WOJCIECH SMOL

Ekstremalne środki ostrożności w sieciach publicznych

Stopień trudności

Podłączenie przenośnego komputera do nieznanej, publicznej sieci komputerowej wiąże się z ogromnym ryzykiem. Wszystkie wykonywane operacje sieciowe mogą zostać przez kogoś podsłuchane, a nasze dane przechwycone. Zagrożenia mogą jednak zostać zminimalizowane poprzez zastosowanie kompleksowej strategii obronnej.

Z ARTYKUŁU DOWIESZ SIĘ

o zagrożeniach związanych z korzystaniem z obcych sieci komputerowych,

w jaki sposób opracować wielowarstwową strategię obrony swego komputera przenośnego,

o narzędziach pomocnych w obronie komputera przenośnego pracującego w obcej sieci,

o sposobach bezpiecznego korzystania z komputera w sieciach publicznych,

o dobrych praktykach w administrowaniu systemem operacyjnym i używanymi aplikacjami.

CO POWINIENEŚ WIEDZIEĆ

znać podstawowe zagadnienia dotyczące administracji systemami operacyjnymi z rodziny Windows oraz Linux,

znać podstawowe rodzaje sieciowych ataków.

Najnowszy rodzaj komputera przenośnego – netbook – okazał się wielkim rynkowym przebojem. Jak grzyby po deszczu pojawiają się coraz to nowe modele miniaturowych komputerków. Typowy netbook waży nieco ponad kilogram i jest w stanie pracować na baterii nawet 10 godzin. Wszystko to zachęca fanów mobilnych gadżetów do korzystanie z mini laptopów w niemal każdej sytuacji. Ponadto, coraz więcej instytucji publicznych oraz prywatnych udostępnia na terenie swych obiektów przewodowe i bezprzewodowe sieci komputerowe przeznaczone dla swych gości. Można więc spotkać osoby surfujące po Internecie w kawiarniach, pubach, dworcach, portach lotniczych czy też hotelowych holach. Czy użytkownicy korzystający z zasobów publicznych sieci komputerowych zdają sobie sprawę z czyhających na nich zagrożeń? Prawdopodobnie większość z nich ani przez chwilę nie zastanawia się nad kwestią bezpieczeństwa danych zgromadzonych na ich komputerach oraz przesyłanych w trakcie korzystania z obcej sieci.

Za linią wroga

Jakie więc zagrożenia niesie ze sobą korzystanie z zasobów nieznanej nam sieci komputerowej? Oczywiście ogromne! Przede wszystkim nie dysponujemy żadną wiedzą na temat konfiguracji obcej sieci, pracujących w niej urządzeniach oraz innych jej użytkownikach. Najważniejsze zagrożenia z jakich należy sobie zdać sprawę, to:

- możliwość fizycznej ingerencji osób trzecich (kradzież, chwilowe skorzystanie z naszego komputera przenośnego, itd.),
- możliwość przechwytywania całego naszego ruchu sieciowego, w szczególności loginów i haseł, przez pośredniczące w transmisji urządzenia sieciowe lub inne komputery pracujące w tej samej sieci,
- możliwość przechwycenia danych znajdujących się na naszym komputerze przez inne osoby korzystające z tej samej sieci.

Jak niebezpieczne jest korzystanie z publicznych sieci oraz jak niska jest czujność nawet zaawansowanych użytkowników komputerów, pokazał dobitnie projekt *Wall of Sheep*. *WoS* to bardzo interesujące przedsięwzięcie pewnej grupy hakerów, niosące ze sobą szczególne walory edukacyjne. W trakcie konferencji poświęconych bezpieczeństwu informatycznemu, takich jak *Defcon* lub *Black Hat*, grupa specjalistów pasywnie analizuje ruch sieciowy w udostępnionej dla gości sieci komputerowej. Hakerzy nie łamią żadnych zabezpieczeń, ani nie deszyfrują jakichkolwiek algorytmów szyfrujących, jedyne czego poszukują to loginy i hasła przesyłane tekstem

