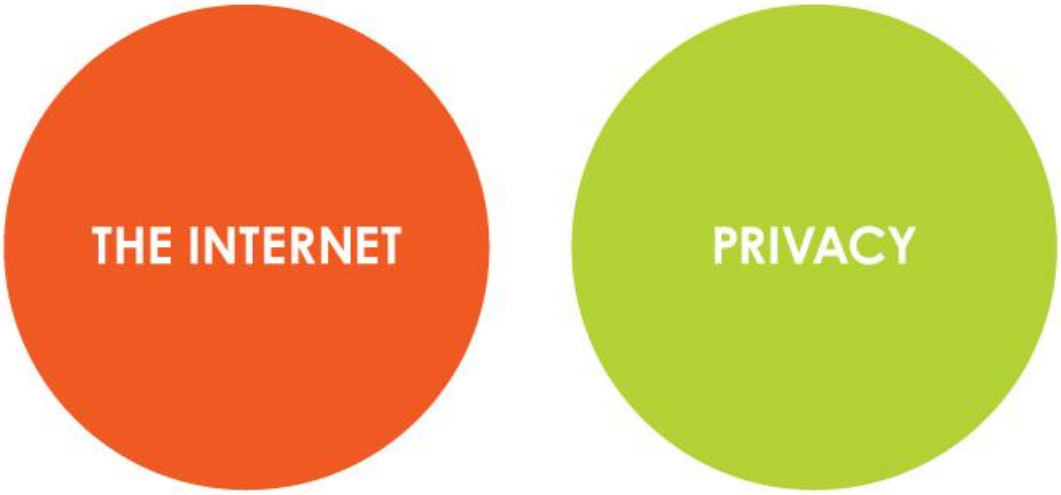
KOMUNIKACJA



A HELPFUL VENN DIAGRAM

Grzegorz Prujszczyk

Kamil Śliwowski

Październik 2010, wersja 1.0. Treść podręcznika dostępna jest na licencji:

Creative Commons – Uznanie Autorstwa – Na Tych Samych Warunkach 3.0 PL

SZKOŁA 2KLASA 2.0

CEO CENTRUM EDUKACJI OBYWATELSKIEJ

PANOPTYKON FUNDACJA

FUNDACJA nowoczesna Polska

SPIS TREŚCI

JAK DZIAŁA INTERNET

Jedną z największych zalet Internetu jest to, że nikt tak naprawdę nie jest jego właścicielem. To wiele mniejszych i większych sieci na całym świecie połączonych ze sobą na wiele różnych sposobów. Podobnie użytkownicy mają wiele różnych możliwych sposobów połączenia się z tymi sieciami. **Całość tych sieci i połączeń między nimi oraz między nimi a użytkownikami nazywamy Internetem.**

Każdy komputer (lub telefon) podłączony do Internetu jest częścią tej sieci. Na przykład, używając domowego modemu (np. Neostrady), wybiera on numer, aby połączyć się z dostawcą usług internetowych (ISP), czyli Telekomunikacją Polską. W pracy, nasze połączenie może być częścią sieci lokalnej (LAN), ale prawdopodobnie nadal łączyć się będziemy z Internetem za pomocą dużego dostawcy, z którym nasza firma zawarła umowę. Podczas łączenia się z usługodawcą internetowym, stajesz się częścią ich sieci. Korzystając z przeglądarki WWW, aby oglądać strony internetowe, korzystając z poczty e-mailowej, ściągając pliki i dzwoniąc przez skype, używasz internetu za pomocą różnych protokołów. Najczęściej jednak zauważasz jedynie fakt, że jesteś połączony lub nie i możesz używać wszystkich tych funkcji. Gdy chodzi o bezpieczeństwo, sprawa jest jednak bardziej skomplikowana. **Protokoły,** o których już wspomnieliśmy, **to metody komunikacji między różnymi sieciami, które działają i są zabezpieczone w różny sposób**. Dlatego tak ważne jest, aby rozumieć podstawy działania każdego z nich.

Dla lepszego zrozumienia kwestii bezpieczeństwa dobrze nauczyć się myśleć osobno o połączeniu z siecią, a osobno o aktywnym korzystaniu z niej. Jak sama nazwa wskazuje, najpopularniejszy sposób w jaki Interent jest dostarczany do naszych domów, „stałe łącze", to połączenie działające 24 godziny na dobę. Nasz komputer jest podłączony do sieci niezależnie czy właśnie korzystamy z przeglądarki, czy nie. Nawet gdy nic na nim nie robimy, wiele procesów działa w tle: ściągają się aktualizacje systemu, włączony Skype czuwa, czekając na czyjś telefon itp. To bardzo pozorny spokój, jeśli nie zadbamy odpowiednio o bezpieczeństwo tych elementów, nasz komputer (i my) może być zagrożony wieloma cyber-niebezpieczeństwami.

Trochę techniki...

Po podłączeniu dowolnego urządzenia do Internetu – komputera czy telefonu zostaje przypisany mu **numer IP (in. adres IP)**. Jest to numer nadawany pojedynczemu urządzeniu bądź całej sieci komputerowej opartej na protokole IP. Adres IP służy identyfikacji elementów w obrębie sieci oraz

poza nią, jest to tzw. adres publiczny. Podobnie jak adres pocztowy, IP jednoznacznie identyfikuje pojedynczy komputer w Internecie. W zależności od dostawcy usług internetowych, komputer może mieć przypisane różne adresy IP w różnych momentach łączenia się z siecią. Wszystkie witryny sieci Web i serwery sieci Web również posiadają adresy IP.

Korzystanie z sieci World Wide Web (popularne „przeglądanie" internetu) jest jednym z wielu sposobów komunikowania się za pomocą Internetu. Wiedza o tym jak działa sieć i jak się po niej poruszać to podstawa przedmiotu Technologie Informacyjno-Komunikacyjne, to również szansa dla Ciebie, byś rozwinął swoje umiejętności i przekazał je rówieśnikom, nauczycielom i rodzicom. Korzystając z tego podręcznika, masz szansę pokazać im, że „ogarniasz" sieć znacznie szerzej. Zapewne nie korzystają oni z najnowszych narzędzi zwiększających bezpieczeństwo w sieci. Możesz im pomóc oraz samemu wiele się nauczyć.

SŁOWNICZEK

Internet Protocol (IP) i Adres IP - *IP to protokół komunikacyjny używany powszechnie w Internecie i sieciach lokalnych. Dane w sieciach IP są wysyłane w formie bloków określanych mianem pakietów.*
Adres zaś to liczba nadawana każdemu urządzeniu lub grupie urządzeń połączonych w jednej sieci. Adres IP nie identyfikuje jednoznacznie urządzenia, może być zmienny, np. z każdym nowym połączeniem z siecią, jeden adres może również dzielić kilka urządzeń.

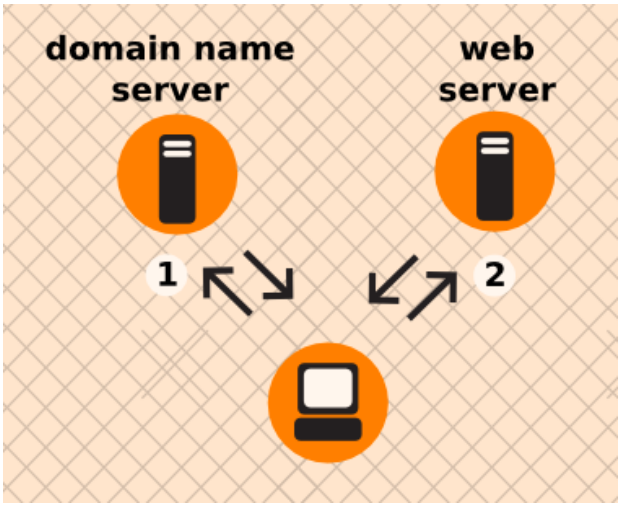
Jeśli chcesz odwiedzić konkretną witrynę sieci Web, zazwyczaj wpisujesz nazwę witryny sieci Web (adres URL) w przeglądarce, a nie adres IP. Po wpisaniu nazwy domeny w przeglądarce, komputer wysyła komunikat o tej nazwie w Domain Name System (DNS). System składa się z dedykowanych komputerów w Internecie, tłumaczących nazwy na adresy IP. DNS umożliwia nam konieczność znania tylko nazw witryn, a nie skomplikowanych ciągów liczbowych.

SŁOWNICZEK

URL ang. "**uniform resource locators**", *to adresy stron internetowych lub plików, np. http://www.wolnelektury.pl/ – adres Szkolnej Biblioteki Internetowej, http://www.wolnelektury.pl/media/lektura/cos-ty-atenom-zrobil-sokratesie.mp3 – adres pliku MP3 z nagraniem wiersza.*
Adresem URL mogą być adresy stron (adres WWW), adresy plików w protokole FTP, lokalne adresy plików na naszym komputerze (czyli adresy ich umiejscowienia na dysku).

Teraz komputer może spróbować skontaktować się z witryną sieci Web przy użyciu jej adresu IP. Ścieżka z komputera do docelowej witryny sieci może przebiegać przez wiele krajów i przez wiele komputerów. **Zadanie kierowania wiadomości do witryny sieci Web (i z powrotem) jest wykonywane przez routery, a proces ten jest znany jako routing**. Router, jaki posiadamy w domu, to tylko pierwsze
ogniwo skomplikowanego łańcucha.

Dla naszych celów, warto zauważyć, że routerom można podać różne instrukcje, jak mają się zachowywać podczas komunikacji. Każdym routerem można manipulować do kopiowania, przekierowania lub blokowania dostępu do niektórych witryn sieci Web. Najprostszym ograniczeniem, jakie można spotkać, np. w kawiarniach lub innych miejscach posiadających publicznie dostępne wi-fi, jest ograniczenie prędkości połączenia lub blokowanie niektórych protokołów, np. takich, które służą do pobierania plików z sieci. Najgłośniejszym przykładem takiej formy cenzury była sprawa Comcast – dostawcy internetowego w Stanach Zjednoczonych. Comcastowi udowodniono przed Federalną Komisją ds. Komunikacji (ang. FCC, polskim odpowiednikiem tego urzędu jest UKE, czyli Urząd Komunikacji Elektronicznej), że blokował swoim użytkownikom połączenia za pomocą protokołu P2P (będzie o nim mowa dalej).



