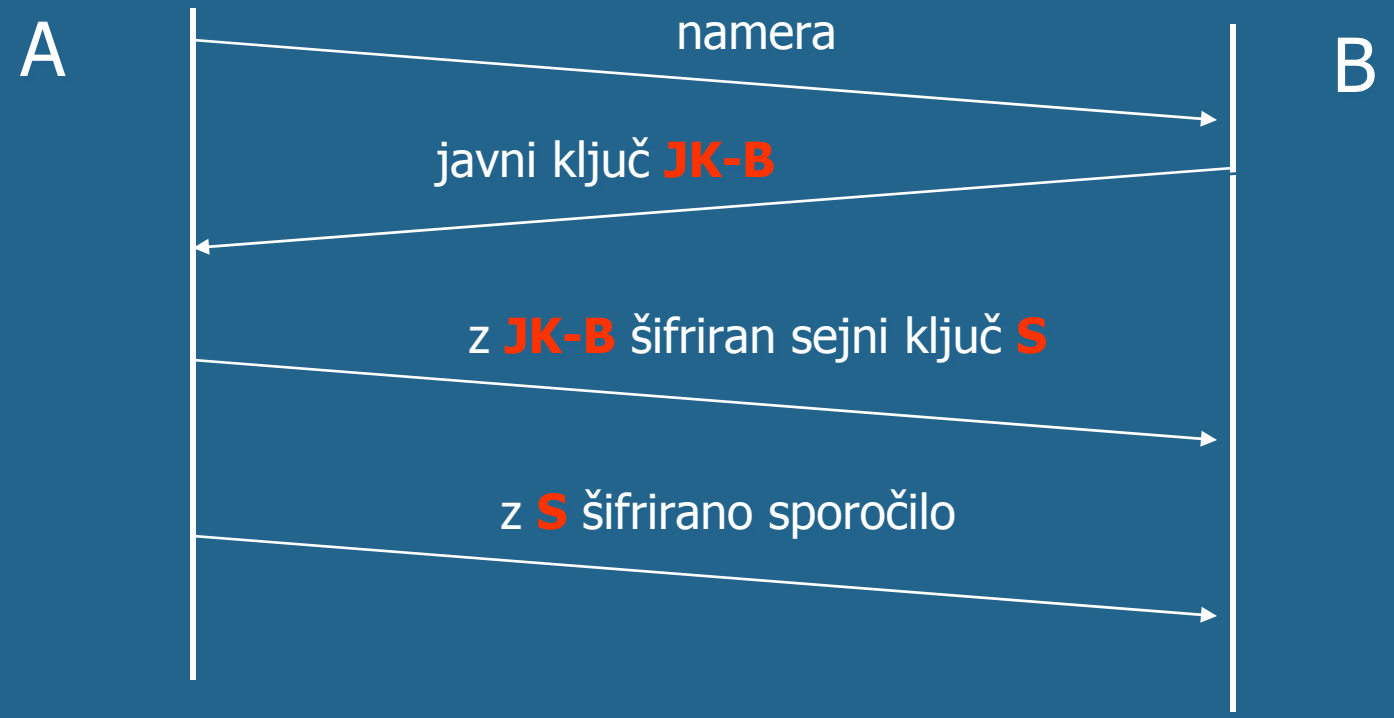
- Različne vidike celovitosti lahko zagotovimo, ko šifrirne postopke uporabimo v ustreznih protokolih.
- Varnost samih šifrirnih postopkov je zelo visoka.
- Kljub temu, da uporabimo varne šifrirne postopke, imajo lahko protokoli šibkosti, ki jih lahko napadalec izkoristi.
- Večina uspešnih napadov v preteklosti je temeljila na šibkostih v protokolih ali neodgovornem obnašanju uporabnikov.

Protokoli

- Zasebnost zagotavljamo z šifriranjem najbolj neposredno. Pri simetričnih postopkih potrebujemo ustrezen protokol za izmenjavo ključev (npr. Diffie Hellmanova eksponentna izmenjava ključev)
- Verodostojnost lahko zagotovimo z uporabo zgoščevalnih funkcij oziroma digitalnega podpisa, ki temelji na asimetričnih šifrirnih postopkih.
- Za zagotavljanje avtentičnosti, predvsem nezmožnosti zanikanja je potreben poseben urad za overjanje javnih ključev (CA – certification authority)
- V določenih primerih je potreben za zagotavljanje avtentičnosti tudi elektronski notar, ki daje časovni žig.