jawnym za pomocą nieszyfrowanych protokołów sieciowych. Okazuje się, że nawet pośród osób interesujących się bezpieczeństwem informacji, znajduje się wiele osób nieświadomych lub ignorujących zagrożenia związane z wykorzystywaniem tego rodzaju protokołów. W trakcie każdego takiego happeningu, hakerom udaje się w prosty sposób zdobyć dziesiątki cyfrowych tożsamości. Dane te są następnie publikowane (pełne loginy oraz częściowo zasłonięte hasła) w trakcie konferencji, na liście wymownie zatytułowanej jako *Wall of Sheep*. W ten oto sposób *złowione owieczki*, mogą następnie skorzystać z porad hakerów dotyczących unikania tego rodzaju zagrożeń oraz zapoznać się z zastosowanymi przez nich narzędziami i metodami zdobywania haseł. Warto wspomnieć, że w trakcie konferencji *Defcon 2005* w Las Vegas, udało się *złowić* hasła należące do inżyniera *Cisco Systems Inc.*, kilku pracowników *Apple Computer Inc.* oraz profesora Harvardu! Zobaczmy więc, w jaki sposób możemy być *mądrzejsi* od wspomnianego profesora w trakcie korzystania z sieci publicznych.

Defence in Depth

Strategia obrony systemów informatycznych znana jako *Defence in Depth* polega na wielowarstwowej obronie przechowywanych w systemie informacji. Warto na początek przyjrzeć się pierwotnemu znaczeniu terminu *DiD*. Otóż pochodzi on z terminologii militarnej i oznacza specyficzną strategię obrony przed nacierającymi siłami nieprzyjaciela. Tradycyjna obrona w postaci skoncentrowania wszystkich sił na linii frontu, w razie jej przerwania w jednym miejscu, załamuje się i pozwala nieprzyjacielowi na przeniknięcie w głąb bronionego terytorium oraz okrążenie pozostałych oddziałów obronnych. Taktyka *DiD* nakazuje natomiast rozproszenie na, o wiele szerszym obszarze, jednostek obronnych, grupując je wedle spełnianych funkcji obronnych, we wzajemnie uzupełniające się oddziały. Mimo że napastnik będzie w takim przypadku zazwyczaj zdolny do szybszego przełamania, stosunkowo słabszej linii frontu, to jednak w miarę swych postępów, będzie napotykał na kolejne linie obronne. Taka taktyka, jeśli nawet nie zatrzyma wroga, to z całą pewnością znacznie opóźni pochód nieprzyjaciela, co właśnie stanowi główną zaletę tej strategii. Wielu czytelników z pewnością osobiście stosowało tego typu taktyką w trakcie wirtualnych walk na polach bitew strategicznych gier komputerowych!

Taktyka *DiD* została z powodzeniem zaadaptowana do obrony systemów informatycznych, stając się jedną z najskuteczniejszych i najpowszechniej stosowanych po dziś dzień. *DiD* sprowadza się do stworzenia wielu warstw ochraniających system informatyczny. Podobnie jak na froncie, jeśli jedna z barier zostanie przez intruza pokonana, natrafi on jedynie na kolejne zabezpieczenie. Zwiększa to znacznie prawdopodobieństwo wykrycia atakującego, stwarza możliwość zastosowania dodatkowych środków ochrony oraz znacznie opóźnia przeprowadzenie udanego ataku.

Rozważając skuteczne środki ochrony komputera podłączonego do nieznanej sieci publicznej, chciałbym zaproponować właśnie strategię obrony wielowarstwowej, jako najskuteczniejszy sposób na zminimalizowanie występujących w takiej sytuacji zagrożeń. Rozważając informatyczną strategię *DiD* należy jeszcze podkreślić, że prawdziwe bezpieczeństwo zapewnia wyłącznie obecność wszystkich rozważanych warstw (zabezpieczeń) jednocześnie. Niezastosowanie choćby jednej z barier spowoduje lukę w całym systemie zabezpieczeń i w łatwy sposób może doprowadzić do kompromitacji chronionego systemu.

Tworząc strategię *Defence in Depth* dla systemu, który ma zostać podłączony do nieznanej sieci publicznej, należy wokół przechowywanych w nim danych stworzyć następujące warstwy ochronne:

- świadomości użytkownika,
- dostępu fizycznego,
- sieciowego dostępu do systemu,
- systemu operacyjnego i pracujących pod jego kontrolą aplikacji,
- dostępu do danych.

Wszystkie, opisane szczegółowo poniżej, warstwy ochronne muszą zostać zbudowane przed podłączeniem systemu do sieci publicznej. Zabezpieczanie systemu już w trakcie pracy w obcej sieci lub co gorsza z wykorzystaniem jej zasobów (np. pobieranie aktualizacji do oprogramowania i systemu operacyjnego w obcej sieci) mija się z celem, a wręcz stwarza dodatkowe zagrożenie! System musi więc zostać w pełni zabezpieczony przed wydarzeniami, które będą wymagały pracy w obcej sieci (wyjazd służbowy, udział w konferencji, itd.), a najlepiej by zawsze był przystosowany do pracy w nieprzyjaznym środowisku.

