Sigurnost u računarskim mrežama

Obrada metapodataka

Nemanja Maček

Sadržaj

Šta su metapodaci?

NSA i metapodaci.

- Edvard Snouden je, između ostalog, ukazao na činjenicu da NSA* sakuplja i obrađuje metapodatke (engl. *metadata*) o komunikacijama građana:
  - ko koga zove, ko kome šalje i-mejl ili prouku,
  - kada se komunikacija odvija,
  - gde se u tom trenutku korisnici usluge nalaze, itd.
- Termin **metapodaci**** se koristi za označavanje podataka koji ne otkrivaju sadržaj komunikacije.

* Američka služba za nacionalnu bezbednost.

** Ovaj termin ima različita značenja u različitim kontekstima.

Šta su metapodaci?

Kako stoje stvari u Evropi?

- Direktivom 2006/24/E3 Evropskog parlamenta i Veća Evropske Unije se svim telefonskim kompanijama i Internet provajderima u EU definiše obaveza zadržavanja podataka potrebnih za:
  - pronalaženje i identifikaciju izvora komunikacije,
  - otkrivanje odredišta komunikacije,
  - utvrđivanje datuma, vremena i trajanja komunikacije,
  - otkrivanje vrste komunikacije,
  - identifikaciju komunikacijske opreme,
  - otkrivanje lokacije opreme za mobilnu komunikaciju.
- Direktiva predviđa da se ovi podaci čuvaju u periodu ne kraćem od 6 meseci, i ne dužem od dve godine.

Šta su metapodaci?

Primeri metapodataka.

- Primere metapodataka ćemo razmatrati na dva slučaja:

T

- Telefonija u fiksnoj ili mobilnoj mreži,

I

- pristup Internetu, elektronska pošta, Internet telefonija.

Šta su metapodaci?

Pronalaženje i identifikacija izvora komunikacije.

- Metapodaci:

T

- Telefonski broj sa kojeg dolazi poziv,
- ime i adresa pretplatnika ili registrovanog korisnika.

I

- Dodeljena korisnička imena,
- korisničko ime i telefonski broj dodeljen svakoj komunikaciji kojom se stupa u javnu telefonsku mrežu,
- ime i adresa pretplatnika ili registrovanog korisnika kojem je u trenutku komunikacije dodeljena adresa Internet protokola (IP), korisničko ime ili telefonski broj.

Šta su metapodaci?

Otkrivanje odredišta komunikacije.

- Metapodaci:

  T

  - Birani brojevi, uključujući i brojeve na koje je poziv eventualno preusmeren,
  - imena i adrese pretplatnika ili registrovanih korisnika.

  I

  - Korisničko ime ili telefonski broj primaoca kome je upućen poziv preko Internet-telefonije,
  - imena i adrese pretplatnika ili registrovanog korisnika, i korisničko ime primaoca kome je komunikacija namenjena.

Šta su metapodaci?

Utvrđivanje datuma, vremena i trajanja komunikacije.

- Metapodaci:

T

- Datum i vreme početka i završetka komunikacije.

I

- Datumi i vremena prijave za uslugu i odjave od usluge pristupa Internetu, prema određenoj vremenskoj zoni, IP-adresa dodeljena komunikaciji, korisničko ime pretplatnika ili registrovanog korisnika,
- datumi i vremena prijave za uslugu i odjave od usluge elektronske pošte ili Internet telefonije, prema određenoj vremenskoj zoni.

Šta su metapodaci?

Otkrivanje vrste komunikacije.

- Metapodaci:

  T

  - Korišćena telefonska usluga.

  I

  - Korišćena Internet usluga.

Šta su metapodaci?

Identifikacija komunikacione opreme.

- Metapodaci:

  T

  - Telefonski brojevi sa kojih se poziva i koji se pozivaju, a za mobilnu telefoniju i identifikatori IMEI i IMSI strane koja poziva i koja se poziva.
  - Za unapred plaćene anonimne usluge: datum i vreme početka vršenja usluge, lokacijska oznaka (identitet ćelije) sa koje je usluga aktivirana.

  I

  - Telefonski broj sa kojeg se poziva,
  - digitalna pretplatnička linija (DSL) ili druga krajnja tačka strane koja započinje komunikaciju.