Rys.1 Ilustracja procesu komunikacji komputera z serwerem DNS. Serwer DNS tłumaczy zapytanie na adres konkretnej strony, którą chcemy odwiedzić. Komputer komunikuje się z serwerem DNS (1) otrzymuje informację o adresie strony, której szukamy, i komunikuje się z jej serwerem (2), aby ją wyświetlić.

CZYM JEST SIEĆ WWW?

W3 wyraża ideę nie podlegającego fizycznym ograniczeniom świata informacji, połączonego za pomocą łączy hipertekstowych w celu łatwego dostępu do różnych zasobów i miejsc w sieci.

Hipertekst to organizacja danych połączonych hiperłączami (linkami) w sposób nielinearny i bez określonej struktury. Hipertekstem jest sieć WWW, w ramach której różne strony, adresy, zasoby są połączone wzajemnie łączami.

Uniform Resource Identifier (**URI**, tłum. unikalny identyfikator zasobu), koncepcja systemu adresowania wdrożona, by umożliwić połączenia sieci, pomimo wielu różnych protokołów.

Hypertext Transfer Protocol (**HTTP**), protokół sieciowy używany do przesyłania stron internetowych, jego bezpieczniejszą odmianą jest **HTTPS**.

HyperText Markup Language (**HTML**), hipertekstowy język znaczników, zrozumiały przez każdą przeglądarkę WWW, służący formatowaniu tekstu, menu oraz pozostałej zawartości strony.

KOMUNIKACJA

Cała komunikacja w sieci przechodząca przez europejskie serwery musi być przetrzymywana przez okres od 6 do 24 miesięcy, aby służby specjalne czy policja miały swobodny dostęp do danych. 15 marca 2006 weszła w życie *Dyrektywa unijna 2006/24/EC* dotycząca retencji danych generowanych lub przetwarzanych podczas połączeń z publicznie dostępnych serwisów komunikacji. Dyrektywa ta wymaga od wszystkich dostawców internetowych (ISP – Internet Service Provider) takich jak TP S.A. oraz operatorów teleinformatycznych, np. Polkomtel, przetrzymywanie (na ich koszt) zapisu całej komunikacji w zakresie mającym umożliwiać m.in. śledzenie źródeł i celu komunikacji, dat i czasu trwania, rodzaju połączenia, rodzaju urządzeń i miejsc, z których nawiązywana jest komunikacja.

Oznacza to, że służby, opierając się na nie zawsze kontrolowanych procedurach, są w stanie uzyskać dostęp do większości korespondencji prowadzonej przez daną osobę przez okres 2 lat od wysłania maila czy wiadomości. Dotyczy to też komunikacji, która została „skasowana" z serwerów. Co najważniejsze, dla przeciętnego użytkownika oznacza to, że każda firma komunikacyjna trzyma treść ich komunikacji, starając się to robić możliwie najtaniej, co z pewnością nie gwarantuje wysokiego poziomu bezpieczeństwa przetrzymywanych treści.

ZAGROŻENIA:

- dane gromadzone dla rządu mogą być wykorzystane w szkodliwych celach przez sam rząd;
- gromadzone dane mogą wpaść w ręce osób niepowołanych – nieuczciwych pracowników, złodziei danych itd.

OCHRONA:

- szyfrowanie komunikacji

E-MAIL

O komunikacji mailowej w żaden sposób nieszyfrowanej najlepiej myśleć jak o pocztówce. Nasz mail jest dostępny dla każdego na drodze z naszego komputera do odbiorcy, dlatego przypomina pocztówkę, którą przeczytać może każdy pracownik poczty, listonosz i wszyscy, z którymi mieszkamy. Dotyczy to tak adresu naszego i odbiorcy, jak i całej treści. Maile zawierają też zawsze adres serwera, z którego wyszły, a zależnie od jego konfiguracji nierzadko także nasze

własne IP. Niektórzy dostawcy poczty gromadzą te dane na własny użytek, np. usługa pocztowa Google (Gmail) zapisuje za każdym razem, gdy wysyłamy z niej maila, nie tylko nasze IP (i co za tym idzie przybliżone położenie), ale też wszelkie dostępne dane osób, z którymi korespondujemy.

ZAGROŻENIA:

- treść dostępna dla wszystkich;
- widoczne dane adresowe niekoniecznie są prawdziwe.

OCHRONA:

- w razie wątpliwości sprawdzamy nagłówki listu;
- potwierdzenie istotnych próśb lub informacji.

SŁOWNICZEK

E-mail spoofing *(fałszerstwo, naciąganie) – przede wszystkim fałszem może być opis nadawcy (co dowolna osoba może zrobić w konfiguracji programu lub usługi poczty), fałszywy może być prezentowany nam email nadawcy (pole „from:") i w końcu fałszywa może być treść stylizowana np. na serwis, bank czy sklep, którego używamy (bądź też nie). E-mail spoofing jest najczęściej wykorzystywany do rozsyłania spamu oraz przy próbach wyłudzenia poufnych danych (np. danych dostępowych do kont bankowości elektronicznej –* ***phishing****).*

LISTY MAILINGOWE

Listy mailingowe to obecnie rzadziej wykorzystywany, lecz dalej popularny w niektórych instytucjach, organizacjach i innych grupach sposób komunikacji. Podstawą działania listy mailingowej jest rozsyłanie emaila wysłanego pod konkretny adres do wszystkich zapisanych na nią osób (subskrybentów).

Listy zależnie od konfiguracji mogą mieć publiczne (otwarte na sieć i wyszukiwarki) archiwa, prezentujące każdego wysłanego na nie maila i adresy nadawców. Nawet jeżeli archiwum jest dostępne tylko dla subskrybentów, dalej warto sprawdzić, czy na listę może zapisać się każdy, czy konieczne jest zatwierdzenie przez moderatora. Jeżeli każdy może się zapisać, to choć treść listy nie będzie dostępna w wyszukiwarkach, dalej mogą do niej dotrzeć osoby trzecie. Korzystając z komercyjnych serwerów list, warto sprawdzić, czy jesteśmy w stanie kontrolować ustawienia listy

oraz czy serwis nie uzurpuje sobie prawa własności do naszej komunikacji – może się okazać, że nie będziemy w stanie usunąć informacji wysłanych na listę lub zostaną one upublicznione bez naszej zgody.

ZAGROŻENIA:

- upublicznienie mniej lub bardziej prywatnej komunikacji i informacji.

OCHRONA:

- świadomość poziomu publicznej dostępności informacji;
- branie pod uwagę możliwości upublicznienia wszelkich wysyłanych przez nas danych;
- upewnienie się, jakie są warunki wykorzystywanej usługi.

KOMUNIKATORY I POCZTA

Komunikatory takie jak Skype, GaduGadu czy Gmail chat wykorzystują różne sposoby przesyłania wiadomości tekstowych, głosowych czy video. Format przesyłanych danych i sposób, w jaki są przesyłane, nazywamy **protokołem**. Protokoły różnią się między sobą w wielu rzeczach, jednak ostatecznie wszystkie mają wspólny cel: dostarczenie wiadomości do osoby, z którą rozmawiamy.

Sam sposób działania niektórych protokołów zapewnia im zwiększone bezpieczeństwo (np. architektura P2P skype). Niektóre domyślnie wykorzystują szyfrowanie SSL, jak np. Gmail chat, inne jak GaduGadu nie zabezpieczają komunikacji w żaden sposób.

Konfigurując połączenie programu pocztowego z pocztą lub logując się na stronę poczty i przy jej czytaniu, najlepiej zabezpieczyć całość komunikacji przy użyciu szyfrowania SSL. Ten typ zabezpieczenia oznacza, że szyfrowane jest połączenie z naszego komputera do serwera poczty, ale już nie pomiędzy serwerami poczty.

SSL na poczcie

Kiedy wchodzimy na stronę poczty, standardem jest opcja „bezpiecznego logowania", która w praktyce przekierowuje nas na stronę zabezpieczoną SSL. To ważne, inaczej posyłamy przez sieć nasze hasło otwartym tekstem, umożliwiając innym jego przechwycenie.

SŁOWNICZEK

Protokoły komunikacyjne *to reguły postępowania programów komputerowych w komunikacji między sobą, które są automatycznie wykonywane przez urządzenia komunikacyjne podczas łączności i wymiany danych. Przykładem protokołu jest DNS (System Nazw Domen) lub XMPP działający w wielu komunikatorach internetowych.*

Na potrzeby tego tekstu **komunikatory** podzielimy na 3 grupy:

1. obsługujące „standardowe" programy i protokoły;
2. Skype;
3. komunikatory działające w przeglądarce.

Do pierwszej grupy zaliczymy programy **Gadu-Gadu** i **tlen.pl**. Oba są programami, które możemy zainstalować na komputerze, różnią się jednak możliwościami; poza opcjami VoIP (rozmów głosowych przez internet) i powiązanymi z komunikatorami usługami i serwisami podstawę dalej

stanowi komunikacja tekstowa. Gadu-Gadu używa tylko własnego protokołu, tlen pozwala na komunikację z wykorzystaniem protokołu Gadu-Gadu (i co za tym idzie komunikację z użytkownikami programu Gadu-Gadu) i własnego serwera protokołu jabber, który określa się jako własną sieć tlen.pl, ale umożliwiającego komunikację ze wszystkimi użytkownikami jabbera.

