Wprowadzenie do bezpiecznej komunikacji dla aktywistek i aktywistów

kolektyw sudoriot.net

www.sudoriot.net

sudo riot to niewielki wrocławski kolektyw starający się wykorzystywać technologie teleinformatyczne do walki z globalnym kapitałem.

Od 2013 roku oferujemy szereg darmowych usług i warsztatów dla grup i osób zmieniających świat na lepszy:

- warsztaty z szyfrowanej komunikacji mailowej
- linux install party
- budowa stron www
- hosting
- narzędzia do zdalnej pracy w grupie

pytajcie - przerywajcie - dopytujcie - komentujcie

- Ocena zagrożeń
- Prawo telekomunikacyjne
- Jak szpiegują nas komórki
- Bezpieczny smartfon?
- Szyfrowane komunikatory
- Kryptografia asymetryczna
- Wysyłamy zaszyfrowanego maila - Enigmail

Co nam grozi? Ocena zagrożenia

Ochrona wszystkich informacji przed wszystkimi jest niepraktyczna i wyczerpująca.

Bezieczeństwo nie sprowadza się do zainstalowanych programów i narzędzi, których się używa.

Bezpieczeństwo to proces osiągania założonych celów przy zrozumieniu związanych z nimi zagrożeń i przeciwdziałaniu tym zagrożeniom.

- Co chcemy osiągnąć?
- Co trzeba wiedzieć, aby nam przeszkodzić?
- Kto może nam przeszkodzić?
- Środki bezpieczeństwa
- Jakie ryzyko wiąże się z wydaniem poszczególnych informacji przeciwnikom?

- Co chcemy osiągnąć?
- Co trzeba wiedzieć, aby nam przeszkodzić?
- Kto może nam przeszkodzić?
- Środki bezpieczeństwa
- Jakie ryzyko wiąże się z wydaniem poszczególnych informacji przeciwnikom?

Zrobiłyśmy o tym zina: **www.zin.sudoriot.net**

Ustawa inwigilacyjna

Od 2003 roku operatorzy telekomunikacyjni **muszą** przetrzymywać i udostępniać służbom dane telekomunikacyjne (billingi, lokalizacje)

Firmy **muszą** udostępniać też dane abonenckie - nazwisko powiązane z numerem telefonu czy IP, adresy, numery konta, itd.

W 2014 roku operatorzy usług telekomunikacyjnych udostępnili takie dane **2 350 000** (!!!) razy

Odkąd ustawa inwigilacyjna ("Prawo telekomunikacyjne") weszła w życie w lutym 2016, sytuacja ma się jeszcze gorzej:

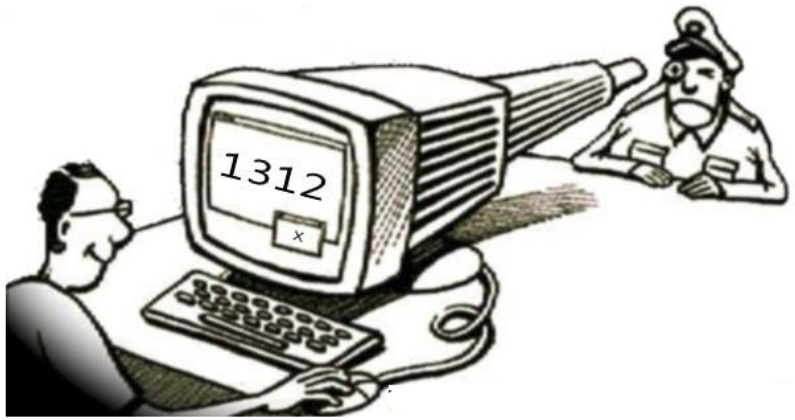
- Służby nie muszą argumentować sięgania po dane
- Nie mamy już wiedzy o skali zjawiska
- Nikła kontrola sądów nad dostępem do danych - już po fakcie
- Dodatkowo służby mają prawo do "bezpiecznych łącz"

Mało?

Służby domagają się również wydawania danych od portali i usług internetowych (np. w pierwszej połowie 2016 r. Facebook takich żądań otrzymał 991).

