# Omrežja in zasebnost

## Cilji

Učenec:

- razume, da je storitev, ki jo nudi računalniško omrežje, dostava sporočil od pošiljatelja do prejemnika po najboljših močeh;
- razloži, da so sporočila, ki jih računalniško omrežje prenaša, omejeno dolga in zato daljša sporočila razdelimo na krajša (pakete), ki se prenašajo neodvisno eno od drugih;
- spozna, da je vsebina sporočila, ki jo omrežje prenaša, ranljiva in da jo lahko zaščitimo s šifriranjem;
- razlikuje med identiteto in potrjeno (overjeno, avtenticirano) identiteto ter, da je s podatki za overovitev potrebno rokovati posebej previdno;
- pojasni, da imajo pravico do vpogleda v posamezne podatke ali uporabo storitev (so avtorizirane) samo overjene identitete;
- razloži, da so nekateri podatki posamezniku posebej pomembni in predstavljajo njegovo zasebnost ter jih mora posebej dobro varovati;
- pojasni, da s svojo dejavnostjo na spletu pušča o tem sled (digitalni odtis), ki lahko razkriva o njem različne zasebnosti.

## Standardi znanja

Učenec:

- razloži, kako lahko preko računalniškega omrežja prenesemo sporočilo, ki je veliko 300 črk, če so posamezna sporočila lahko velika samo 123 črk;
- razloži zakaj je vsebina sporočila, ki jo omrežje prenaša, ranljiva;
- opiše različne načine overitve identitete, s čemer slednjo varujemo pred krajo;
- pojasni zakaj je s podatki za overovitev potrebno rokovati posebej previdno (močna gesla ipd.);
- razloži, kaj je digitalni odtis in opiše primer, ko razkriva kakšno posameznikovo zasebnost (npr. fotografije, ime in priimek, kraj bivanja, EMŠO, slika osebnega dokumenta, …);

## Termini

- računalniško omrežje
- Internet in splet
- paket
- zakrivanje podatkov (šifriranje)
- identiteta
- overovitev (avtentikacija)
- pravica do dostopa (avtoriziranost)
- digitalni odtis
- zasebnost

## Didaktična priporočila za skupino ciljev

Na osnovi https://redmine.lusy.fri.uni-lj.si/documents/321.

Doseganje učnih ciljev lahko preoblikujemo v spoznavanje naslednjih principov in konceptov, ki jih podajamo v treh delih:

1. ***Tehnologija računalniških omrežij***:
   - storitev, ki jo nudi računalniško omrežje, je dostava sporočil od pošiljatelja do prejemnika po najboljših močeh;
   - sporočila, ki jih računalniško omrežje prenaša, so omejeno dolga in zato daljša sporočila razdelimo na krajša (pakete), ki se prenašajo neodvisno eno od drugih;
   - ker je vsebina sporočila, ki ga omrežje prenaša, ranljiva ga lahko zaščitimo s šifriranjem;
2. ***Identifikacija, overitev (avtentikacija) in pravica do dostopa (avtorizacija)***:
   - kaj je identiteta in kaj je potrjena (overjena, avtenticirana) identiteta;
   - kakšni so običajni pristopi za potrjevanje identitete in zakaj je s podatki za overovitev potrebno rokovati posebej previdno;
   - kako je pravica do vpogleda v posamezne podatke ali uporabo storitev (so avtorizirane) zasnovana na konceptu identitete;
3. ***Zasebnost***:
   - podatki, ki so posamezniku posebej pomembni,- predstavljajo njegovo zasebnost ter jih mora posebej dobro varovati;
   - posameznikova dejavnost na spletu  se tako ali drugače lahko beleži in na spletu pušča o tem sled (digitalni odtis), ki lahko razkriva o posamezniku različne zasebnosti.

Splošna navodila:

- vse dejavnosti se lahko izvajajo brez računalnika, vseeno pa ta navodila dopolnjujemo tudi s kratkimi komentarji, kako lahko vključimo digitalno tehnologijo;
- priporoča se, da je izvedba kar se da interaktivna in da so učenci izzvani, da identificirajo probleme ter da tudi predlagajo rešitve zanje – vsi problemi, ki jih obravnavamo so izrazito preprosti.

# Tehnologija računalniških omrežij:

Problem, ki ga ima Borut je, da bi rad povabil ob 5:12 Ano na čaj, a Ana živi v drugem kraju.