Świadomość użytkownika systemu

Piękno znajduje się w oczach patrzącego, natomiast bezpieczeństwo systemu informatycznego spoczywa w umyśle jego właściciela. Nie ma bezpiecznego systemu komputerowego bez świadomości zagrożeń wśród jego użytkowników.

Świadomość zagrożeń oraz znajomość metod ochrony własnych informacji musi zawsze stanowić pierwszą i w wielu przypadkach najważniejszą warstwę obronną strategii *Defence in Depth*. W przypadku korzystania z zasobów obcych sieci, zdawanie sobie sprawy z czyhających na nas zagrożeń nabiera szczególnego znaczenia.

Przede wszystkim, chcąc skorzystać z dostępu do Internetu w miejscach ogólnie dostępnych (lotnisko, kawiarenka internetowa, konferencja), nigdy nie wolno korzystać z komputerów udostępnianych przez osoby trzecie! Będąc w kawiarence internetowej, zamiast korzystać z przygotowanych tam komputerów, poprośmy o podłączenie naszego komputera przenośnego. Skorzystanie z komputera przygotowanego przez osoby trzecie grozi między innymi następującymi konsekwencjami:

- nasze loginy, hasła oraz wszelkie informacje wprowadzane za pomocą klawiatury mogą zostać przechwycone przez zainstalowany w systemie programowy lub sprzętowy *keylogger* (program lub urządzenie

przechwytujące wszystkie znaki wprowadzane z klawiatury),
- używane w trakcie pracy na obcym komputerze pamięci przenośne (np. pendrive) mogą zostać zainfekowane groźnymi wirusami poprzez samo ich podłączenie do obcego systemu i w konsekwencji przeniesione na komputer domowy lub służbowy,
- wszelkie dane (zdjęcia, dokumenty, załączniki poczty elektronicznej, itd.) otwierane, edytowane lub zapisywane na obcym komputerze, nawet po ich wykasowaniu, mogą zostać później z powodzeniem odtworzone przez osoby trzecie.

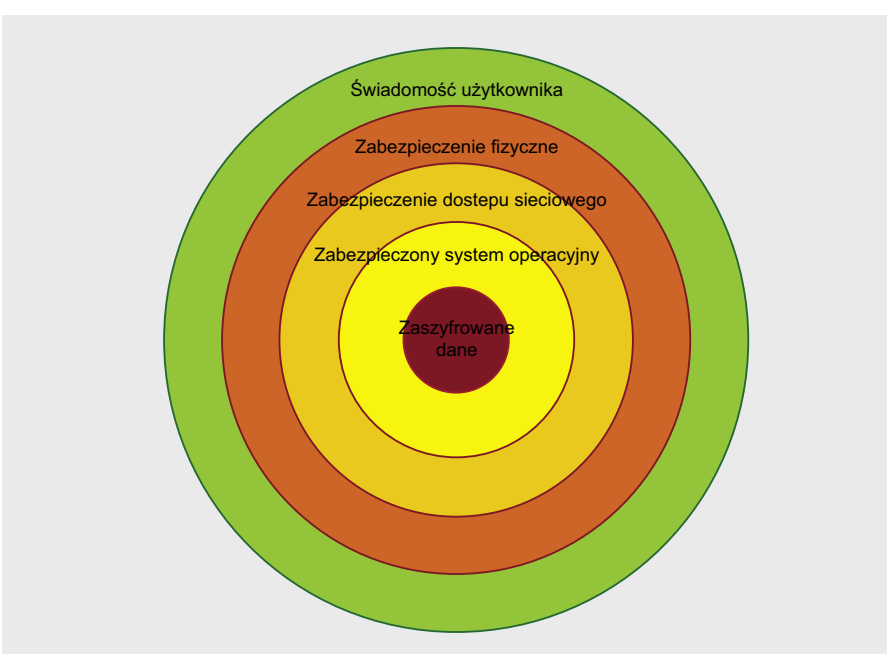
Warto zauważyć, że nawet jeśli właściciel obcej sieci nie ma złych zamiarów i sam w żaden sposób nie podgląda swych gości, to system, z którego korzystamy, mógł zostać zmodyfikowany lub zainfekowany przez jedną z korzystających z niego przed nami osób. Jeśli nie dysponujemy komputerem przenośnym lub nie możemy go z różnych względów zabrać w konkretną podróż, przygotujmy sobie na tę okazję własną płytę Live CD. Korzystając z obcego komputera, zapytajmy czy możemy go uruchomić korzystając z własnego systemu operacyjnego uruchamianego z płyty, takiego jak choćby *Knoppix*. Korzystając z takiego systemu operacyjnego, będziemy mieli pewność, że nie jest on w żaden sposób zmodyfikowany i nie zawiera złośliwego oprogramowania.