Komunikatory różnią się pod względem bezpieczeństwa i możliwości jego rozszerzania. W najnowszej wersji Gadu-Gadu wprowadzono możliwość szyfrowania SSL. Zmniejsza to ryzyko, że ktoś nas „podsłucha", ale nie oznacza wcale, że nasza komunikacja nie jest czytelna dla firmy obsługującej Gadu-Gadu (SSL zapewnia tylko szyfrowanie między nami a ich serwerem). Inny, bezpieczniejszy model wykorzystuje komunikator tlen (dla połączeń „swoim" protokołem), szyfrując całą komunikację pomiędzy użytkownikami, a nie tylko między użytkownikiem a serwerem.

SŁOWNICZEK

***VoIP** (ang. Voice over Internet Protocol) – technologia umożliwiająca przesyłanie mowy lub mowy i przekazu wideo za pomocą łączy internetowych lub dedykowanych sieci wykorzystujących protokół IP. Dane przesyłane są za pomocą protokołu IP. Jedną z najpopularniejszych usług opartych o tę technologię jest telefonia internetowa Skype.*

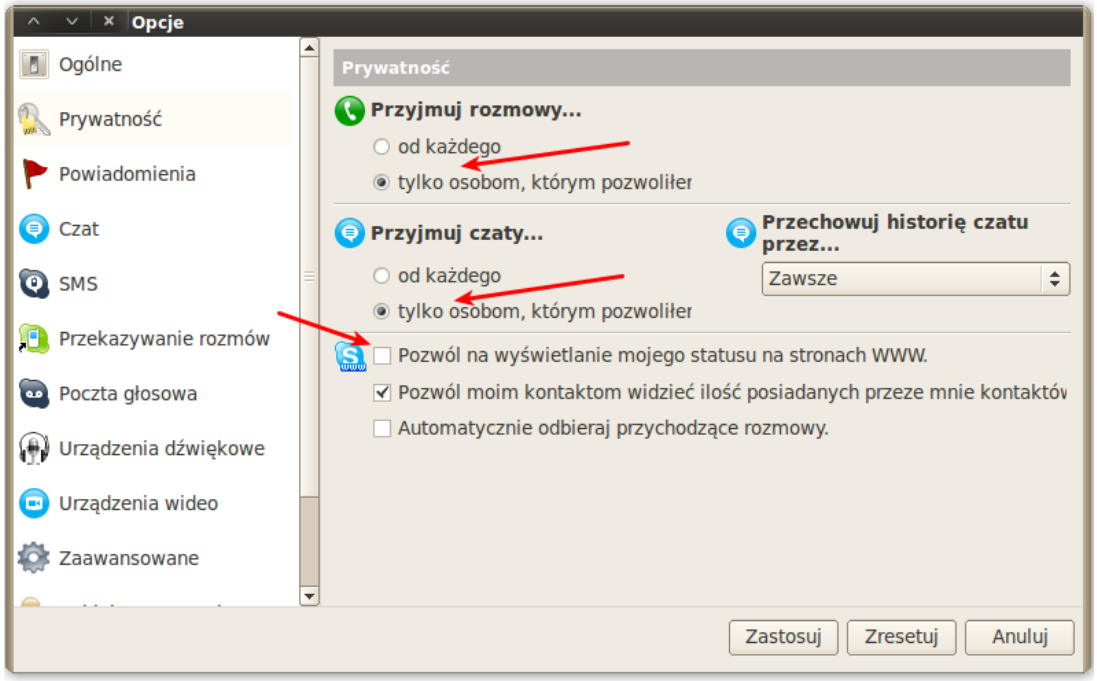
Popularny komunikator **Skype** to dość szczególny przypadek. Skype jest oparty na strukturze **peer2peer**, co oznacza, że całość komunikacji nie przepływa przez centralne serwery, tylko przez komputery innych użytkowników,w związku z czym od początku cała komunikacja jest też szyfrowana pomiędzy końcowymi użytkownikami. Według ostatnich badań nie jest to mocny szyfr, jednak ciężko ustalić trasę, jaką prowadzona będzie komunikacja, co znacznie zwiększa bezpieczeństwo przesyłanych informacji.

Ostatnią grupą są komunikatory, których używamy przeważnie przez strony takie, jak **gmail chat** na stronie poczty Gmail, **facebook chat** na facebooku i **nktalk** na Naszej klasie. Poziom ich bezpieczeństwa zależy od bezpieczeństwa naszego połączenia z serwisem: gmail wymusza połączenie SSL, w facebooku jest to opcjonalne, a nasza klasa pozwala na połączenie SSL tylko przy logowaniu. Tak więc każda osoba w sieci lokalnej mogąca mieć dostęp do naszego niezaszyfrowanego połączenia ze stroną, uzyska też połączenie do naszego 'komunikatora' na tej stronie. Niestety, łączenie za pomocą protpokołu HTTPS z Facebookiem automatycznie wyłącza chat (możemy z niego wówczas korzystać wyłącznie za pomocą zewnętrznego komunikatora, np. Pidgin).

Osobnym, wygodnym i prawdopodobnie najbezpieczniejszym rozwiązaniem jest **multikomunikator Pidgin**. Domyślnie obsługuje protokoły jabber i gadu-gadu oraz wiele innych protokołów, w tym popularne na świecie ICQ, msn i yahoo, przez wtyczki może obsługiwać też kolejne w tym skype, facebook i gmail chat. Może on wykorzystywać wbudowane zabezpieczenia protokołu i połączenia (SSL lub szyfrowanie, które jest częścią protokołu), ale dzięki systemowi wtyczek pozwala na dodatkowe zwiększenie bezpieczeństwa, np. wtyczką OTR, którą opiszemy dalej.

SŁOWNICZEK

Extensible Messaging and Presence Protocol (XMPP) *– protokół bazujący na języku XML umożliwiający przesyłanie w czasie rzeczywistym wiadomości oraz statusów. Protokół jest stosowany w komunikatorach internetowych takich jak Jabber czy Google Talk (Gmail Chat) i in. Cechuje się otwartością standardu i wysokim bezpieczeństwem.*



Rys.2. Ustawienia prywatności w programie Skype. Po uruchomieniu programu otwórz *Opcje*, a dalej zakładkę *Prywatność*. Można tu wyłączyć możliwość komunikowania się z nami osób, których wcześniej nie zaakceptujemy, zarządzać historią naszej komunikacji oraz kontrolować nasze podstawowe informacje o koncie.

SZYFROWANIE I AUTENTYFIKACJA POCZTY

PGP to skrót od „Pretty Good Privacy" („dość dobra prywatność"), oryginalnej nazwy komercyjnego programu szyfrującego, stworzonego przez Philipa Zimmermanna. Z kolei **GPG** lub **GnuPG** (skrót od „GNU Privacy Guard", czyli„Strażnik Prywatności GNU") to otwarta, darmowa wersja. Zarówno PGP, jak i GPG działają na bazie standardu OpenPGP i współpracują ze sobą, jednak wersja komercyjna ma pewne rozszerzone funkcje przydatne firmom.

Mechanizm działania szyfrowania PGP opiera się na strukturze **kluczy publicznych i prywatnych**. Klucz publiczny danej osoby pozawala nam zaszyfrować np. e-mail do tej osoby tak, że tylko ona będzie go w stanie odszyfrować przy użyciu swojego klucza prywatnego. Jest to możliwe dzięki specyficznemu typowi równań matematycznych działających w jedną stronę. Szyfrowanie poczty działa podobnie do zabezpieczeń fizycznych. Obie strony komunikacji muszą posiadać narzędzia do bezpiecznego zamykania i otwierania swoich listów (klucze). Nikt, kto nie otrzymał od nas naszego klucza i nie został zweryfikowany, nie będzie mógł odczytać naszej korespondencji. PGP pozwala też na bezpieczne podpisanie listu. Dzięki temu osoba, która go otrzyma, będzie w stanie potwierdzić nasze autorstwo i autentyczność treści (czyli, że treść nie została zmieniona po jego podpisaniu).

Nie jest to zabezpieczenie konieczne przy codziennym użyciu Internetu, jednak zapewnia znacznie wyższy poziom bezpieczeństwa przy przesyłaniu jakichkolwiek istotnych danych czy po prostu prywatnej korespondencji. Zazwyczaj PGP instaluje się na swoim domowym komputerze/laptopie i używa tylko z niego, razem z programem poczty. Możliwe jest też użycie pendriva z oprogramowaniem i kluczem prywatnym oraz obsługa webmaila (poczty sprawdzanej przez przeglądarkę), jednak są to trudniejsze i mniej bezpieczne konfiguracje, więc ich opis na razie pominiemy.

INSTALACJA I KONFIGURACJA PGP/GPG

Na początek będziemy musieli zaopatrzyć nasz komputer w odpowiednie oprogramowanie. Dla każdego systemu można je pobrać ze stron podanych poniżej i automatycznie zainstalować.