Jest jeszcze ustawa antyterrorystyczna - sąd nie musi wyrażać zgody na podsłuchy, kontrolę korespondecji (także e-maili), uzyskiwanie danych z "informatycznych nośników".

Służby z innych krajów też mogą nas inwigilować.



A więc...

Nie używaj polskich skrzynek mailowych, a najlepiej szyfruj całą komunikację.

Jak szpiegują nas komórki

- Informacje o tym, **kto, z kim, i kiedy** się łączył przechowywane są przez 12 miesięcy.
  Dotyczy to też SMSów i ich treści.
- Przechowywane są też informacje o **lokalizacji**, jak również numery IMEI (identyfikator telefonu) i IMSI (identyfikator karty SIM).

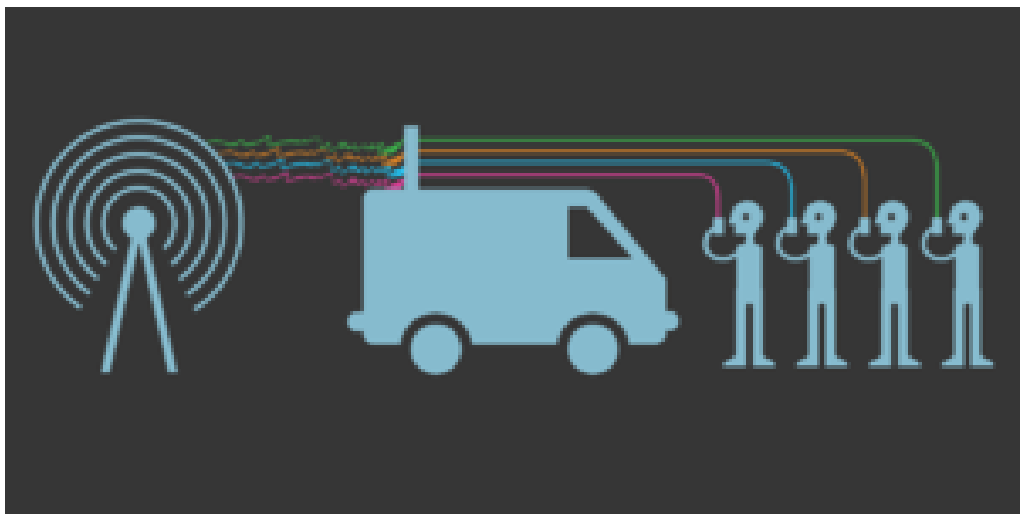
Problemy rodzi: przekładanie kart SIM, noszenie telefonów razem, sporadyczne wyłączanie lub włączanie telefonu.

Ważne: na podstawie tych danych zapadają w Polsce wyroki.

Idziesz na ważne spotkanie? Zostaw włączony telefon w domu.

Jak szpiegują nas komórki

Na podsłuch trzeba sobie zasłużyć, ale trzeba być świadomym istnienia technologii o nazwie stingray:



Telefony na akcjach

- Rozważ zostawienie go w domu
- Załóż hasło
- Zaszyfruj dane
- Albo miej osobny telefon tylko na akcje

Czy możliwy jest bezpieczny smartfon?

Mówiąc o smartfonach należy mieć w pamięci wszystko to, co powiedzieliśmy o telefonach komórkowych.

Dodatkowo smartfon to gigantyczny bank danych o tobie, który jest łatwo dostępny dla osób trzecich (dostęp fizyczny).

Jak nie musisz mieć smartfona, to go nie miej.

Smartfon - podstawy BHP

- Zrób kopię zapasową danych ze swojego smartfona (na zaszyfrowany dysk).
- Zaszyfruj dysk telefonu.

Android, czyli nie taki diabeł straszny?

Android, czyli najpopularniejszy system operacyjny na telefony komórkowe i tablety:

- ma w większości otwarty kod źródłowy,
- umożliwia zaszyfrowanie danych,
- oferuje kilka aplikacji poprawiających bezpieczeństwo użytkowników (Orbot, Briar).

Android - podstawowe problemy

- Wymuszanie na użytkownikach zalogowanie kontem Google, które zyskuje dostęp do wielu danych - ale można używać Androida bez Googla!
- Liczne aplikacje zbierają dane np. o lokalizacji, albo kontaktach. Nie zawsze wiadomo, gdzie je przekazują.