Oczywiście uniknięcie korzystania z obcego systemu operacyjnego nie powinno uśpić naszej czujności. Nadal nie jesteśmy bezpieczni, pozostają przecież zagrożenia czyhające w samej obcej sieci.

Przede wszystkim, korzystając z publicznych sieci, należy bezwzględnie unikać korzystania z protokołów nieszyfrowanych, takich jak:

- Telnet,
- HTTP,
- SMTP,
- SNMP,
- POP3,
- FTP.

Korzystanie z powyższych protokołów, szczególnie w nieznanej sieci, jest równoznaczne z proszeniem się o kłopoty. Każdy z tych protokołów przesyła hasła w postaci niezaszyfrowanej. To z kolei oznacza, że zarówno operator obcej sieci (podsłuchując ruch sieciowy przepływający przez centralne urządzenia sieci – np. korzystając z funkcji *Port Mirroringu* przełącznika sieciowego, czyli replikowania całego ruchu sieciowego dowolnego portu na innym wybranym porcie), jak i jej dowolny inny użytkownik (korzystając z ataku *ARP Spoofing*, dowolny klient jest w stanie podsłuchać ruch sieciowy z całego segmentu sieci) może za pomocą dość prostych metod poznać nasze hasła.



Rysunek 1. *Schemat proponowanej strategii Defence in Depth*

Rozwiązaniem jest niestety wyłącznie całkowita rezygnacja z korzystania z tych niebezpiecznych protokołów. Dana usługa może przecież być dostępna za pomocą innego, bardziej bezpiecznego interfejsu. Przykładowo, zamiast korzystać z poczty elektronicznej, za pomocą klienta pocztowego skonfigurowanego najczęściej do pracy z wykorzystaniem protokołów POP3 oraz SMTP, w sieci obcej warto skorzystać z dostępu do konta poprzez interfejs webowy. Większość serwerów pocztowych oferuje obecnie możliwość obsługi poczty z poziomu strony internetowej za pomocą szyfrowanego połączenia HTTPS. Należy przy tym zwrócić uwagę, czy szyfrowane jest całe połączenie, czy też może tylko sam moment logowania (dzieje się tak nawet w przypadku wielu znanych serwisów, takich jak choćby Gmail). W takim wypadku chronione będzie wyłącznie nasze hasło dostępowe, ale już cała pozostała sesja (wszystkie przesyłane dane) może zostać podsłuchana! Natomiast jeśli serwer wspiera szyfrowane odpowiedniki protokołów pocztowych (tzn. POP3S oraz Secure SMTP) wystarczy tylko zmodyfikować odpowiednio ustawienia naszego klienta pocztowego. Sprowadza się to zazwyczaj do zaznaczenia opcji Ten serwer wymaga zaszyfrowanego połączenia (SSL) lub podobnej (w zależności od stosowanego klienta) i określenia portów na których działają połączenia szyfrowane (POP3S – 995, Secure SMTP – 465). Dzięki takim rozwiązaniom będziemy w stanie w każdej sytuacji bezpiecznie korzystać z poczty elektronicznej.

Korzystanie wyłącznie z protokołów szyfrowanych, takich jak HTTPS, nie zwalnia nas jednak z zachowania czujności. Wspomniana wcześniej technika *ARP Spoofing* może pozwolić intruzowi na wykonanie niezwykle groźnych ataków typu *Man in the middle*. Tego rodzaju atak polega na takim przekierowaniu ruchu sieciowego pomiędzy dwoma uprawnionymi stronami transmisji, by cały ruch przechodził przez punkt

