Cryptoparty priručnik

Cryptoparty rečnik

Model pretnje (eng. *Threat model*) je sistem ili model za određivanje nivoa potrebne sigurnosti na osnovu pretpostavljenih sposobnosti napadača.

Tekst ili poruka (eng. *Plaintext*) je nešifrovana, nezaštićena poruka ili tekst razumljiv čoveku.

Šifrat (eng. *Ciphertext*) je šifrovana poruka ili informacija nerazumljiva čoveku za koju je potreban ključ ili šifra kako bi se razumela.

OTR (eng. *Off-The-Record*) je protokol (skup pravila) za šifrovanu i verifikovanu čet komunikaciju dva korisnika.

Otisak (eng. *Fingerprint*) je kratak i jedinstveni niz karaktera matematički vezan za veći ključ za šifrovanje – obično javni ključ. Koristi se za proveru da koristite odgovarajući javni ključ osobe sa kojom šifrovano komunicirate.

Internet provajder (eng. *Internet Service Provider* – ISP) je pružaoc usluge pristupanja internetu.

Izvor: https://goo.gl/ivG521 i Vikipedija

Cryptoparty rečnik

PGP (*Pretty good privacy*) je jedan od prvih kriptografskih softvera za šifrovanje dostupan civilnim licima devedesetih godina.

OpenPGP je otvoreni protokol i standard za softver koji obavlja šifrovanje poruka.

GPG (*Gnu Privacy Guard*) je implementacija OpenPGP standarda pod *GPL* licencom od strane fondacije slobodnog softvera (*FSF*) .

Javni ključ (eng. *Public key*) je deo para asimetričnih ključeva koji neko koristi kada treba da šifruje poruku koju ćete samo vi moći da dešifrujete i odgovara vašem tajnom ključu.

Tajni ključ (eng. *Private key*) je drugi, tajni deo asimetričnog para ključeva koji ne delite sa drugima, služi da dešifrujete šifrovane poruke poslate vama, kao i za digitalno potpisivanje.

SSL *(Secure Socket Layer)* je način obezbeđivanja komunikacije između vašeg računara i veb sajta na koji se povezujete.

Izvor: **https://goo.gl/ivG521** i Vikipedija

Internet pretraživači

Fajerfoks (eng. *Firefox*) je Mozilin pretraživač otvorenog koda koji poštuje privatnost korisnika. Može se lako konfigurisati da se što bolje zaštitite dok surfujete:
https://www.privacytools.io/#about_config
Podržane platforme: Windows, Mac, Linux, Android, BSD.

firefox.org

Tor pretraživač je modifikovana verzija Mozilinog Fajerfoks pretraživača koji svu komunikaciju štiti upotrebom Tor anonimne mreže. Dolazi sa već instaliranim dodacima za povećanje privatnosti.
Otvorenog je koda, a podržane platforme su: Windows, Mac, Linux, iOS, Android, OpenBSD.

torproject.org

Brejv (eng. *Brave*) je noviji pretraživač otvorenog koda baziran na Hromijumu. Lako i automatski blokira reklame i internet kolačiće što pretraživanje čini bržim.
Podržane platforme: Windows. Mac, Linux, Android, iOS.

brave.com

Više na: https://www.privacytools.io/#browser

Operativni sistemi

Debijan (eng. *Debian*) je uniksolika linuks distribucija sačinjena samo od softvera otvorenog koda i slobodnog softvera, od kojih je većina pod GPL licencom.

debian.org

Tejls (eng. *Tails*) je lajv operativni sistem fokusiran na bezbednost i anonimnost. Za njegovo pokretanje nije potrebna instalacija, već se koristi sa USB-a, tako da ne ostavlja tragove na računaru na kojem se koristi. Sav internet saobraćaj obavlja preko Tor anonimizujuće mreže i opremljen je alatima za šifrovanje.

tails.boum.org

Kjubs (eng. *Qubes*) je operativni sistem otvorenog koda dizajniran za pružanje snažne sigurnosti za desktop računare. Karakteriše ga Zen (eng. Xen) virtuelizacija aplikacija koja smanjuje rizik od zaraze virusima celog sistema.

qubes-os.org

Više na: https://www.privacytools.io/#os

Menadžeri za šifre

Kipas (eng. *KeePass*)je besplatan menadžer šifara otvorenog koda, koji vam pomaže u upravljanju šiframa na siguran način. Sve šifre su u bazi podataka koja je zaključana jednom glavnim šifrom ili ključnim fajlom. Baza podataka je šifrovana pomoću najsigurnijih algoritama za enkripciju koji su trenutno poznati: AES i Twofish. Slični programi: KeePassX i KeePassXC. Podržane platforme: Windows, Mac, Linux, Android, iOS, BSD.

keepass.info

Master pasvord (eng. *Master password*) je program koji se zasniva na inovativnoj ideji za generisanje šifara bez njihovog čuvanja. Šifre se jedinstveno generišu određenim algoritmom, a na osnovu glavne šifre koju pamtite i imena sajta ili aplikacije za koju se prave. Nije potrebno sinhronizovanje, rezervne kopije ili pristup internetu.
Podržane platforme: Windows, Mac, Linux, Android, iOS, veb

masterpasswordapp.com

O šiframa više možete pročitati iz Libre! časopisa sa linkova:
https://pad.riseup.net/p/lozinke
Više na: https://www.privacytools.io/#pw

Šifrovani SMS i pozivi

Signal je mobilna aplikacija koja pruža šifrovano dopisivanje, kao i glasovne i video pozive. Sva komunikacija je šifrovana tako da je samo krajnji korisnici mogu dešifrovati. Signal je slobodan i otvorenog koda.
Podržane platforme: iOS, Android, Linux,Windows, Mac

signal.org

Vajr (eng. *Wire*) je aplikacija koja omogućava razmenu šifrovanih poruka između krajnjih korisnika, kao i vođenje glasovnih i video poziva. Vajr je slobodan i otvorenog koda.