Co można zrobić?

- Włączaj GPS i Wi-Fi tylko wtedy, gdy ich używasz.
- Nie instaluj aplikacji, których nie potrzebujesz.
- Nie wyrażaj zgód na dostęp do danych aplikacjom, jeśli nie wiesz po co chcą go uzyskać.
- Spróbuj obejść się bez Google Play, używaj F-Droid.
- Spróbuj obejść się bez smartfona.

Dodatkowa kwestia: zdjęcia i video

- Nie wrzucaj zdjęć i filmów z telefonu bezpośrednio do sieci, jeśli nie musisz tego robić.
- Jeśli rejestrujesz czynności związane z ryzykiem prawnym lub fizycznym, poświęć czas na przegranie ich na komputer w celu usunięcia metadanych i anonimizację (wymazanie twarzy, itp.)
- Usuwaj wrażliwe informacje (w tym zdjęcia, filmy) z telefonu tak szybko, jak to możliwe.

Szyfrowanie end-to-end

Fig. 1a: Encryption in transit

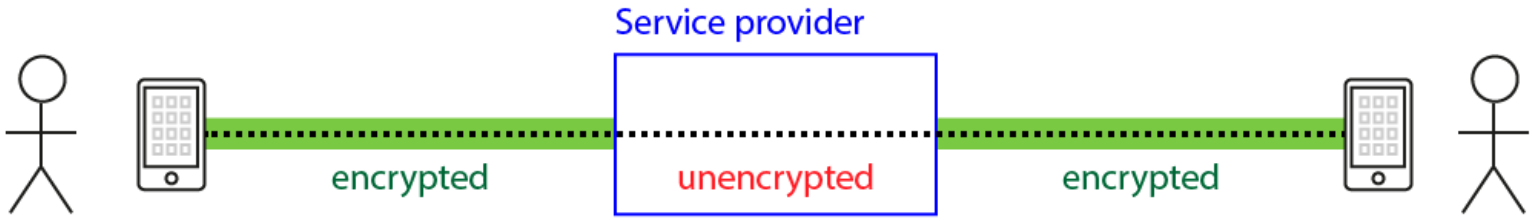


Fig. 1b: End-to-end encryption

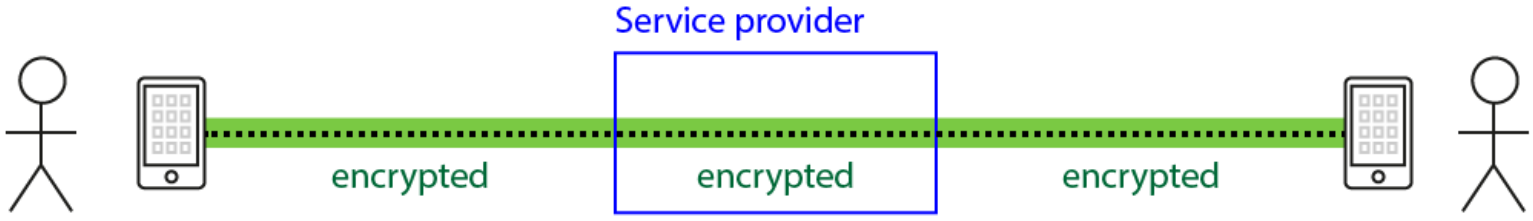
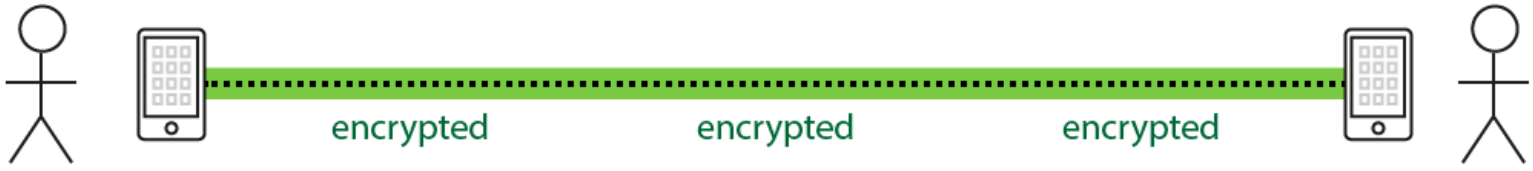


Fig. 1c: End-to-end encryption (no service provider)



Bezpieczne komunikatory: Signal

Szyfrowanie end-to-end, także plików, rozmów głosowych i video.