pośredniczący, jakim staje się komputer intruza. Tego rodzaju działanie pozwala na pośredniczenie w transmisjach szyfrowanych za pomocą (zazwyczaj) bezpiecznych protokołów, takich jak SSL i SSH i w efekcie przechwycenie wszystkich newralgicznych informacji (w szczególności haseł dostępowych do usług sieciowych). Korzystanie z tzw. bezpiecznych protokołów, w nieznanej nam sieci komputerowej, może się więc okazać niezwykle groźne, szczególnie gdy świadomość szyfrowania transmisji uśpi czujność użytkownika. Po pierwsze należy uświadomić sobie, że żadne połączenie nie jest do końca bezpieczne. Po drugie należy zwracać uwagę na pewne, czasem subtelne, sygnały świadczące o mogącym się właśnie odbywać ataku. Jeśli nasze połączenie HTTPS będzie się odbywało za pośrednictwem komputera intruza, wielce prawdopodobne jest, że nasza przeglądarka internetowa wyświetli przy próbie połączenia jakieś ostrzeżenie (Rysunek 2). Może to być komunikat o nieważności certyfikatu serwera, braku jego podpisu lub potwierdzenia przez zaufane centrum certyfikacji. W trakcie nawiązywania połączenia SSH, takim sygnałem ostrzegawczym będzie natomiast informacja o zmianie klucza hosta, z którym chcemy nawiązać połączenie. Tego rodzaju ostrzeżenia, szczególnie jeśli korzystamy z obcej sieci, należy zawsze poważnie traktować i natychmiast przerwać zagrożone połączenie. Innym symptomem odbywającego się właśnie ataku *ARP Spoofing* może być nadmierne obciążenie sieci (w wyniku wielokrotnego powielania ruchu przez pośredniczący w nim komputer intruza) lub chwilowe problemy w nawiązywaniu połączeń. Tego rodzaju symptomy będzie jednak bardzo trudno odróżnić od zwykłych, przejściowych problemów w działaniu sieci. Najskuteczniejszym zabezpieczeniem przed tego rodzaju atakami będzie używanie oprogramowania IDS (*Intrusion Detection System*) lub niewielkich programów dedykowanych do wykrywania ataków ARP.

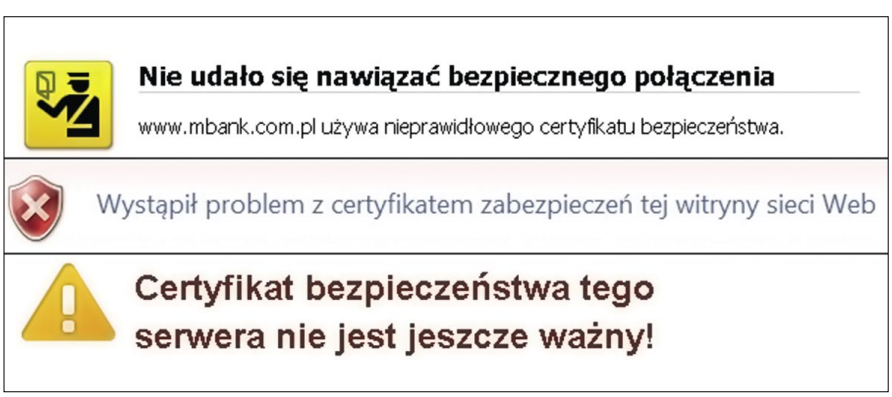
Mówiąc o świadomości użytkownika korzystającego z nieznanych mu sieci, warto również powiedzieć kilka słów na temat polityki tworzenia haseł dostępowych do poszczególnych rodzajów usług sieciowych. Każdy użytkownik wielu usług powinien sobie wypracować pewną politykę zarządzania własnymi hasłami. Oczywiście stosowanie jednego hasła do wszystkich usług jest niedopuszczalne. Najbezpieczniejsze byłoby stosowanie za każdym razem innego hasła, jednak z powodu tego, że liczba kont, które obecnie posiada przeciętny użytkownik Internetu stale rośnie, nie jest to wygodne, a wręcz grozi częstym zapominaniem poszczególnych haseł w natłoku wymaganych do zapamiętania informacji. Najrozsądniejsze wydaje się więc zastosowanie jednego hasła do danego rodzaju usługi. Przykładowo, stosujmy to samo (oczywiście mocne) hasło do wszystkich naszych internetowych kont bankowych, inne hasło do wszystkich kont poczty elektronicznej, jeszcze inne hasło do wszystkich stron internetowych wymagających logowania, itd. W ten oto sposób, użytkownik korzystający z 4 kont pocztowych, 3 kont bankowych, oraz 7 portali wymagających logowania, będzie musiał zapamiętać tylko 3 hasła, w stosunku do 14 haseł, które musiałby zapamiętać, w przypadku tworzenia zawsze unikalnych haseł. Tego rodzaju funkcjonalny podział haseł nie tylko odciąży naszą pamięć, ale też zwiększy nasze bezpieczeństwo. W przypadku gdy, w razie korzystania z obcej sieci, użyte przez nas hasło do poczty internetowej zostanie podsłuchane, intruz będzie dysponował co najwyżej dostępem do wszystkich naszych kont pocztowych, ale już nie do kont bankowych, czy też innych ważnych usług.