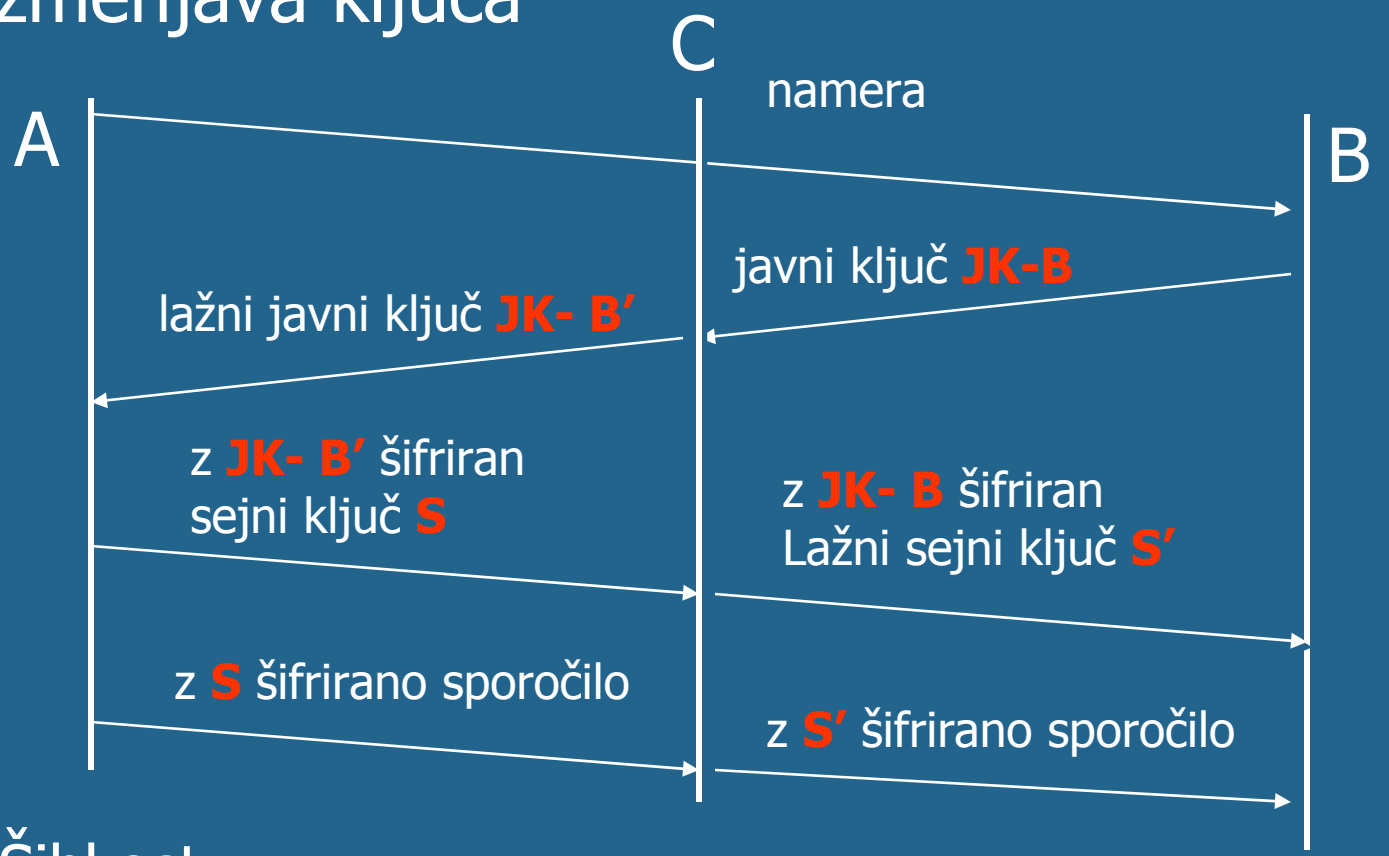
Primer protokola

Izmenjava ključa



Šibkost protokola

Izmenjava ključa



Šibkost:

Ni zagotovljena verodostojnost pri prenosu javnega ključa in avtentičnost uporabnikov.

Varnostna politika

- Informacijski sistemi so vedno bolj povezani in vedno bolj dostopni.
- Dostopnost teh sistemov povečuje njihovo ranljivost.
- Povezanost v javno Internet omrežje je lahko zelo koristna vendar tudi zelo nevarna.
- Z gotovostjo lahko trdimo, da bo sistem povezan v javni Internet slej ko prej napaden (npr. preko 2000 poskusov vdora na moj računalnik v zadnjem letu)
- Celovita zaščita je lahko zelo draga. Cena zaščite naj ne bi presegala vrednosti varovanih podatkov.
- Kaj in kako bomo ščitili, določimo z varnostno politiko.

Varnostna politika

Z varnostno politiko določimo:

- kateri deli informacijskega sistema so posebno vitalni in jih je potrebno bolj zaščititi,
- kateri uporabniki sistema imajo pravico dostopa do javnega omrežja in kakšne so te pravice,
- kateri uporabniki imajo pravico dostopa iz javnega omrežja in kakšne so te pravice,
- kakšne zaščitne ukrepe bomo uvedli (požarni zid, protivirusna zaščita, ločitev delov omrežij, ...) in
- pravila obnašanja uporabnikov sistema.