- Podsetnik:
  - IMEI (*International Mobile Station Equipment Identity*) je ID mobilnog telefona.
  - IMSI (*International Mobile Subscriber Identity*) je ID korisnika mobilnog telefona.

Šta su metapodaci?

Kako to izgleda u praksi?

- Malte Špilc (Malte Spiltz), nemački političar iz stranke Zelenih, je, posle podnošenja tužbe, od Dojče Telekoma (*Deutsche Telekom*) dobio izveštaj o 35830 unosa o svojim komunikacijama u periodu od 6 meseci.
- U proseku, podaci o njemu su beleženi na svakih 7-8 minuta.

Šta su metapodaci?

Šta na ovo kažu (neki) zvaničnici?

- „To su samo metapodaci“.
- Drugim rečima, pošto metapodaci ne uključuju sadržaj komunikacije, trebalo bi da zaključimo da je njihovo sakupljanje bezopasno.
- Ovakav zaključak je pogrešan!
  - Metapodaci takođe nose informaciju o vama!
  - A pošto su strukturirani njihova obrada je relativno laka.
- U nastavku ćemo razmotriti izabrane aspekte obrade metapodataka i ukazati na bezbednosne rizike vezane za ovu raširenu praksu.

Šta su metapodaci?

Šta na ovo kažu (neki) zvaničnici?

- Stjuart Bejker (Stewart Baker), bivši generalni savetnik NSA, je izjavio: „Metapodaci nam govore apsolutno sve o nečijem životu. Ukoliko imate dovoljno metapodataka, ne treba vam stvarno sadržaj“.
- Majkl Hejden (Michael Hayden), bivši generalni direktor CIA i NSA, je 2014. godine izjavio: „Ubijamo ljude na osnovu metapodataka“.

Obrada telefonskih metapodataka

Metapodaci = veze između ljudi.

- Jedan od ciljeva analize telefonskih metapodataka je da se utvrde veze između različitih entiteta.

Mapiranje veza

Osumnjičeni ...

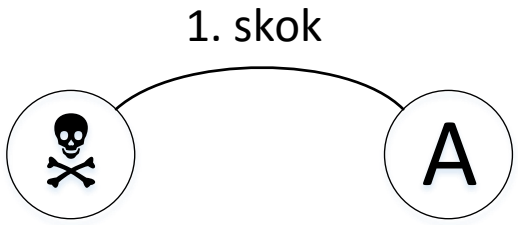
- Identifikuje se broj za čijeg vlasnika postoji osnovana sumnja da, na primer, učestvuje u terorističkim aktivnostima.
- Kriterijumi za izbor osumnjičenih nisu obavezno restriktivni.

- Za ovaj broj se, između ostalog, primenjuju mere prikupljanja podataka o telefonskim razgovorima.

Mapiranje veza

Direktni kontakti ...

- Ako je ☠ direktno kontaktirao sa A, onda se i za A mogu primeniti mere prikupljanja podataka o telefonskim razgovorima.

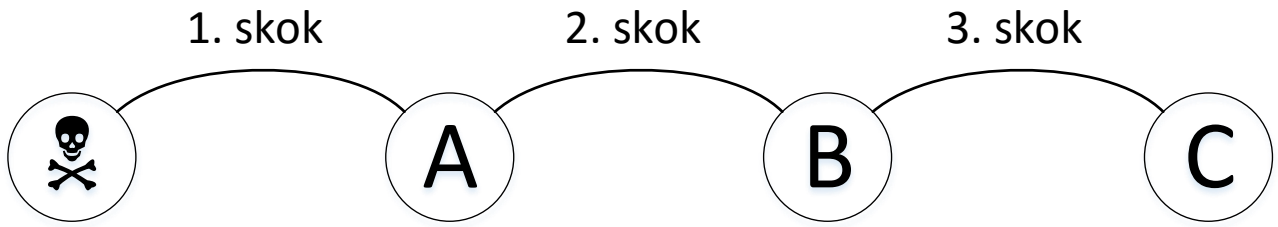


- Ni ovde kriterijumi nisu restriktivni – na primer, dovoljno je da su ☠ i A ostvarili jedan telefonski razgovor u poslednjih pet godina.

Mapiranje veza

Posredni kontakti ...

- Pretpostavimo da je A komunicirao sa B, a B sa C.
- I za njih se mogu primeniti mere prikupljanja podataka o telefonskim razgovorima.