Borut najde novo tehnologijo, računalniško omrežje, ki naj bi omogočala takšno posredovanje sporočil med oddaljenimi kraji:


Opomba: zeleni oblak predstavlja omrežje in ga lahko narišemo tudi na tla (glej naprej).

Učence vprašamo: »Če bi vi bili Borut, kakšno točno pomoč ali storitev bi si želeli od omrežja?«

Po pogovoru se oblikuje odgovor, da je storitev, ki si jo želimo, dostava sporočil od pošiljatelja do prejemnika, pri čemer prejemnik poleg sporočila dobi še informacijo, od koga je sporočilo.

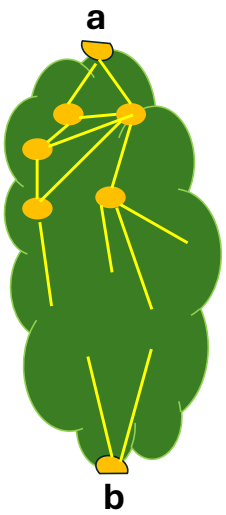
Borut napiše sporočilo listek, ga preda omrežju in le-to ga preda Ani vključno z dodatnim listkom, na katerem piše »Borut«, saj on pošilja sporočilo.

Opomba: Ta del lahko naredimo na računalniku s programom v jeziku Python:

| Borut | Ana |
|---|---|
| `import socket`<br>`Borut = "127.0.0.1"`<br>`kje = 5005`<br><br>`vtic = socket.socket(socket.AF_INET,`<br>`socket.SOCK_DGRAM)`<br>`vtic.sendto(b"Greva na caj ob 5:12?",`<br>`(Borut, kje))` | `import socket`<br><br>`Borut = "127.0.0.1"`<br>`kje = 5005`<br>`nvs = 1024 # najv. velikost sporocila`<br><br>`vtic = socket.socket(AF_INET, SOCK_DGRAM)`<br>`vtic.bind((Borut, kje))`<br><br>`sporocilo, posiljatelj = vtic.recvfrom(nvs)`<br>`print(f"{posiljatelj}: {sporocilo}")a` |

Učence vprašamo: »Kako pa omrežje zagotovi opisano storitev?« Preden pričnemo pogovor o vprašanju pripomnimo, da se omrežje sestoji iz vozlišč. Le-ta si podajajo sporočilo tako dolgo, da pride od pošiljatelja **b** do naslovnika **a**.

Opomba: Slika na desni je shematična, sicer sestoji iz množice (~20) medsebojno naključno povezanih vozlišč, ki naj bodo označena s številkami.




Učence vprašamo: »Kako izgleda eno vozlišče? Kaj pravzaprav je vozlišče?«

Po pogovoru ugotovimo, da je vozlišče nekakšen računalnik z aplikacijo, ki:

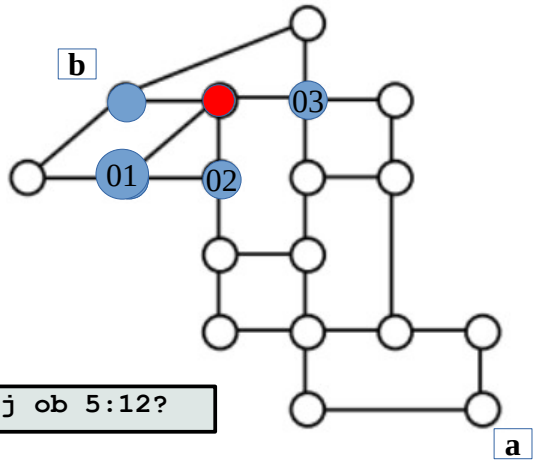
- prejme sporočilo od soseda
- če je naslovnik na njegovem vozlišču, mu preda sporočilo,
- sicer ga preda sosedu, da ga on dostavi naslovniku.

Učence vprašamo: »Kaj pravzaprav potuje po omrežju?«

Opomba: Slika na desni je shematična, sicer sestoji iz množice (~20) medsebojno naključno povezanih vozlišč, ki naj bodo označena s številkami.

| Greva na čaj ob 5:12? |
|---|

Po pogovoru z učenci ugotovimo, da potuje samo sporočilo s povabilom na čaj. »Ali, ko sporočilo pride do, recimo, rdečega vozlišča, le-to ve, komu je namenjeno?«