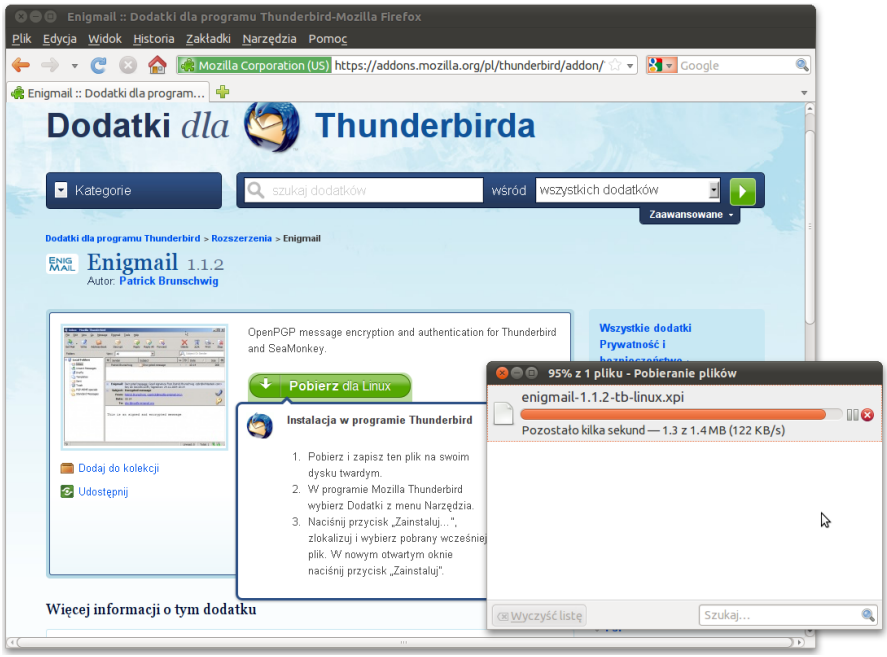
Microsoft Windows: WindowsGnuPG

http://www.gnupg.org/download/

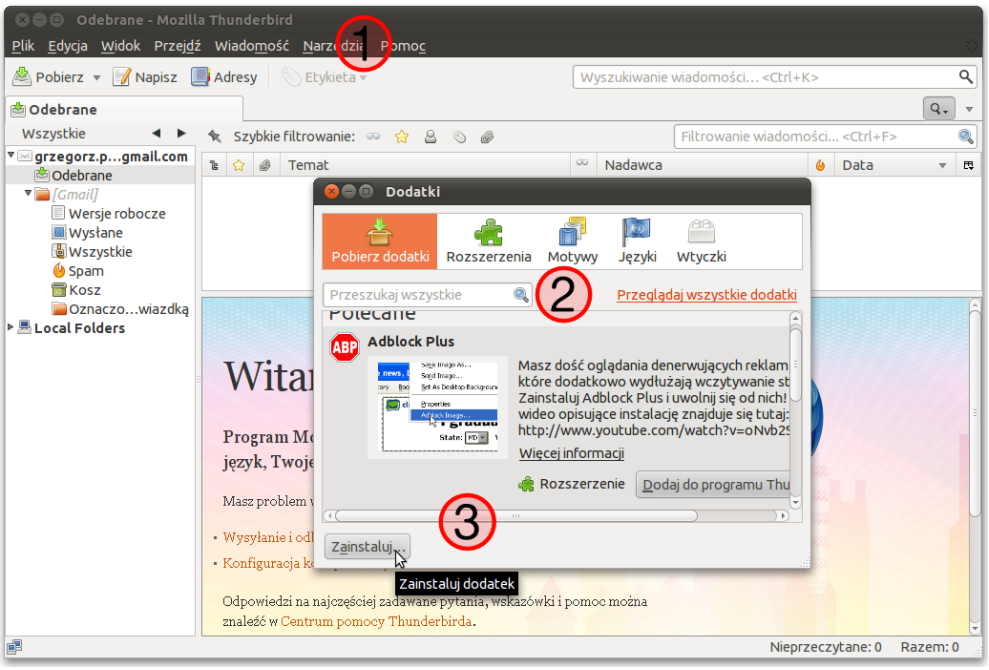
Mac OSX: Mac GNU Privacy Guard:

http://macgpg.sourceforge.net/

Linuks: Większość znanych nam dystrybucji Linuksa automatycznie instaluje PGP. W Ubuntu znajdziemy go w menu Programy→Akcesoria→Hasła i klucze szyfrujące. Zakładamy też, że GPG ma być instalowane do współpracy z programem Mozilla Thunderbird, polecanym przez nas klientem poczty. Instrukcje jego instalacji i konfiguracji można znaleźć na stronach Mozilli i w wielu innych miejscach, więc je pominiemy. Oczywiście standardu PGP można używać praktycznie ze wszystkimi klientami poczty, jednak albo wtyczki,, albo same programy mogą być płatne, a więc trudniej dostępne dla użytkowników.

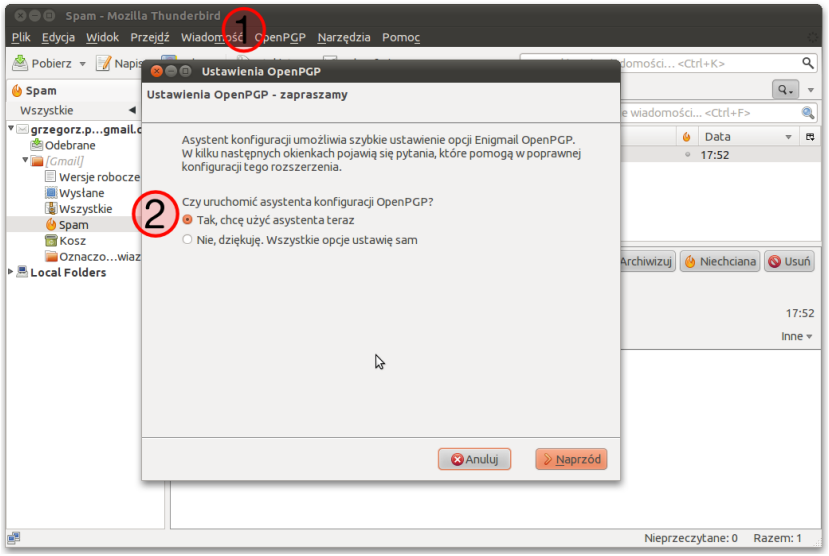


Rys.3. Dodatek Enigmail dla Thunderbirda musimy pobrać ze strony ***addons.mozilla.org****, używając przeglądarki.*



Rys.4. Instalacja dodatku Enigmail przez program Mozilla Thunderbird.

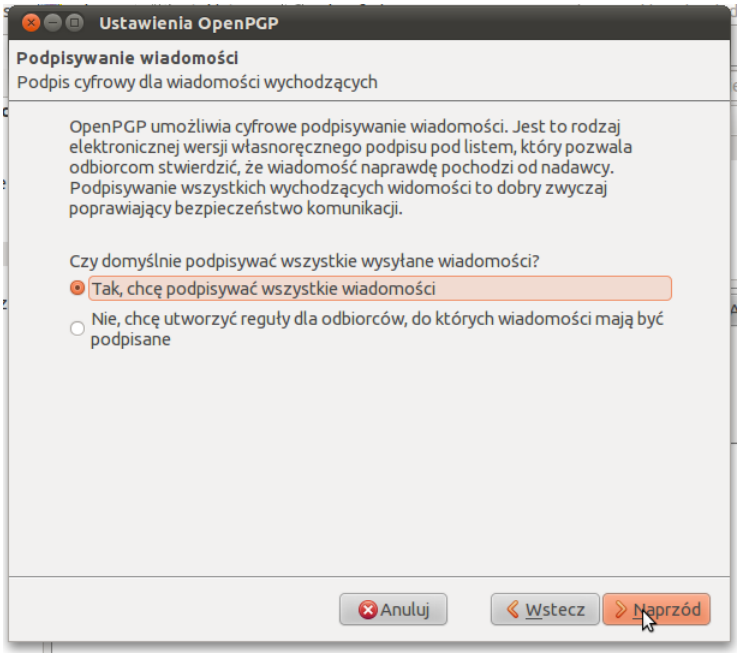
1. Wchodzimy w menu Narzędzia → Dodatki
2. Klikamy „Zainstaluj”. Następnie wybieramy wcześniej ściągnięty plik (enigmail(...).xpi), po instalacji program poprosi nas o ponowne uruchomienie.



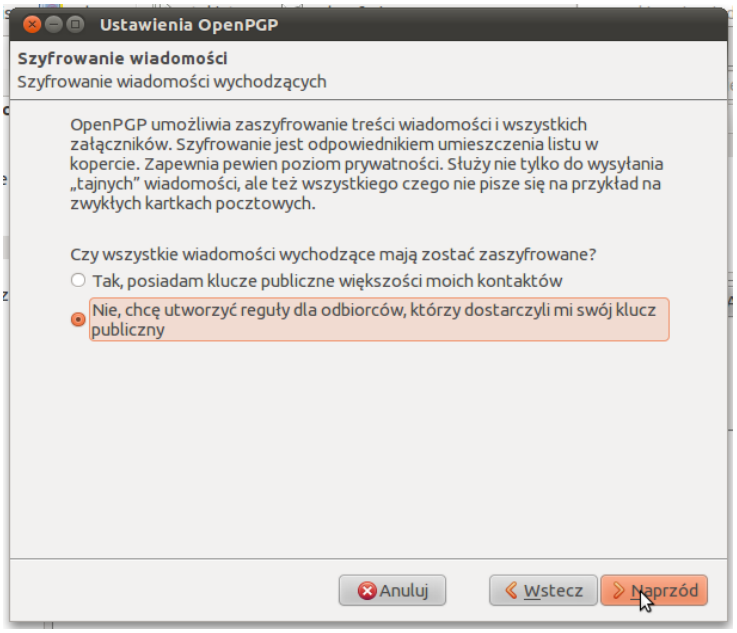
Rys.5. Rozpoczęcie konfiguracji OpenPGP (dzięki dodatkowi Enigmail) w Mozilla Thunderbird.

1. W pasku menu programu pojawi się dodatkowa zakładka *OpenPGP*. Wchodzimy w nią, a następnie w *Ustawienia*.

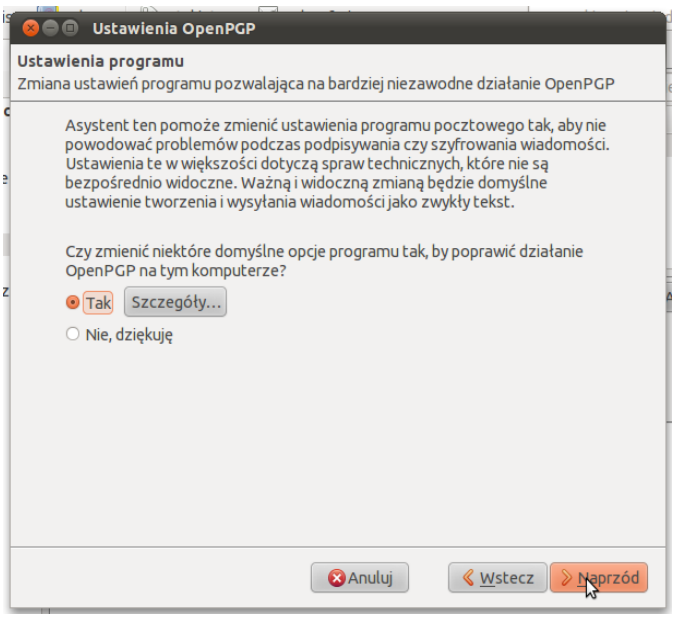
2. Rozpoczynamy od zgody na pomoc Asystenta konfiguracji (lub jeśli jesteśmy zaawansowanym użytkownikiem potrafiącym skonfigurować program samodzielnie wybieramy opcję konfiguracji manualnej).