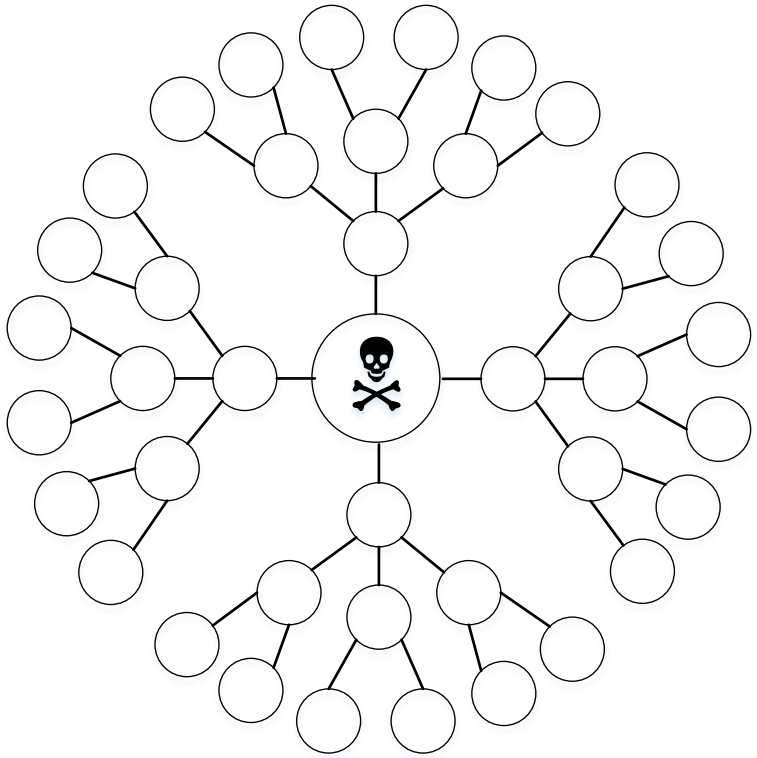


- Koliko skokova se praktikuje?
  - Ne možemo odgovoriti sa sigurnošću.
  - NSA je 2013. godine navodno koristila tri skoka.

Mapiranje veza

Mreža praćenih entiteta.

- Međutim, ☠ ne komunicira samo sa A, niti A sa B itd.
- Broj praćenih entiteta u ovoj mreži raste eksponencijalno.



Mapiranje veza

Procena broja praćenih entiteta.

- Primera radi, neka su:
  - k – fiksni broj novih komunikacija po čvoru,
  - s – broj skokova.
- Tada je broj entiteta u mreži:

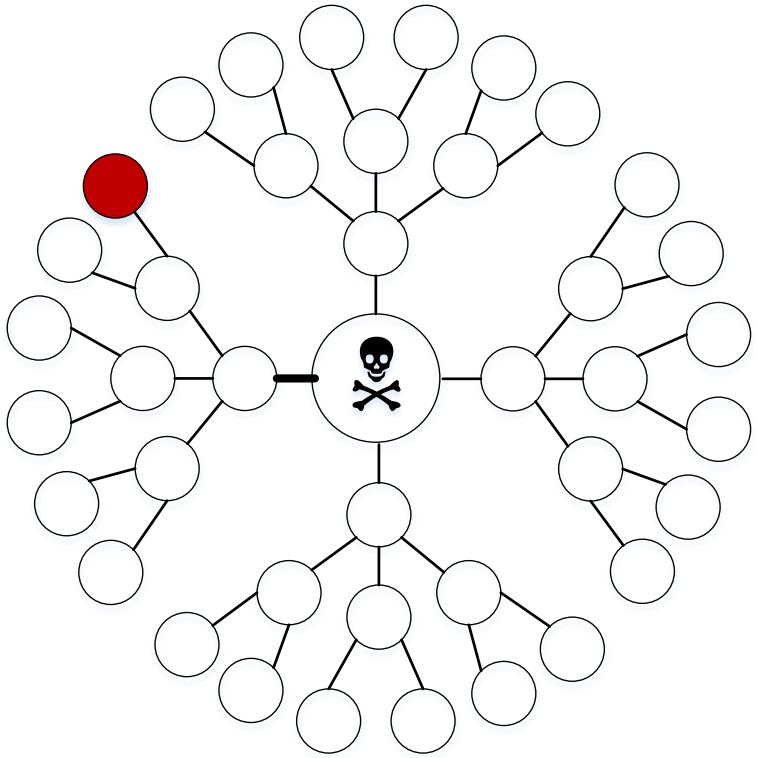
$$\frac{k^{s+1} - 1}{k - 1}$$

- U praksi:
  - NSA je samo u jednom danu 2013. aktivno pratila 117675 entiteta.
  - Kada se konzervativno procene broj kontakata koji ostvari svaka osoba (≈40) i broj preklapanja njihovih konverzacija, procenjuje se da je broj nadziranih ljudi, samo u ovom sistemu, bio veći od 20 miliona.

Mapiranje veza

Da li ste uključeni i vi?

- Koja je šansa da ste ovo vi?



Mapiranje veza

Uvid u istraživanje.

- Empirijsko istraživanje*:
  - nekoliko stotina dobrovoljnih subjekata,
  - uslov je da imaju pametni telefon sa operativnim sistemom Android,
  - subjekti nisu direktno povezani – samo dva subjekta su bila u direktnom telefonskom kontaktu,
  - metapodaci o njihovim „telefonskim“ aktivnostima su sakupljani tokom kraćeg vremenskog perioda.
- Očekivanje je bilo da graf koji povezuje kontakte između subjekata nije povezan.

* Detalji o istraživanju dostupni su na adresi https://jonathanmayer.org.

Mapiranje veza

Međutim …

- Preko 90% subjekata se našlo u istoj komponenti grafa (tj., bili su povezani).
- Preko 10% subjekata je bilo udaljeno samo dva skoka.
- Preko 65% subjekata je bilo udaljeno ne više od četiti skoka.
- Pitanje:
  - Koji je razlog za visok stepen povezanosti subjekata?

Mapiranje veza

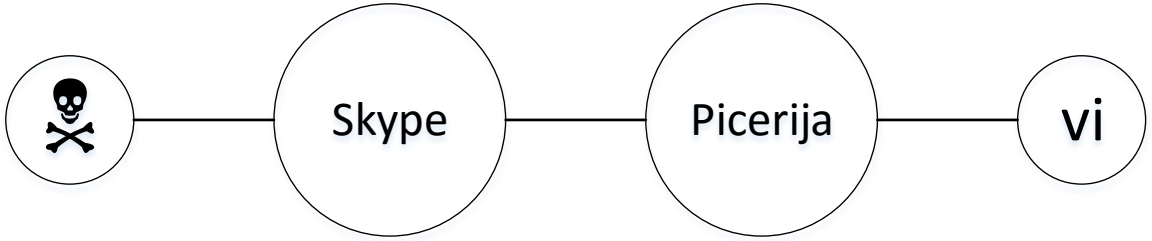
Objašnjenje.

- Da bi učesnici A i B bili povezani, dovoljno je da ostvare kontakt sa istim brojem (koji ne mora da pripada nekom od učesnika u istraživanju):
  - govorna pošta telekomunikacione kompanije,
  - Skype poziv,
  - telefonska autentifikacija Google naloga,
  - reklamna agencija,
  - agencija za istraživanje javnog mnjenja,
  - picerija,
  - …

Mapiranje veza

Objašnjenje.

- Na primer, zamislite sledeću situaciju:
  - ☠ je dobio Skype poziv,
  - drugi korisnik Skype-a je pozvao piceriju,
  - vi ste pozvali piceriju.
- ☠ i vi ste povezani.



Mapiranje veza

Obrasci ponašanja.

- Povezivanje entiteta koji se prate se ne vrši samo na osnovu telefonske komunikacije, već i na osnovu lokacije entiteta, obrazaca ponašanja itd.
  - Setite se da metapodaci uključuju i lokaciju učesnika u komunikaciji itd.
- Neki primeri iz prakse NSA …

Mapiranje veza

Obrasci ponašanja od interesa za praćenje.

- Osobe A i B se jednog dana nalaze u istom restoranu, nedelju dana kasnije u istom kafiću, a mesec dana kasnije na aerodromu.
  - A s povezuje sa B iako nisu elektronski komunicirali.
- Telefon je uključen, korišćen kraće vreme, a zatim isključen i više nikad nije korišćen.
- Grupa ljudi se nalazi na istoj lokaciji i isključuje svoje telefone, a nakon nekog vremena ih uključuje.
  - Drugim rečima, tajni sastanak.