Bardzo popularny. Wymaga podania numeru telefonu.

Działa na Androidzie i iOS, dodatkowe programy na Linuksach, Windowsach i MacOSach.

Darmowy, ma otwarty kod źródłowy. Zdarza mu się nie działać.

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

June 15, 2018

BY ECF AND HAND

The Honorable Kimba M. Wood
United States District Judge
Southern District of New York
500 Pearl Street
New York, NY 10007

Re: *Cohen v. United States*, 18 Mag. 3161 (KMW)

Dear Judge Wood:

The Government respectfully submits this letter to update the Court as follows about the status of our production to Michael Cohen of materials seized pursuant to search warrant on April 9, 2018:

- *BlackBerries*: As previously noted, two BlackBerries were seized. On June 14, 2018, the Government produced to Cohen the contents of one of these BlackBerries; the Federal Bureau of Investigation (the "FBI") is still in the process of attempting to extract data from the second BlackBerry. While the FBI cannot, therefore, estimate the volume of data on this latter device, the BlackBerry produced yesterday contains approximately 315 megabytes of data.

- *Reconstructed Shredded Documents*: As also previously noted, the contents of a shredding machine were seized on April 9, 2018. The reconstructed documents were produced today, and are approximately 16 pages long.

- *Contents of Encrypted Messaging Applications*: The Government was advised that the FBI's original electronic extraction of data from telephones did not capture content related to encrypted messaging applications, such as WhatsApp and Signal. The FBI has now obtained this material. There are approximately 731 pages of messages, including call logs, which were also produced today.

Bezpieczne komunikatory: Briar

Wiadomości NIE SĄ w żadnej formie przetrzymywane na serwerach. Co za tym idzie - działa tylko, gdy obie osoby są online.

Działa przez Internet (Tor) i Bluetooth. Działa również bez dostępu do Internetu.

Otwarty kod źródłowy, darmowy, wyłącznie na Androida.

"as simple to use as WhatsApp, as secure as PGP, and that keeps working if somebody breaks the Internet."