Oprez: Kompanija čuva popis svih korisnika koje kontaktirate dok ne izbrišete svoj nalog.
Podržane platforme: iOS, Android, Linux, Windows, Mac, veb

get.wire.com

Više na: https://www.privacytools.io/#im

Zaštita na mreži

Tor mreža je grupa volonterskih servera koji omogućava ljudima da poboljšaju svoju privatnost i sigurnost na Internetu i zaobiđu cenzuru. Tor omogućava korisnicima da razmjenjuju informacije preko javnih mreža bez ugrožavanja njihove privatnosti.

Podržane platforme: Windows, Mac, Linux, iOS, Android, OpenBSD

torproject.org

VPN (*Virtual Private Network*) je šifrovani tunel između klijenta i VPN servera koji korisnicima omogućava da se zaštite na javnim mrežama, sakriju aktivnost od internet provajdera, zaobiđu cenzuru i sakriju svoju IP adresu od krajnjeg veb sajta kojem pristupaju.

Oprez: VPN servisi se obično naplaćuju, a VPN provajder može imati uvid u to kojim veb sajtovima ili servisima pristupate. Podržane platforme: Windows, Mac, Linux, Android.

https://www.privacytools.io/#vpn

I2P (*The Invisible Internet Project*) je sloj računarske mreže koji dozvoljava aplikacijama da pseudonimno i sigurno šalju poruke jedne drugima. Korišćenje uključuje anonimno pretraživanje veba, ćaskanje, blogovanje i prenos fajlova. Podržane platforme: Windows, Mac, Linux, Android

geti2p.net

Šifrovanje mejlova

Enigmejl (eng. *Enigmail*) je dodatak za Tanderbrd (eng. *Thunderbird*) mejl klijenta i GPG menadžer koji vam omogućava da lako šifrujete, dešifrujete, digitalno potpisujete poruke i proveravate digitalne potpise primljenih poruka. Podržane platforme Tanderbrd klijenta: Windows, Linux, Mac, BSD.

enigmail.net/index.php/en/
mozilla.org/en-US/thunderbird/

GPG tuls (eng. *GPG Tools*) je program za Mek operativni sistem (eng. *Mac OS*) i menadžer ključeva koji omogućava da lako šifrujete, dešifrujete, digitalno potpisujete poruke i proveravate digitalne potpise primljenih poruka. Radi sa preinstaliranim mejl klijentom na Mek sistemu.

gpgtools.org

APG (*Android Privacy Guard*) je OpenPGP implementacija za Android i menadžer ključeva koja omogućava šifrovanje, dešifrovanje, digitalno potrpisivanje I proveru digitalnih potpisa primljenih poruka. Radi u kombinaciji sa mejl klijentom kao što je K-9.

Više na: https://www.privacytools.io/#clients

Šifrovano dopisivanje

Čet-sekjur (eng. *ChatSecure*) je program za mobilne telefone koji šifruje dopisivanje preko interneta upotrebom XMPP protokola. Podržane platforme: Android, iOS

zom.im

Pidžin (eng. *Pidgin*) je multiplatformski klijent za dopisivanje preko interneta pomoću koga možete da se povežite na AIM, MSN, Yahoo, XMPP i druge naloge istovremeno. Nudi šifrovanje poruka između klijenta i servera, i između dva klijenta korišćenjem OTR dodatka . Podržane platforme su: Windows, Linux, Mac, BSD.

pidgin.im

Kibejs (eng. Keybase) je platorma za šifrovano dopisivanje, deljenje fajlova i služi kao registar javnih ključeva.
Podržane platforme: Windows, Linux, Mac, Android, iOS, Chromium/Firefox

keybase.io

Šifrovana video i audio komunikacija

Žici (eng. *Jitsi*) je multiplatformski program za audio i video komunikacije za koju nudi mogućnost šifrovanja upotrebom SRTP i ZRTP protokola. Podržani protokoli komunikacije su: SIP, XMPP, ICQ, AIM i drugi. Podržane platforme: Windows, Linux, Mac, Android, BSD, iOS, online.

jitsi.org

Toks (eng. *Tox*) je program za decentralizovanu šifrovanu tekstualnu, video, audio komunikaciju i prenos fajlova. Podržane platforme: Windows, Mac, Linux, Android, iOS, BSD.

tox.chat

CsipSimpl (eng. *CsipSimple*) je program za audio komunikaciju na koju se može primeniti protokol za šifrovanje SRTP.

guardianproject.info/howto/callsecurely/

Korisni linkovi:

https://www.privacytools.
https://www.eff.org/node/82654
https://prism-break.org/en/
https://ssd.eff.org/en
https://myshadow.org/
https://securityinabox.org/en/
https://freedom.press/training/
https://pack.resetthenet.org/
https://cryptoparty.rs/

Ceo spisak korisnih linkova na:

https://pad.riseup.net/p/Cryptoparty-Rijeka