Niektóre sposoby ochrony przed inwigilacją w sieci – 2

11 października 2010

SZYFROWANIE ROZMÓW PRZEZ KOMUNIKATORY INTERNETOWE

Pidgin – wieloplatformowy komunikator internetowy, obsługujący szereg protokołów transmisyjnych. Pidgin jest wolnym oprogramowaniem, dostępnym na warunkach GNU GPL. Pidgin umożliwia kontakt z użytkownikami komunikatorów: AOL Instant Messenger, Facebook chat– możliwość importowania listy znajomych z portalu społecznościowego FACEBOOK (wymagany plugin), Gadu-Gadu, ICQ, Internet Relay Chat, XMPP (Google Talk, …), MSN Messenger, MySpaceIM, MXit, Novell GroupWise, OpenNAP, SILC, SIMPLE, Skype , Tencent QQ, tlen.pl ,Xfire, Yahoo! Messenger, Zephyr. Stosowanie Pidgin – a z wtyczkami szyfrującymi umożliwia korzystanie więc jednocześnie szyfrowanie rozmów prowadzonych za pomocą wyżej wymienionych komunikatorów. Do multikomunikatora Pidgin dostępne są następujące wtyczki szyfrujące:

1. OTR używa kombinacji algorytmu klucza symetrycznego AES, protokołu Diffiego-Hellmana i funkcji skrótu SHA-1. Pozauwierzytelnianiem i szyfrowaniem, OTR zapewnia doskonałą poufność przesyłania i szyfrowanie z możliwością zaprzeczania. Jest najbezpieczniejszym z dostępnych protokołów szyfrujących dla Pidgina, jest także domyślnym komponentem zawartym w Adium..

2. Pidgin Encryption: Pidgin Encryption nie oferuje bezpiecznej metody wymiany kluczy szyfrujących i ich weryfikacji, co może skutkować fałszywym poczuciem bezpieczeństwa.

3. Pidgin Paranoia: Pidgin Paranoia korzysta z szyfrowania, które jest silne na papierze, ale w praktyce jest dość podatne na ataki.

4. XMPP/PGP: XMPP/PGP nie jest tak bezpieczne jako OTR, ale jest już standardem. Pidgin-PGP pozwala na szyfrowanie komunikatów wysyłanych do użytkowników off-line.

Pidgin – a ściągnąć można na przykład stąd: http://www.instalki.pl/programy/download/Windows/komunikatory/Pidgin.html. A tutaj znajdziecie instrukcję instalacji i użytkowania: http://aragwain.wordpress.com/2010/08/25/szyfrowanie-rozmow-w-pidginie/

Miranda – otwarty multikomunikator internetowy dla systemów z rodziny Microsoft Windows. Dla Mirandy dostępne są wtyczki szyfrujące. W zależności od wersji Mirandy szyfrowanie opiera się na protokole OTR lub na kluczach PGP. Mirandę ściągniesz z Polskiego Portalu Mirandy, tak także znajdziesz wszelkie potrzebne informacje, niestety autorzy strony nie zezwalają na jej linkowanie, więc linka nie wkleję.

EKG2 – oparty na wtyczkach komunikator internetowy dla systemów uniksowych (Linux, BSD). Oprogramowanie obsługuje różne protokoły m.in. XMPP (Jabber, z obsługą GTalka i Tlena), Gadu-Gadu (przy zastosowaniu biblioteki libgadu), IRC, rozpowszechniane jest na licencjiGPL. Moim zdaniem, z uwagi na obsługę wielu komunikatorów można zaliczyć EKG2 do multikomunikatorów. Jest on wyposażony w protokół ORT. EKG2 oraz potrzebne informacje zaczerpniesz z tej strony: http://pl.ekg2.org/index.php

X-IM – komunikator pod Windowsa. Ma wbudowane 256-bitowe szyfrowanie i 2048-bitowe klucze. Dostępny tutaj: http://x-im.net/

ODRĘBNY PROGRAM DO SZYFROWANIA KOMUNIKATORÓW

SIMP – współpracuje z MSN Messenger, Yahoo! Messenger, ICQ/AOL Instant Messenger (AIM), Jabber/Google Talk i działa systemach Windows i Linux. Należy go uruchomić w tle, po odpowiedniej konfiguracji sam będzie wykrywał połączenia i szyfrował je.

SZYFROWANIE POCZTY ELEKTRONICZNEJ

EnigMail – dodatek do aplikacji Mozilli został przygotowany, który może szyfrować nie tylko treść e-maila, ale również załączniki.

A-LOCK – który służy do szyfrowania poczty elektronicznej. W Internecie można ściągnąć darmową wersję A-LOCK-5.1 , która nie ma ograniczeń czasowych , ale ma ograniczenia funkcji. Program po uruchomieniu pracuje w tle redukując się do ikony w pasku zadań w prawym dolnym rogu ekranu. Klikając prawym przyciskiem myszy użytkownik może wybrać funkcję programu. Program w wersji darmowej potrafi zaszyfrować plik tekstowy przy pomocy podanego klucza. Klucz ten w wersji darmowej jest ograniczony do 5 znaków, w wersji pełnej może mieć do 56 znaków dla użytkowników z USA i Kanady, a 7 znaków dla pozostałych. Plik do szyfrowania można otworzyć w oknie edycji (Private Window), albo w oknie zewnętrznego edytora.

CenturionMail – umożliwia w szybki i łatwy sposób szyfrowanie poczty elektronicznej. Produkt przeznaczony jest dla klientów korporacyjnych i znakomicie współpracuje z najpopularniejszym programem do obsługi poczty elektronicznej – Microsoft Outlook. Aplikacja wykorzystuje do szyfrowania 256 bitowy klucz. Jedną z ciekawszych opcji jest możliwość tworzenia zaszyfrowanych maili, których nie można otworzyć przed określonym czasem lub datą (opcja Time Bomb).

Z pewnością nie wyczerpałem jeszcze tematu. Zawsze znajdzie się coś, co przeoczyłem, lub o czym nie wiedziałem. Chciałbym więc zachęcić koleżanki i kolegów, którym temat nie jest obcy do rozszerzenia zagadnienia.

Opracowanie: Cartafirus
Źródło: New World Order

BIBLIOGRAFIA

1. http://pl.wikipedia.org/wiki/Pidgin

2. http://pidgin-encrypt.sourceforge.net/index.php

3. http://grzglo.jogger.pl/2009/01/17/szyfrowanie-w-pidginie/

4. http://hack.pl/forum/faq/5059-szyfrowanie-danych-praktyczne-zastosowania.html

5. http://pl.ekg2.org/index.php

6. http://rafalwit.klub.chip.pl/a_Lock.htm

7. http://www.zoom.idg.pl/ftp/pc_9651/CenturionMail.3.0.3.html