Identifikacija vlasnika broja

Metapodaci = identifikacija.

- Koliko je teško identifikovati vlasnika broja na osnovu metapodataka?
- Ispostavlja se – sasvim jednostavno.

Identifikacija vlasnika broja

Uvid u istraživanje.

- Epirijsko istraživanje nad datim korpusom:
- Od 5000 slučajno izabranih brojeva, na osnovu tri javno dostupna izvora – Yelp, Google Places i Facebook – identifikovano je 27,1% brojeva.
- Od 100 slučajno izabranih brojeva, koristeći Google pretragu, za manje od sat vremena su identifikovani osoba ili posao za 60 brojeva.
  - Kad su uključeni i izvori Yelp, Google Places i Facebook identifikovano je 73 broja.
  - Kad je uključen i komercijalni (i relativno jeftini) izvor Intelius, identifikovan je 91 broj.
- Ovo su rezultati koje je postiglo nekoliko akademskih istraživača sa malim budžetom.
  - Opravdano je pretpostaviti da bi profesionalne službe bile još efikasnije.

Osetljivi podaci

Metapodaci = osetljivi podaci.

- Da li telefonski metapodaci otkrivaju osetljive informacije (na primer, zdravstveno stanje i slično)?
- Odgovor je, opet, pozitivan.

Osetljivi podaci

Obrasci komunikacije.

- Subjekat A.
  - Subjekat A je kontaktirao sa
    - više neuroloških grupa,
    - specijalizovanom apotekom,
    - vrućom linijom za lek koji se koristi za multiplu sklerozu,
    - …
  - ?

Osetljivi podaci

Obrasci komunikacije.

- Subjekat A.
  - Subjekat A boluje od multiple skleroze.

Osetljivi podaci

Obrasci komunikacije.

- Subjekat B.
  - Subjekat B je
    - vodio duže razgovore sa kardiolozima u velikoj medicinskoj ustanovi,
    - primio poziv iz apoteke,
    - koristio vruću liniju za medicinske uređaje koji prate srčanu aritmiju,
    - …
  - ?

Osetljivi podaci

Obrasci komunikacije.

- Subjekat B.
  - Subjekat B je doživeo srčani udar.

Osetljivi podaci

Obrasci komunikacije.

- Subjekat C.
  - Subjekat C je
    - više puta zvao prodavnicu oružja specijalizovanu za AR (ArmaLite Rifle) poluautomatske puške, i
    - imao duži razgovor sa korisničkim servisom firme koja proizvodi AR liniju oružja.
  - ?

Osetljivi podaci

Obrasci komunikacije.

- Subjekat C.
  - Subjekat C je vlasnik poluautomatskog oružja.

Osetljivi podaci

Obrasci komunikacije.

- Subjekat D.
  - Subjekat D je u periodu od tri nedelje kontaktirao
    - radnju za prepravku kuće,
    - bravara,
    - dilera za hidroponsko uzgajanje biljaka i
    - hed šop (*head shop*).
  - ?

Osetljivi podaci

Obrasci komunikacije.

- Subjekat D.
  - Subjekat D uzgaja marihuanu u kućnim uslovima.

Osetljivi podaci

Obrasci komunikacije.

- Subjekat E.
  - Subjekat E je imao dug jutarnji razgovor sa sestrom.
    - Dva dana kasnije, ostvario je niz poziva lokalnoj organizaciji za planiranje porodice, i još dva poziva – nakon dve nedelje i mesec dana.
  - ?

Osetljivi podaci

Obrasci komunikacije.

- Subjekat E.
  - Subjekat E je imao abortus.

Osetljivi podaci

Obrasci komunikacije.

- Zaključci su izvedeni samo na osnovu telefonskih metapodataka!

Literatura

1. M. Gnjatović (2017): Radni materijal iz predmeta Upravljanje informacionom bezbednošću, Visoka škola elektrotehnike i računarstva strukovnih studija, Beograd.
2. Jenn Riley: Understanding Metadata. NISO Press. Preuzeto 25.11.2017. http://www.niso.org/publications/press/UnderstandingMetadata.pdf
3. Direktiva 2006/24/E3 Evropskog parlamenta i Veća Evropske Unije.

Hvala na pažnji

Pitanja su dobrodošla.