BRIAR

Bezpieczne komunikatory: Tox

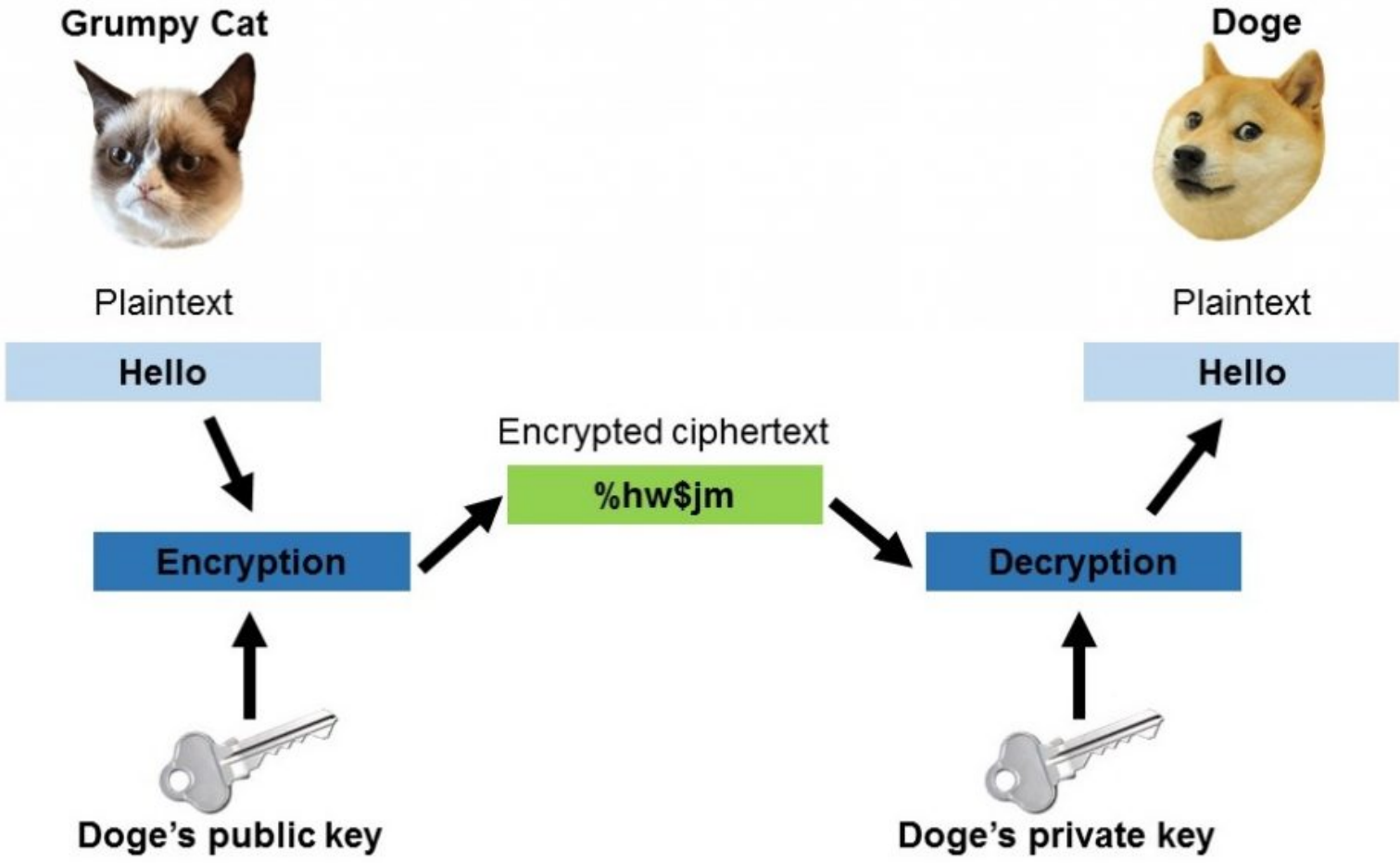
(Dokładnie rzecz ujmując, to protokół komunikacyjny, a nie komunikator)

Tak jak Briar - działa tylko, gdy użytkownicy są online.

Szyfrowanie end-to-end, także rozmów głosowych i plików.

Otwarty kod źródłowy, darmowy, programy-klienci na wszystkie systemy operacyjne - mobilne i desktopy.

Kryptografia asymetryczna?



Szyfrowanie maili w praktyce

Thunderbird - program do wysyłania i odbierania maili (klient poczty, jak Outlook)

GPG (Gnu Privacy Guard) - program szyfrujący, będący integralną częścią wielu dystrybucji Linuxa. Jest w pełni kompatybilny z Pretty Good Privacy (PGP), stąd częsty zapis GPG/PGP.

GPG może być użyte do szyfrowania danych oraz wiadomości. Obsługuje zarówno szyfrowanie symetryczne, jak i niesymetryczne.

Enigmail = GPG dla Thunderbirda. Czyli wtyczka zapewniająca prostą kryptografię asymetryczną w praktyce.

Szyfrowanie maili w praktyce

Thunderbird z Enigmailem mogą pracować także pod Windowsem i Mac OS (instalacja jest nieco bardziej skomplikowana i NIE zalecamy tych rozwiązań).

K-9 Mail i OpenKeyChain pozwalają używać GPG do maili pod Androidem (bardziej skomplikowane).

Szyfrowanie maili w praktyce

Pamiętaj: zgodnie z Polskim prawem masz prawo **bezkarnie** odmówić wydania służbom hasła bądź klucza kryptograficznego.

Podsumowując...

Bezpieczeństwo to proces - analizuj cele swoje i swojej organizacji, staraj się dopasować taktyki do zagrożeń. Znaj ryzyko związane ze swoją działalnością.

Bądź na bieżąco i edukuj swoje otoczenie.

Pamiętaj, że to szkolenie nie jest wyczerpującym źródłem informacji.

W razie wątpliwości - zrezygnuj z telefonu i komputera, przestaw się na osobiste rozmowy z dala od telefonów i komputerów.

