Pričanje, šifrovanje, privatnost i koga briga

Doni Pracner

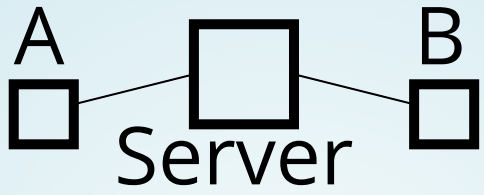
@DoniPracner | doni.pracner@dmi.uns.ac.rs

Fedora 26 Release Party, Novi Sad

Elektronska komunikacija

- Mail
- Telefonski razgovor
- SMS
- Raznorazni protokoli za trenutne poruke (tekst, glas, video, fajlovi)

Tipična komunikacija ide preko 1 ili više servera



Prisluškivanje

- na A i B kraju
- od klijenta do servera
- između raznih servera
- na samom serveru

- Kompromitovanje krajeva veze je do korisnika
- SMS je zaštićen dosta slabom šifrom
- Sigurna veza sa serverom (SSL/TLS) štiti transport na internetu
- Ostaje problem šta ostaje na serveru

- Poruke u nekoj dostupnoj formi stoje na serveru
- Poverenje u kompaniju i zaposlene
- Sudski nalozi i drugi pritisci za otkrivanje podataka
- Sigurnosni upad može pokupiti sve podatke

- Veliki broj "normalnih" programa deli ovaj problem
- Klasični mail
- Google Hangouts i XMPP uopšteno, IRC, Discord, Skype, Facebook messenger, itd

Šifrovanje od kraja do kraja

- *End to end encryption - e2e*
- Nije bitno šta ostaje gde, ako ne može da se čita

- Rašireni sistemi privatnih i javnih ključeva
- PGP i slično se koriste za mail i druge svrhe
- Problemi nameštanja ovih sistema i ključeva
- Stalno se koristi isti ključ
- OTR (Off-the-record) i OMEMO za XMPP

Signal

- Razvija ga Open Whisper Systems
- Open source i klijent i server

- iOS i Anroid klijenti
- Mogu se koristiti i za normalan SMS
- Chrome app za desktop
  - nije samostalna aplikacija, zahteva brauzer instaliran
  - donekle autonomna, nije samo proksi do telefona

- Vezuje se za broj telefona
- Privatni ključ se generiše na uređaju
- Poruke se šifruju kombinacijama ključeva pre slanja
- Protokol predviđa da se poruke mogu falsifikovati

- Imenik i kontakti su lokalni
- Za korisnika se centralno čuva broj telefona, dan registrovanja i dan poslednje konekcije
- Poruke sa rokom trajanja

WhatsApp

- U vlasništvu Facebook-a
- Koristi Signal protokol
- Mnogo više skladišti podataka o korisnicima
- Kazna zbog integrisanja podataka sa Facebookom

Telegram

- Sopstveni protokoli, zatvoreni i neprovereni
- Normalne poruke nisu e2e zaštićene
- Tvrdnja da su ključevi na serverima u drugim državama od poruka
- Čudna struktura kompanije, čudna istorija glavnih lica

Drugi popularni programi

- Viber
- Skype
- Google Allo

Jaka i neobična rešenja

- Ring
- Ricochet
- Tox
- Riot/Matrix/Vector
- Mumble/murmur

Hvala na pažnji