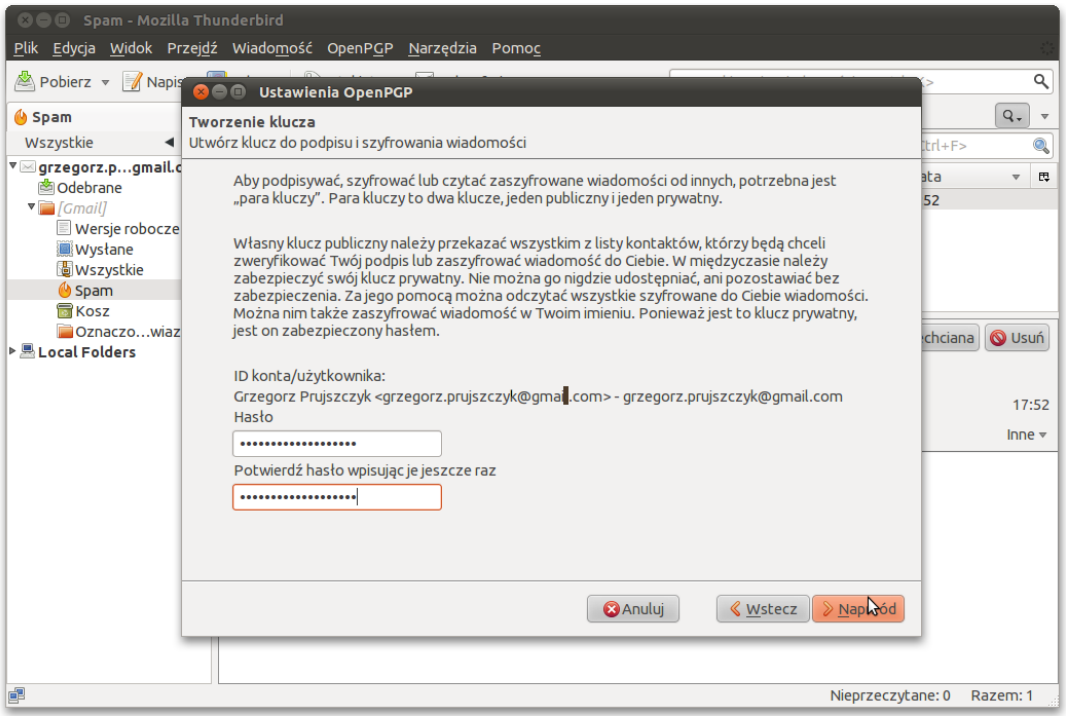
Rys.6. Kolejny krok – wybieramy opcję podpisywania wszystkich wiadomości. Dołączy to mały plik z podpisem do naszej korespondencji, przy okazji informując innych, że używamy PGP i umożliwiając im potwierdzenie autorstwa.



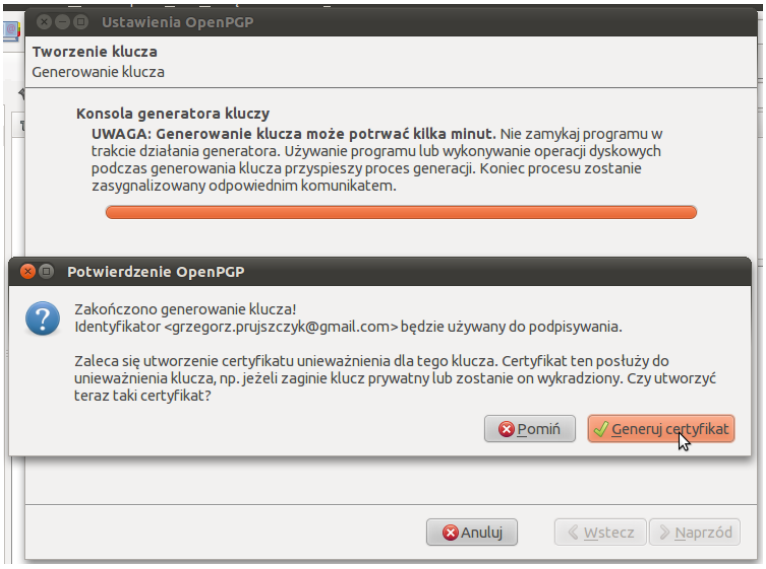
Rys.7. Opcja szyfrowania wiadomości. Zależnie od tego czy posiadamy klucze wszystkich naszych kontaktów czy chcemy utworzyć reguły dla wybranych, odznaczamy stosowną opcję. W przypadku naszej instrukcji prezentujemy opcję dla wybranych użytkowników, przeważnie większość osób nie używa PGP, więc nie będziemy mieli ich kluczy.



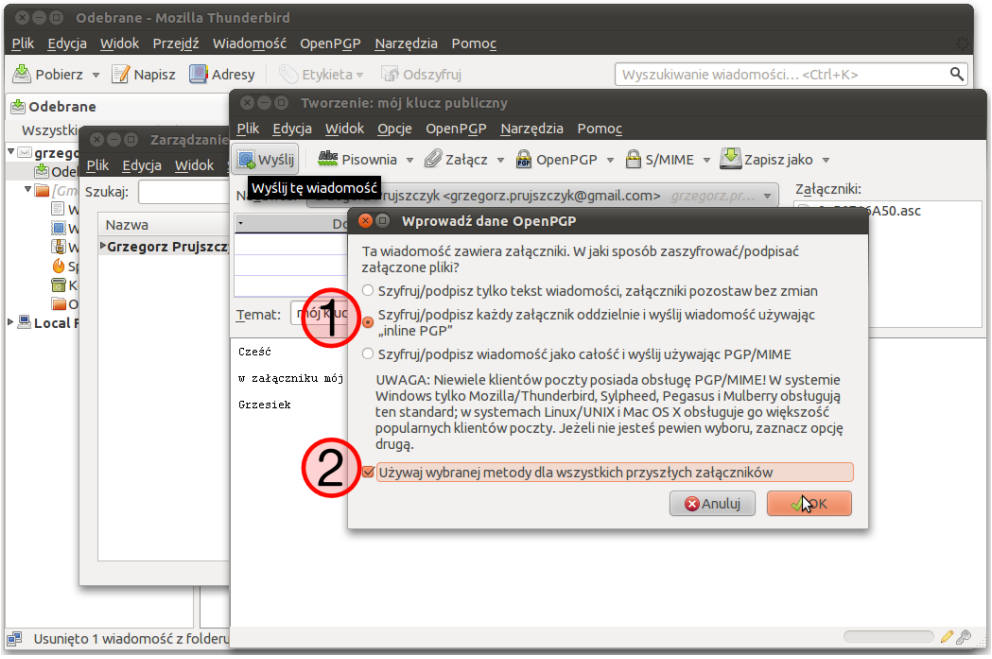
Rys.8. Zgadzamy się na zmianę ustawień. Są małe poprawki, dzięki którym programy będą lepiej współpracować.



Rys.9. Tworzenie klucza. Podczas tworzenia klucza do podpisu i szyfrowania wiadomości musimy wygenerować hasło do kluczy (pamiętaj o regułach tworzenia silnych haseł). Hasło to będziemy musieli podać, aby odblokować klucz prywatny (np. przy każdym uruchomieniu poczty). Hasło stanowi główne zabezpieczenie klucza, tak więc z jednej strony nie należy przesadzać z jego długością, a z drugiej nie może być zbyt proste do złamania – ponad 10 znaków to absolutne minimum, jeśli klucz ma być bezpieczny.



Rys.10. Generowanie certyfikatu. Podczas generowania kluczy istnieje również opcja wygenerowania certyfikatu służącego do unieważniania kluczy, w razie gdyby wpadły w niepowołane ręce.



Rys.11. Wysyłanie pierwszej wiadomości. Klucze zostały utworzone. Teraz możemy wysyłać pierwszy email do adresata, z którym chcemy prowadzić zaszyfrowaną korespondencję. Przy wysyłaniu pierwszego emaila określamy też, czy chcemy szyfrować załączniki, czy tylko emaile, co jest ostatnim koniecznym ustawieniem.

1. Po kliknięciu w oknie nowego listu kliknij na opcję *OpenPGP*. Następnie zaznacz opcję *Szyfruj/Podpisz każdy załącznika oddzielnie.*

2. Zaznaczamy również opcję używania wybranej metody dla wszystkich przyszłych załączników. Teraz możemy wysłać podpisany i zaszyfrowany mail, wybierając potrzebną nam opcję z menu OpenPGP.