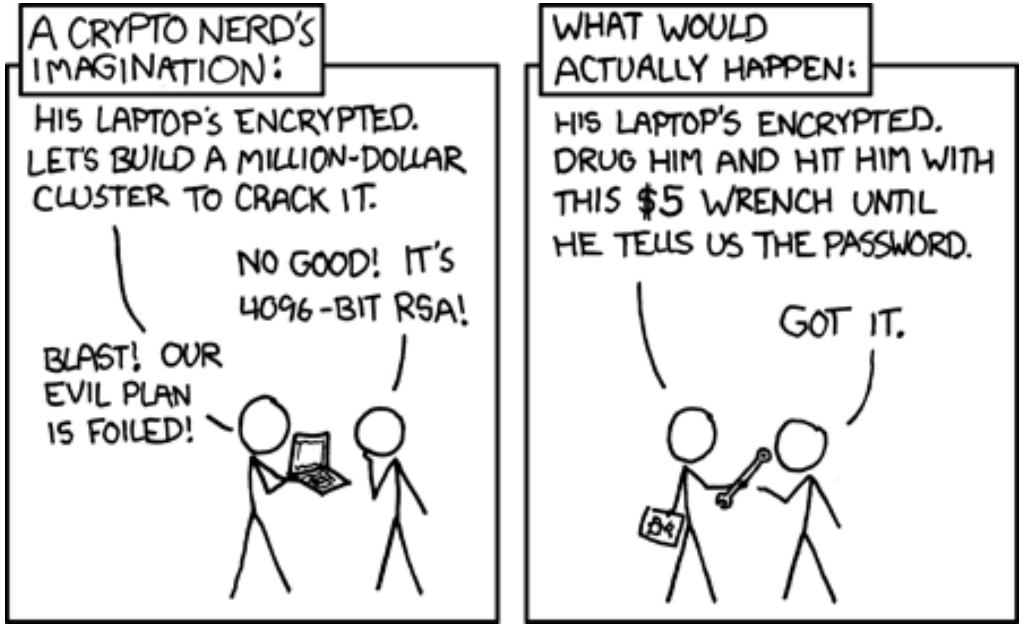
Dziękujemy za uwagę!

www.sudoriot.net
fatguy@sudoriot.net

Pilnujemy swoich haseł

Wszyscy już słyszeliśmy, że hasła...

- musimy każdorazowo wymyślać nowe do nowych kont
- muszą być długie i skomplikowane - najlepiej, żeby nie zawierały wyrazów zrozumiałych dla ludzi
- trzeba regularnie zmieniać



Pilnujemy swoich haseł

Z pomocą nadchodzi **menadżer haseł** - program, który pamięta nasze hasła za nas. Trzyma je w zaszyfrowanej postaci.

KeePassX - darmowy, otwarty kod źródłowy, działa na Linuksach, Windowsach, MacOSach.