Po pogovoru ugotovimo, da moramo sporočilo dopolniti z dodatkom, ki bo hranil podatke o naslovniku. Tem dodatnim podatkom rečemo metapodatki, ki se hranijo ločeno od sporočila v glavi:

| za: **a** | Greva na čaj ob 5:12? |
|---|---|

Ko končno pripotuje sporočilo s podatki do **a**, ga predamo Ani. »Je vse v redu?« Po pogovoru ugotovimo, da je storitev obljubljala, da bo prejemnik zvedel kdo je pošiljatelj – glej zgoraj. »Pa lahko sporočimo, kdo pošilja sporočilo glede na sporočilo in metapodatke?«

Po pogovoru razširimo metapodatke s podatki o pošiljatelju.

| za: **a**, od: **b** | Greva na čaj ob 5:12? |
|---|---|

Učence vprašamo: »Kako se naj vozlišče odloči, kateremu sosedu naj preda sporočilo? Konkretno, komu naj preda rdeče vozlišče sporočilo, da bo prišlo do **a**?«

Učenci bodo verjetno predlagali, da se sporočilo prepošlje vozlišču 02 ali 03, ker sta na poti proti **a**. Opozorimo jih, da rdeče vozlišče »vidi« zgolj modra vozlišča, »Kaj sedaj?«

Verjetno bo moral pomagati učitelj, ki predlaga, da ima vsako vozlišče dodatno tabelo, v kateri piše, katermu sosedu naj preda sporočilo, če je namenjeno **a** in kateremu, le je namenjeno **b**. Rdeče vozlišče ima tabelo z vsebino:

| Za koga | Kateri sosed |
|---|---|
| a | 03 |
| b | b |

Tabela se imenuje prepošiljevalna tabela.

Dodatne aktivnosti:

1. učenci za vsa vozlišča omrežja sestavijo podobne prepošiljevalne tabele;
2. v vsako vozlišče se postavi en učenec, ki ima pri sebi prepošiljevalno tabelo tega vozlišča. Sedaj, ko od soseda prejme sporočilo, pogleda metapodatke in glede na vnos v svoji prepošiljevalni tabeli ter preda sporočilo ustreznemu sosedu;
3. na enem vozlišču tabelo povsem pokvarimo. Z učenci preverimo, ali sporočila še vedno prihajajo? Ugotovimo, da morda nekatera sedaj ne pridejo več do prejemnika.

   Učence spomnimo, da smo na začetku o dostavi sporočil zapisali, da storitev omrežja dostavi sporočilo od pošiljatelja do prejemnika, kar pomeni, da ji to vedno uspe. Ker pa lahko, kot smo opisali, prihaja do okvar na vozliščih ni nobene garancije, da bo sporočilo

dostavljeno. Zato omilimo zahtevo po dostavi v dostava sporočil **po najboljših močeh**.

Posledično je popravljena definicija storitve, ki jo nudi računalniško omrežje: »dostava sporočil od pošiljatelja do prejemnika po najboljših močeh, pri čemer prejemnik poleg sporočila dobi še informacijo, od koga je sporočilo«

4. nazadnje prepošiljevalne tabele v vozliščih razširimo tako, da dodamo vnose (vrstice) za vsa vozlišča in ne samo **a** in **b**;

Borut in Ana sta ondan se le dobila na čaju in izkazalo se je, da je bilo to zelo koristno, saj je Borut povsem pozabil na domačo nalogo, na kar ga je Ana opozorila. Ni pa šlo vse gladko, saj Ana ni vedela, v katerem lokalu se naj bi dobila. A sta se le nekako našla.

Tokrat je na čaj vabila Ana, ki pa je seveda želela v sporočilu tudi zapisati, kje se na dobita: »Greva na čaj ob 5:12? V istem lokalu kot zadnjič.« Pojavila se je zadrega:

| | |
|---|---|
| za: **b**, od: **a** | **Greva na čaj ob 5:12? V** |

Učence vprašamo; »Sporočila, ki jih računalniško omrežje prenaša, so omejeno dolga in kaj sedaj?«

Po pogovoru predlog, da se daljše sporočilo razdeli na vč krajših sporočil (paketov), ki se prenašajo neodvisno eno od drugih.

| | |
|---|---|
| za: **b**, od: **a**, zap=1 | **Greva na čaj ob 5:12? V** |
| za: **b**, od: **a**. zap=2 | **istem lokalu kot zadnj** |
| za: **b**, od: **a**, zap=3 | **ič.** |

Učence vprašamo: »Med metapodatki se je pojavil podatek zap – zakaj?«

Simulirajte prenos teh treh paketov ter vmes pokvarite prepošiljevalno tabelo in opazujte kaj se dogaja. Komentirajte.