OTR – SZYFROWANIE W KOMUNIKATORZE

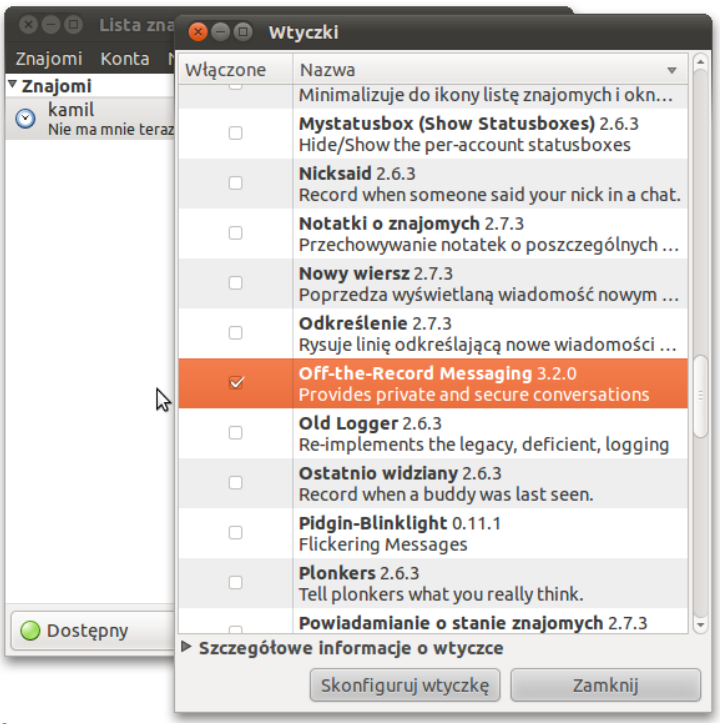
Jest to mniej znany sposób szyfrowania przewidziany do użycia z komunikatorami. Dostępny w formie wtyczki dla niektórych komunikatorów, np. Pidgin, pozwala na szyfrowanie przesyłanego tekstu niezależnie od protokołu komunikacji. Działa na zasadzie klucza publicznego, podobnie jak PGP, jednak w odróżnieniu od niego ma znacznie uproszczony sposób wymiany kluczy. OTR szyfruje ruch pomiędzy komunikatorami i samemu programowi udostępnia już odszyfrowaną wersję wiadomości, co oznacza, że archiwa nie będą zaszyfrowane. OTR możemy zainstalować w komunikatorze Pidgin, który obsługuje wiele protokołów: możemy podłączyć do niego nasze konto Gadu-Gadu, Google Talk, Jabber, Facebook Chat i wiele innych.

WAŻNY LINK

Pidgin – http://www.pidgin.im/ uniwersalny komunikator i klient chatowy. Dostępny dla systemów Windows, Linux i Mac OS. Obsługuje najpopularniejsze protokoły i sieci: AIM, Google Talk, IRC, Yahoo!, MSN, GaduGadu, ICQ, XMPP/Jabber i inn.

OTR - KONFIGURACJA

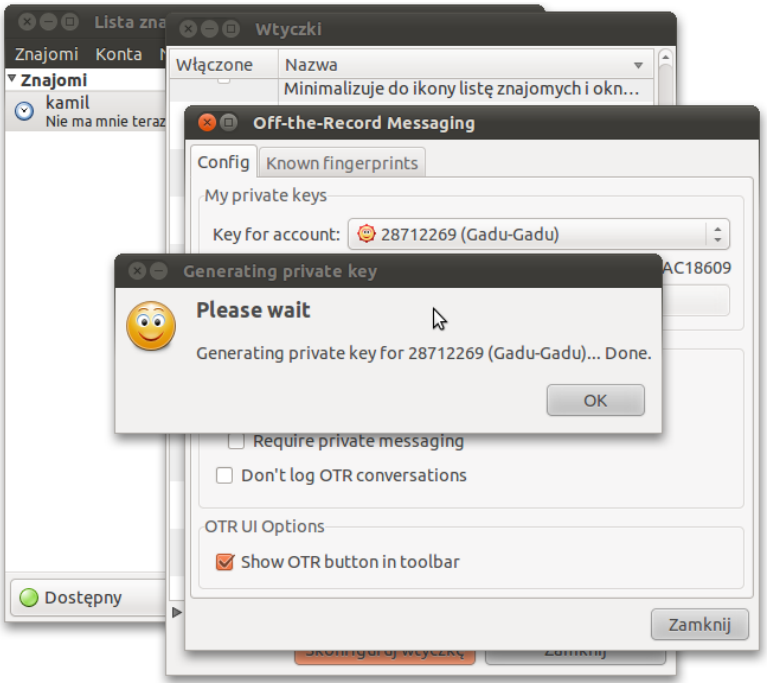
Po zainstalowaniu komunikatora Pidgin ściągamy i instalujemy wtyczkę OTR – do pobrania z http://www.cypherpunks.ca/otr (dostępne wersje na Windows, Mac i Linuksa). Po zainstalowaniu wtyczki musimy ją uruchomić w menu Narzędzia - Wtyczki.



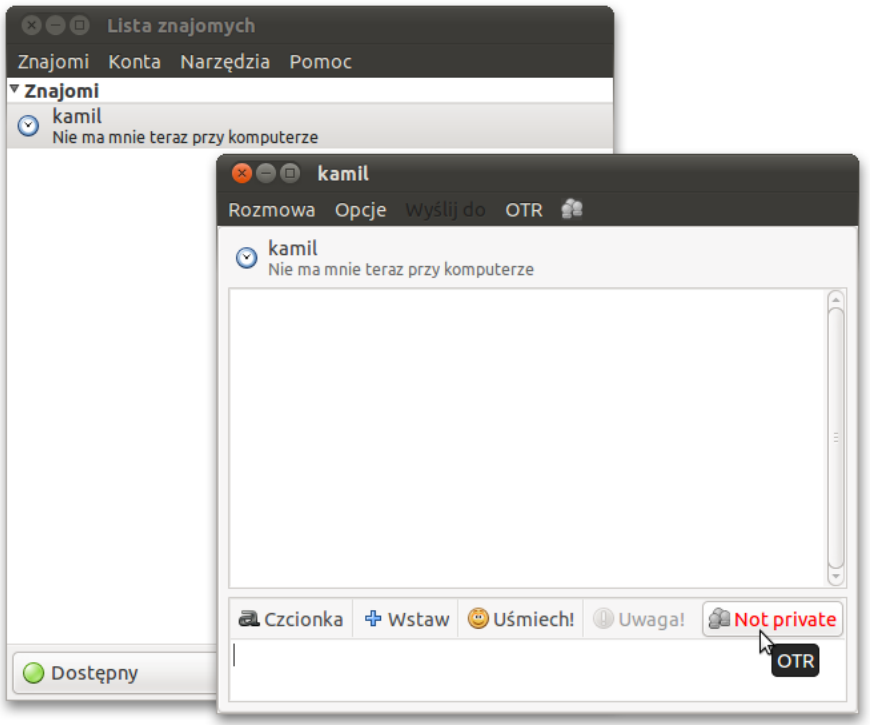
Rys.12. Lista wtyczek do programu Pidgin

Messaging. Po zainstalowaniu wtyczki OTR w Pigdinie wchodzimy w *Ustawienia* → *Wtyczki*, gdzie odnajdujemy *Off-The-Record Messaging*. Zaznaczamy tę opcję na liście, co spowoduje jej uruchomienie. Wchodząc w konfigurację, możemy od razu wygenerować klucze; można to również zrobić później w oknie rozmowy.

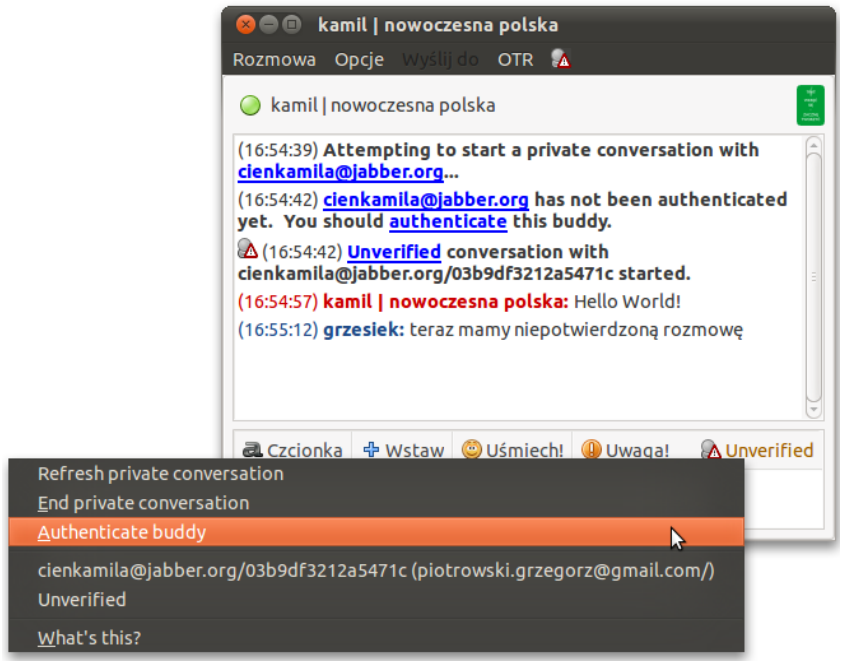
1.



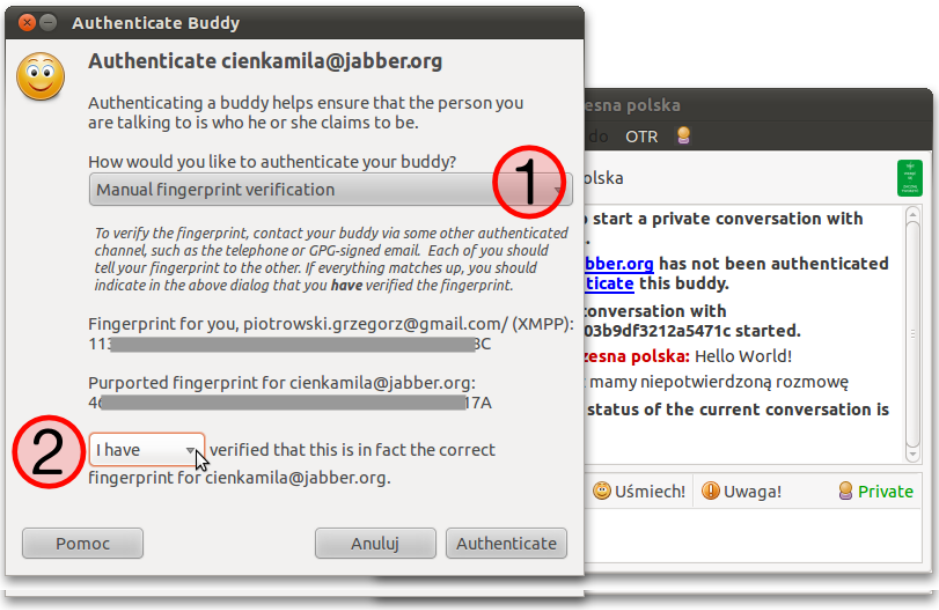
Rys.13. Generowanie klucza prywatnego. Przez właściwości wtyczki możemy skonfigurować ją dla wybranych kont, np. Gadu-Gadu czy czatu Facebook'a. W tym miejscu generujemy prywatny klucz dla danego kanału.