Alternatywy (w tym na Androida): KeePass, LastPass, 1Password

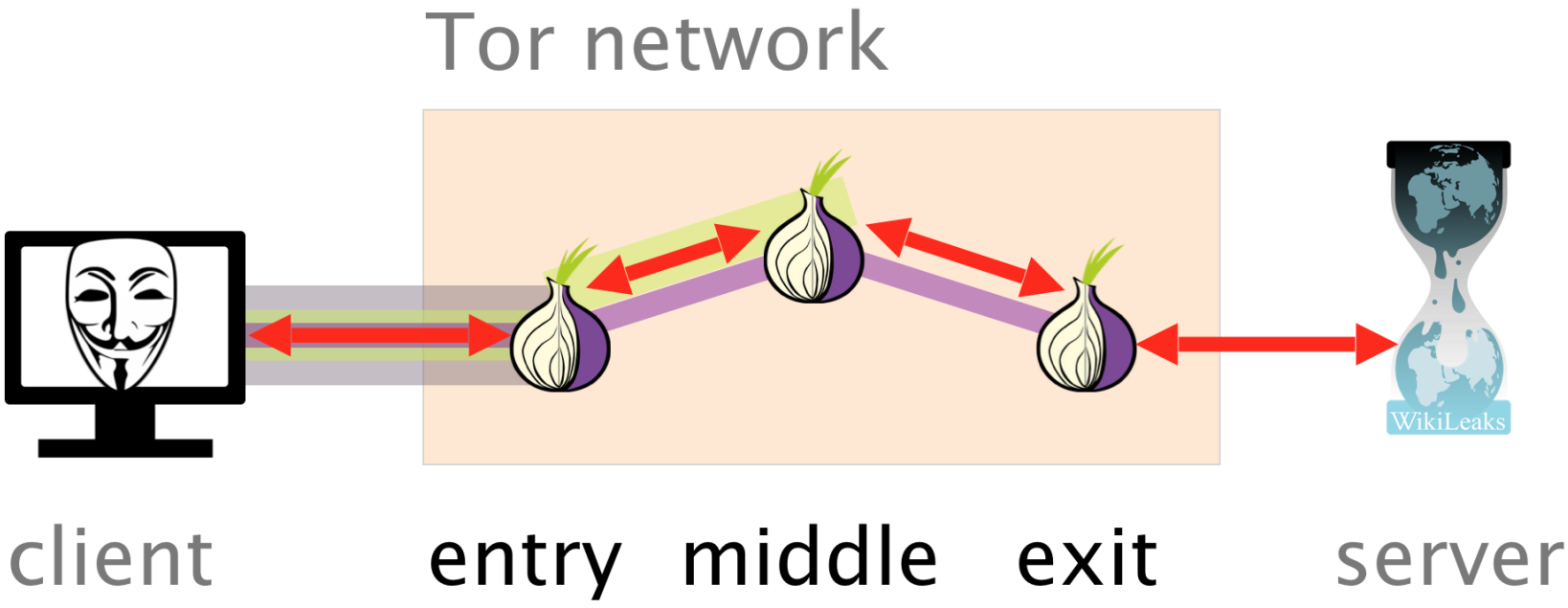
TOR - bezpieczne przeglądanie stron

Każde urządzenie podłączone do Internetu posiada adres IP. Adres IP użytkownika dostępny jest dla wszystkich operatorów serwerów w Internecie (zarządcy forów, serwisów pocztowych, blogów i stron).

Stąd:

- reklamy personalizowane pod miejsce zamieszkania
- policja u drzwi autorów wpisów na forach

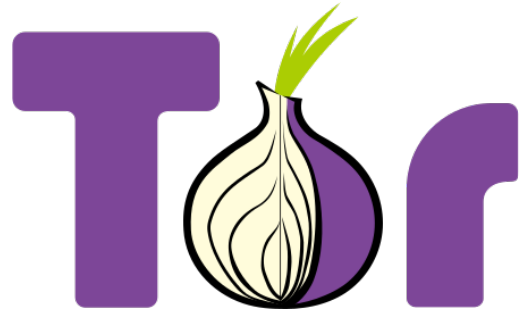
TOR - bezpieczne przeglądanie stron



TOR - bezpieczne przeglądanie stron

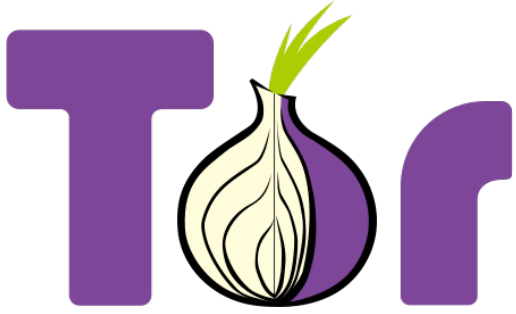
Tor spełnia trzy funkcje:

- Ukrywa adres IP użytkownika przed zarówno dostawcą usługi jak i osobami podsłuchującymi ruch.
- Szyfruje treść komunikacji (podsłuchujący wie tylko, że użytkownik używa TORa, nie wie z czym się łączy).
- Pozwala obejść cenzurę (wyświetlić treści zablokowane w danym kraju).



TOR - wady

- Nieznacznie spowalnia przesył danych.
- Google dyskryminuje użytkowników TORa (konieczność korzystania z innych wyszukiwarek np. DuckDuckGo).
- Nie nadaje się do ściągania torrentów.



TOR - czy to trudne?

Tor Browser jest dostępna na Linuxa, MacOSa, Windowsa.

Orbot + Orfox pozwalają korzystać z TORa na Androidzie.

https://www.torproject.org