Tokrat se je zdelo, da bo s čajem vse v redu, a glej ga zlomka – v lokalu se je pojavil Anin mlajši brat Cene. Ana in Borut sta se spogledala, kako je lahko Cene zvedel za čaj?

Vprašanje za učence: »Kako je lahko Cene zvedel za čaj?«

V vodenem pogovoru učenci ugotovijo, da kdorkoli, ki lahko dostopa do paketov, lahko prebere sporočilo. Rešitev je šifriranje vsebine (gl. https://encrypt-online.com/ - učenci naj poskusijo).

Borut in Ana izmenjata ob čaju skupno sklrivnost, ki jo poznata samo onadva: 6115f54e-42ec-4d96-a7ab-cd35de8bf43f in se dogovorita za DES3 šifriranje. Tako Ana tokrat pošlje sporočilo
U2FsdGVkX1+CTXNCz/XuwuMpZ0RW8GsZfYgtxwiMeuDC7GuUuU4nanuQPv7RcRMEmUmupt7WBY8k+YlG7nT+3d9lvti4Km3H.

Dodatne aktivnosti:

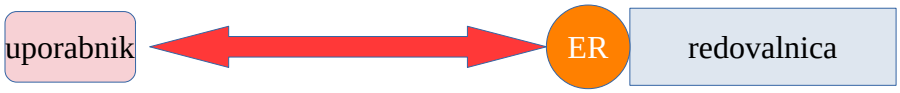
1. učenci oblikujejo pakete in jih pošljejo
2. pogovor z učenci, zakaj ne pošiljamo skupne skrivnosti kot dela sporočila;

3. še se še kaj doda med metapodatke; namig DES3;
4. v brskalniku pokažemo na zaklenjeno ključavnico, kar pomeni, računalniško omrežje samo šifrira podatke v premikanju,

## Identifikacija, overitev (avtentikacija) in pravica do dostopa (avtorizacija):

Pogovor z učenci pričnemo pri neki aktivnosti, ki jo nekdo ima pravico izvesti in nekdo drug ne. Ker moramo posameznika razlikovati, ima vsak od njiju s identiteto, oziroma trdi, da jo ima. To, da res ima identiteto, kot trdi, mora dokazati, oziroma jo moramo overiti.

Borut in Ana sta tudi sošolca, njun razrednik je Urban. Obstaja razredna redovalnica in vanjo lahko vpisujemo ocene in jih pogledamo. Očitno ima Urban pravico (je avtoriziran) vnosa ocen, medtem ko imata Ana in Borut pravico (sta avtorizirana) za vpogled vsak v svoje ocene.




Narišemo shematsko zgornjo sliko in pričnemo z učenci pogovor o toku pogovora med uporabnikom in sistemom elektronske redovalnice.

**Primer 1**: Uporabnik je Ana.

1. uporabnik: jaz sem Ana (to je isto, kot bi posredovali svoje uporabniško ime, e-naslov – pač naš ID)
2. ER: pozdravljena Ana
3. uporabnik: Kakšna je zadnja Borutova ocena
4. ER: nedovoljen vpogled, samo Borut lahko to vidi
5. uporabnik: Kakšna je zadnja Anina ocena
6. ER: 5

**Primer 2**: Uporabnik je Cene.

1. uporabnik: jaz sem Ana (to je isto, kot bi posredovali svoje uporabniško ime, e-naslov – pač naš ID)
2. ER: pozdravljena Ana
3. uporabnik: Kakšna je zadnja Borutova ocena
4. ER: nedovoljen vpogled, samo Borut lahko to vidi
5. uporabnik: Kakšna je zadnja Anina ocena
6. ER: 5

V tem primeru se Cene izdaja za Ano, kar ER upošteva in smatra, da je uporabnik Ana.

Sledi pogovor z učenci, kaj je narobe? Ugotovijo, da ER verjame na besedo uporabniku in ne preverja njegove trditve – identiteta ni overjena.

Pogovor: kako naj ER preveri uporabnikovo trditev glede identifikacije? Konkretno, kako naj Ana prepriča ER, da je res ona ona?

Kmalu se izoblikuje predlog, da je to nekaj, kar poznata samo Ana in ER. Geslo je primer takšnega podatka ali skupna skrivnost za šifriranje zgoraj in podobno.