Rys.14. Rozmowa. Teraz wystarczy rozpocząć czat z inną osobą używającą OTR. W okienku rozmowy zobaczymy komunikat *Not Private* (niepoufna). Napis ten informuje nas o aktualnym stanie i zmienia się zależnie od niego. Po kliknięciu możemy wybrać opcję *Start private conversation* (rozpocznij prywatną rozmowę), która automatycznie ustawi podstawowe szyfrowanie.



Rys.15. Authenticate buddy. Jeżeli chcemy potwierdzić tożsamość i ustawić automatyczne szyfrowanie komunikacji z daną osobą, będziemy musieli potwierdzić kontakt, używając opcji *Authenticate buddy*.



Rys.16. Weryfikacja. Teraz musimy wybrać opcję weryfikacji. Najprostszą jest *Manual fingerprint verification*, przy której wystarczy potwierdzić, że obie osoby widzą poprawne „odciski" swoich kluczy. Po zatwierdzeniu (*I have...*) nasza komunikacja będzie już zabezpieczona i możliwa do odczytania tylko na naszych komputerach. W razie potrzeby możemy przeprowadzić weryfikację, sprawdzając wzajemnie z drugą osobą nasze podpisy, np. przez telefon.

SPAM

Spam to całość niechcianej komunikacji, która jest do nas kierowana. Może do nas docierać przez wszelkie możliwe kanały komunikacji i przybierać wiele różnych form, a osoba kierująca jego wysyłką może mieć bardzo różne cele. Spam to obecnie 78% wszystkich przesyłanych emaili, to plaga, która nawiedza też serwisy społecznościowe i komunikatory.

Program, który rozsyła spam może znać nasze imię i nazwisko lub pseudonim, tak więc wiadomość może być nie tylko wysłana do nas, ale i bezpośrednio do nas skierowana. Spamer może znać nasze przybliżone miejsce zamieszkania i dostosować język lub ofertę swojej wiadomości, tak jak to robią internetowe reklamy stron randkowych oferujące poznanie atrakcyjnych partnerów „w naszej okolicy".

SPAMVERTISING – SKLEPY

Najczęstszym typem spamu są po prostu reklamy różnych mniej lub bardziej nielegalnych produktów („leków", replik zegarków, elektroniki itd.). Oczywiście handlowcy rozsyłający spam są równie godni zaufania w kwestii wysyłki towaru, co w poszanowaniu naszej prywatności, więc zakupy u nich są fatalnym pomysłem. Za spam można też uznać niechciane reklamy od faktycznie istniejących sklepów, jednak te przeważnie dają jakąś opcję wypisania się z ich list adresowych.

SCAM – „NIGERIAN SPAM"

Częstym celem niechcianej poczty jest przekonanie nas do przelania pieniędzy na konto wysyłającej ją osoby pod różnymi pretekstami: cudownej oferty biznesowej; wygranej w loterii, w której nigdy nie braliśmy udziału; prośby o pomoc dla śmiertelnie chorego i tym podobne. Zawsze należy zastanowić się nad prawdopodobieństwem danej sytuacji (czemu miałby do nas pisać np. bankier z Indii czy żona byłego prezydenta jakiegoś afrykańskiego kraju?) i ewentualną korzyścią drugiej strony (na Skype może się do nas odezwać nieznajoma osoba mająca ochotę pogadać, ale jeśli stara się nas przekonać, że powinniśmy jej z jakiegoś powodu wysłać pieniądze, to coś jest nie tak).

PHISHING

Są to komunikaty, które celowo wyglądają jak wiadomość od naszego banku, sklepu, gry czy innej usługi. Komunikaty te przekonują nas do „zalogowania się", co w praktyce oznacza przekazanie hasła złodziejom. Email mający nas do tego nakłonić może wyglądać jak prawdziwy, jednak

nierzadko można go rozpoznać od razu po błędach w pisowni, absurdalnych wyjaśnieniach lub domenie, na którą jesteśmy kierowani. Linki pojawiające się w tekście składają się z faktycznego adresu i opisu linku, który jest wyświetlany (przeważnie jako niebieski podkreślony tekst). Oczywiście nadawca zawsze może dowolnie opisać każdy link (np. jako www.login.facebook.com), dlatego możemy mieć wrażenie, że faktycznie tam ten link nas skieruje. Zawsze warto jednak najechać na link myszką – po paru sekundach wyświetli nam się faktyczny adres, który może wyglądać lub brzmieć podobnie (powiedzmy login.facebuk.com zamiast login.facebook.com), ale kieruje na stronę kontrolowaną przez osobę, która chce zdobyć nasze hasło. Strona ta ponownie może wyglądać jak ta dobrze nam znana. Co więcej po „zalogowaniu się" i otrzymaniu podziękowania możemy zostać przekierowani na właściwą stronę tak, żebyśmy nie nabrali większych podejrzeń.

ZAGROŻENIA:

- phishing,
- wirusy,
- kradzież (pieniędzy, kont na usługach/grach, danych),
- upublicznienie mniej lub bardziej prywatnej komunikacji i informacji.

OCHRONA:

- nieklikanie na żadne linki z niechcianej poczty,
- uważne przyjrzenie się adresom i sprawdzenie prawdziwości linku przed jego kliknięciem,
- ochrona swojego adresu e-mail i używanie jednorazowych adresów w sytuacjach wymagających podania adresu.

WAŻNY LINK

Jednorazowe adresy mailowe

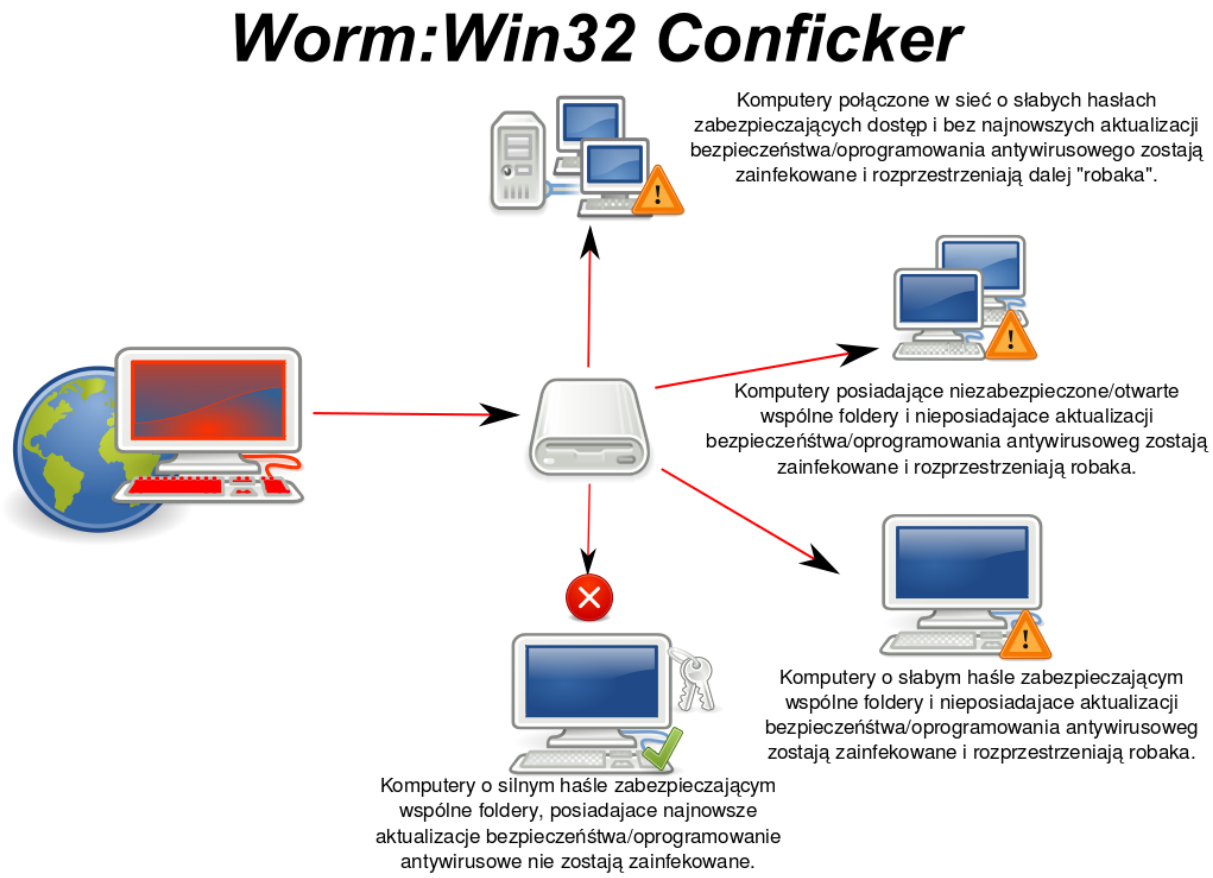
http://www.yopmail.com/pl/ to prosta usługa, dostępna również w języku polskim, umożliwiająca tworzenie jednorazowych adresów e-mail oraz tymczasową skrzynkę pocztową (8 dni). http://mailnull.com/ podobna usługa w języku angielskim umożliwiająca założenie konta i przypisywanie do niego kolejnych tymczasowych adresów email.