**Primer 1a**: Uporabnik je Ana.

1. uporabnik: jaz sem Ana (to je isto, kot bi posredovali svoje uporabniško ime, e-naslov – pač naš ID)
2. ER: Lahko dokažeš, da si res Ana
3. uporabnik: Moje geslo je ********
4. ER: res si Ana
5. Kakšna je zadnja Borutova ocena
6. ER: nedovoljen vpogled, samo Borut lahko to vidi
7. uporabnik: Kakšna je zadnja Anina ocena
8. ER: 5

**Primer 2a**: Uporabnik je Cene.

1. uporabnik: jaz sem Ana (to je isto, kot bi posredovali svoje uporabniško ime, e-naslov – pač naš ID)
2. ER: Lahko dokažeš, da si res Ana
3. uporabnik: Moje geslo je ********
4. ER: ti nisi Ana

Pogovor z učenci:

- o razliki med potrjeno (overjeno, avtenticirano) identiteto in nepotrjeno identiteto v navezavi s pravicami;
- o tem, kaj pravzaprav pomeni, če je identiteta overjena – ali v resnici gre za Ano ali samo za nekoga, ki zna potrditi Anino identiteto?
- Kako se lahko zgodi, da nekdo zna potrditi Anino identiteto?
  - En način je, da ugane skupno skrivnost => skupna skrivnost (geslo) naj bo čim bolj naključen niz znakov.
  - Drug način pa je, da je ukradel ali dobil skupno skrivnost od Ane.
  - V obeh primerih gre za krajo identitete.
- Pogovor o varovanju gesla in kaj bi pomenilo njegovo deljenje v najslabšem primeru.

Zaključek: geslo naj bo čim bolj naključno in nikoli ga ne delimo z nikomer.

Pogovor z učenci kakšni so običajni pristopi (drugi načini) za potrjevanje identitete? Poskusimo usmerjati pogovor tako, da se pogovor osredotoči na različne naprave. Dobimo na primer: prstni odtis (telefon, hiša, …), pin koda, digitalni certifikat, …

V grobem delimo načine potrjevanja na tiste, ki preverjajo, kaj vemo (geslo, PIN, …) in na tiste, ki preverjajo kaj posedujemo (telefon, prstni odtis, …). Opis konkretnega primera posedovanja telefona.

Seveda lahko kombiniramo pristope in dobimo večdelno overitev.

## Zasebnost:

Najprej je potrebno opredeliti pojem zasebnosti in nato kako ga varovati.

SSKJ, druga, dopolnjena in deloma prenovljena izdaja, www.fran.si, dostop 25. 10. 2025.:

> zasébnost -i ž (ẹ́)
> 1. značilnost zasebnega: zasebnost premoženja / zasebnost izpovedi
> 2. zasebno življenje, delovanje: razlika med zasebnostjo in javnim delovanjem / zanimati se za zasebnosti koga

Sledi pogovor o tem, kaj je zasebno in kdo določa kaj je zasebno in kako varujemo zasebnost?
V grobem bo odgovor da so podatki, ki opisujejo posameznikovo zasebnost njemu posebej pomembni. Zato jih mora še posebej dobro varovati.
V nadaljevanje pogovora z učenci o konkretnih primerih; npr.:

- poletne počitnice in objava slik z njih, kaj pomeni in kako lahko škoduje ali koristi njihova objava.
- Ob tem se vračamo z učenci na to, kdo ima pravico vpogleda; v razmisleku naj opazijo, da vpogled pomeni kopiranj in nadaljnje razpečevanje.

Zadnja tema so opažanja in pogovor o njih:

- ko vprašamo Google (ali kakšno drugo storitev) za pot, nam dodatno sporoči, da je na njej precej prometa. Kako to ve?
- ko iščemo na spletu naslov knjige, nam brskalnik magično ponudi zanimive naslove. Kako to zna?

V pogovoru ugotovimo, da

- v prvem primeru naši telefoni sporočajo Google, kje so in iz tega podatka lahko naračuna gostoto prometa; in
- v drugem primeru si brskalnik zapomni, kaj smo že kdaj iskali in tako poskuša podati prejšnjim iskanjem skladne predloge.

V pogovoru najdemo še več primerov »pametnega« obnašanja storitev in vsi podatki skupaj, ki jih uporabljajo stoitve tvorijo naš digitalni odtis.
Posameznikova dejavnost na spletu  se tako ali drugače lahko beleži in na spletu pušča o tem sled (digitalni odtis), ki lahko razkriva o posamezniku različne zasebnosti.

Sledi pogovor o zmanjšanju digitalnega odtisa in njegivi povezanosti s posameznikovo zasebnostjo.