SŁOWNICZEK

Wirus komputerowy *– to najczęściej program komputerowy celowo zaprogramowany, aby się powielał i działał wbrew woli i zgody użytkownika urządzenia, na którym działa. Podobnie jak wirusy w przyrodzie, wirusy komputerowe potrzebują „nosiciela" (czyli programu, który będzie je przenosił) lub dystrybucji pocztą elektroniczną. Nosicielami zwykle są programy komputerowe lub pliki wykonywalne, odpowiadające za różne mikroprocesy w systemie operacyjnym. Podstawą ochrony przed wirusami jest unikanie otwierania i korzystania z podejrzanych załączników, programów i plików ściąganych z niezaufanych źródeł. Wirusy mogą działać w różny sposób i wywoływać różnego rodzaju szkody. Ich zwalczaniu służą programy antywirusowe, np. darmowy AVAST lub płatny Norton Antyvirus. Różne systemy operacyjne są w różnym stopniu odporne na wirusy. Za najbardziej podatny system uważa się najpopularniejszy Windows. Nie istnieją wirusy na systemy linuksowe.*

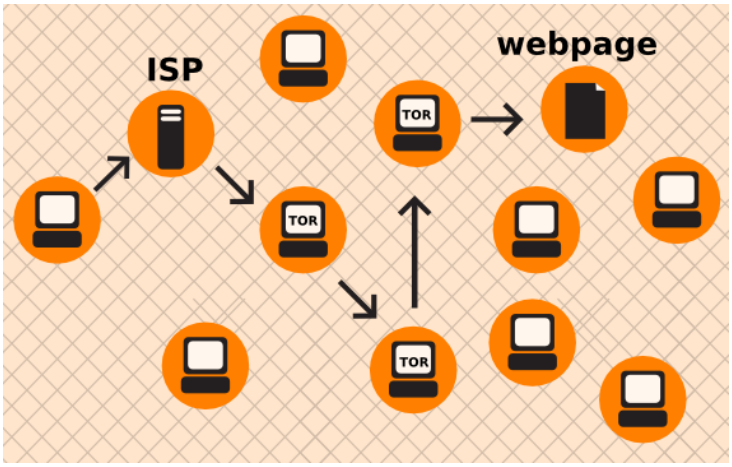
Robak (worm) *– samo-replikujący się program komputerowy, podobny do wirusa komputerowego. Główną różnicą między wirusem a robakiem jest to, że podczas gdy wirus potrzebuje nosiciela, robak rozprzestrzenia się własnymi siłami. Robak rozprzestrzenia się we wszystkich sieciach podłączonych do zarażonego komputera poprzez wykorzystanie luk w systemie operacyjnym lub naiwności użytkownika. Robak nie tylko się replikuje, może również: niszczyć pliki, wysyłać pocztę (z reguły spam), pełnić rolę backdoora lub konia trojańskiego.*

Współczesne robaki potrafią uzupełniać i zmieniać swoją funkcjonalność, pobierając z sieci dodatkowe moduły. Posiadają również możliwość zdalnego sterowania dalszym działaniem, tworząc botnety. Najczęściej są dystrybuowane (np. rozsyłane za pomocą poczty elektronicznej) w postaci tzw. downloaderów – względnie prostych i małych programów, których jedynym zadaniem jest skomunikowanie się z „centrum operacyjnym" i pobranie dodatkowych modułów.



Rys.17. Rozprzestrzenianie się robaków. Schemat przedstawia sposób rozprzestrzeniania się „robaków" komputerowych na przykładzie jednego z najgroźniejszych Win32 Confikcer, który wykorzystuje głównie słabo zabezpieczone sieci i wspólne dyski dzielone przez nie. Źródło: Wikimedia Commons, *http://commons.wikimedia.org/wiki/File:Conficker.svg na licencji CC-BY-SA.*

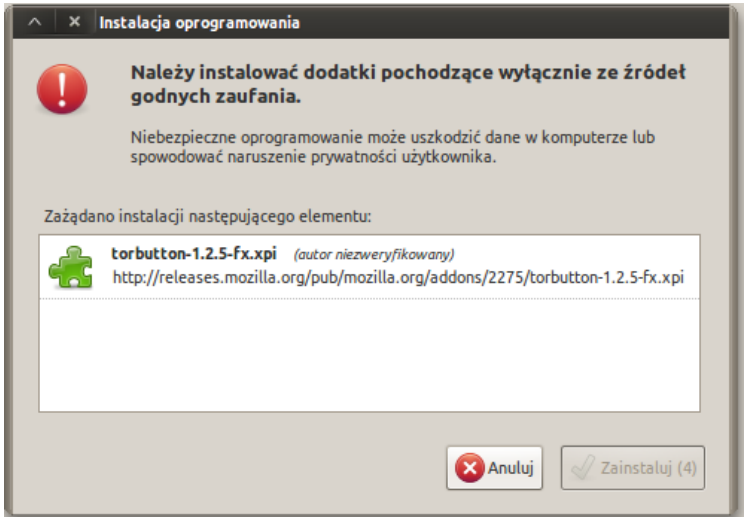
TOR



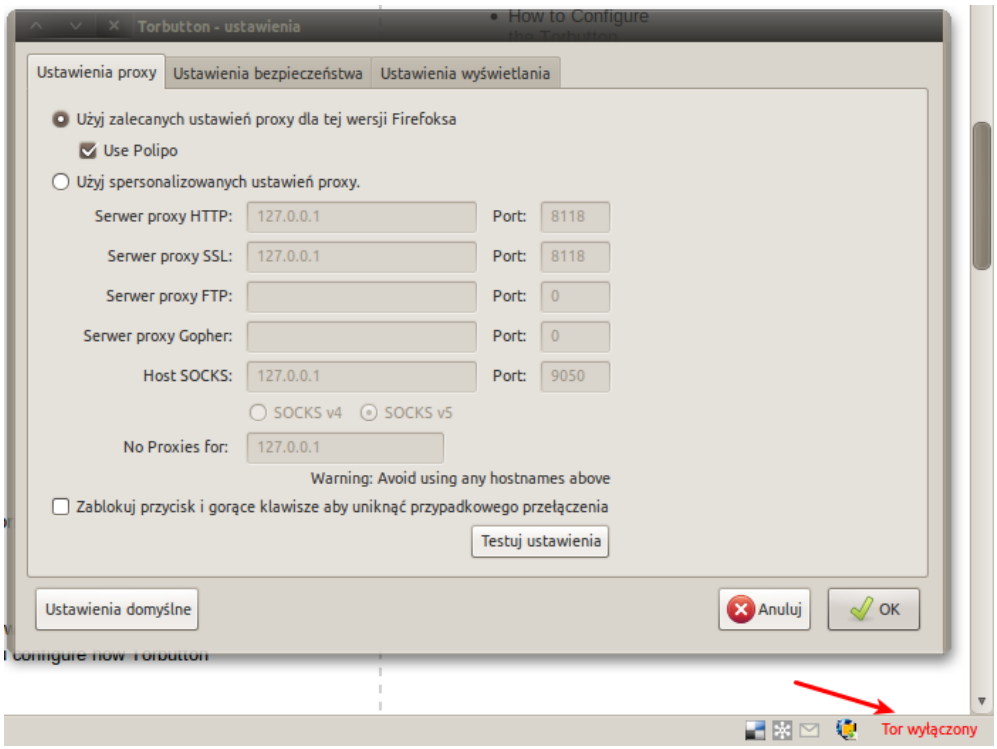
Rys.18. Schemat działania sieci TOR. Schemat przedstawia połączenia między komputerami działającymi w sieci, gdzie każdy przekaźnik zna jedynie adres poprzedzającego i następującego po nim przekaźnika, ale nie zna ostatecznego celu połączenia. Rysunek dostępny na CC-BY-SA, http://en.flossmanuals.net/CircumventionTools/TorTheOnionRouter

TOR (ang. The Onion Router) jest wirtualną siecią komputerową zapobiegającą analizie ruchu sieciowego i w konsekwencji zapewniającą użytkownikom prawie anonimowy dostęp do zasobów Internetu. Podobnie jak sieci Freenet, GNUnet czy MUTE, Tor może być wykorzystywany w celu ominięcia mechanizmów filtrowania treści, cenzury i innych ograniczeń komunikacyjnych. Gdy używasz Tora do przeglądania witryn sieci Web, Twoje połączenia są losowo kierowane przez sieć niezależnych serwerów Proxy, czyli serwerów pośredniczących w komunikacji. Cały ruch między serwerami Tor (lub przekaźnikami) jest szyfrowany, a każdy z przekaźników zna adres IP tylko dwóch innych przekaźników – tego, który go bezpośrednio poprzedza i tego, który następuje bezpośrednio po nim. Dzięki zapewnianiu prawie całkowitej anonimowości TOR, jak każde narzędzie, może być wykorzystywany w dobrej i złej wierze, np. w prowadzeniu działalności przestępczej. Więcej o projekcie znajdziecie na stronie: **www.torproject.org**

Najprostszym sposobem na rozpoczęcie pracy z TOR-em jest zainstalowanie pakietu wraz z wtyczką do przeglądarki Firefox o nazwie **TOR Button** (https://www.torproject.org/torbutton/), która umożliwia zmianę trybu pracy ze standardowego do połączenia przez TOR za pomocą jednego przycisku. Więcej o konfiguracji TOR-a oraz serwerów proxy znajdziecie w podręczniku o obchodzeniu cenzury w sieci z serii Floss Manuals. Znajdziecie tam dokładne informacje, jak konfigurować swoje połączenie w najbezpieczniejszy sposób.



Rys.19. Instalacja wtyczki TorButton w Mozilla Firefox.



Rys.20. Ustawienia. Po instalacji TorButton pojawi się jako napis na pasku stanu przeglądarki. Kliknięcie lewym przyciskiem uruchamia połączenie poprzez TOR, kliknięcie prawym przyciskiem myszki umożliwia wejście w ustawienia wtyczki. Domyślne ustawienia są skonfigurowane w sposób wystarczający dla większości użytkowników.

Dla pełniejszego bezpieczeństwa komunikację poprzez TORa również zawsze powinniśmy szyfrować, ponieważ może zostać przechwycona na początku lub końcu drogi w sieci.