Korzystając z Internetu w ogólnodostępnej sieci warto również pamiętać o zasadzie korzystania wyłącznie z tego co jest naprawdę niezbędne. Jeśli nie musimy akurat w tym momencie wykonać jakiegoś ważnego przelewu, to nie logujmy się do banku internetowego, tylko po to by sprawdzić stan konta. Z im mniejszej ilości usług skorzystamy, tym mniejsze prawdopodobieństwo, że jakieś krytyczne dane zostaną przez intruza przechwycone. Jeśli natomiast wiemy już przed wyjazdem, że w jego trakcie będziemy musieli korzystać tylko z jednej konkretnej usługi, np. z jednego konta poczty internetowej, to zmieńmy przed podróżą hasło do tej usługi na jakieś niewykorzystywane nigdzie indziej. W ten sposób, jeśli takie hasło zostanie przechwycone, to pozwoli to intruzowi wyłącznie na dostęp do tejże konkretnej usługi. Po powrocie natomiast, należy z powrotem zmienić takie tymczasowe hasło.

Stosując się do powyższych zdroworozsądkowych zasad korzystania z obcych sieci, bez zastosowania specjalnych metod technicznych, znacznie podniesiemy bezpieczeństwo własnych informacji. Jest to jednak tylko pierwszy etap na drodze do osiągnięcia całkowitego bezpieczeństwa.

Dostęp fizyczny

W trakcie korzystania z przenośnego komputera w miejscach publicznych należy zawsze mieć na uwadze łatwość jego utraty (zgubienie, kradzież, itd.) oraz łatwość z jaką mogą mieć do niego dostęp niepowołane osoby.



Rysunek 2. *Komunikaty mogące świadczyć o wystąpienie ataku Man in the middle (od góry: Mozilla Firefox, Windows Internet Explorer oraz Google Chrome)*

Co to oznacza z punktu widzenia bezpieczeństwa naszych informacji? Oczywiście potencjalne, ogromne kłopoty. Urządzenia infrastruktury informatycznej (komputery, serwery, urządzenia sieciowe, drukarki, itd.) są przez producentów zazwyczaj konstruowane wg takiej zasady, że osoba która ma do urządzenia dostęp fizyczny, może prostymi metodami uzyskać dostęp do konfiguracji oraz danych zawartych w urządzeniu. Oznacza to, że postronna osoba, która wejdzie w posiadanie naszego komputera przenośnego, przejmie również wszystkie zawarte w nim dane. Zazwyczaj każdy zdaje sobie z tego przecież sprawę, jednak mało kto stosuje jakieś środki ostrożności w zakresie bezpieczeństwa fizycznego swego sprzętu komputerowego.

Okazuje się jednak, że producenci przenośnych komputerów przewidzieli zabezpieczanie fizyczne swych produktów. Obecnie, około 99% laptopów jest przecież wyposażonych w gniazdo *Kensington Lock* (inne nazwy to *K-Slot* lub *Kensington Security Slot*).

Jest to gniazdo pozwalające za pomocą specjalnego zamka oraz kłódki (z szyfrem lub kluczem) na zamocowanie stalowej linki zabezpieczającej sprzęt przed kradzieżą. Istnieją również rozwiązania konkurencyjne, np. zamki mocowane na portach VGA, przez co nie wymagana jest obecność specjalnego złącza. Istnieją również zabezpieczenia elektroniczne, emitujące sygnał alarmowy, w razie usunięci zabezpieczenia.

Jeśli jednak mimo zabezpieczenia laptopa za pomocą stalowej linki, dojdzie do jego kradzieży, zadbajmy o to, by nasze dane mimo wszystko nie dostały się w niepowołane ręce. Zabezpieczy nas przed tym jedynie zaszyfrowanie całego dysku twardego. W tym celu polecam świetne oprogramowanie *Open Source*, jakim jest *TruCrypt*. Jest to uniwersalne oprogramowanie dla systemów operacyjnych Windows 2000/XP/2003/VISTA, Linux oraz Mac OS, umożliwiające szyfrowanie całych partycji dyskowych. Po wprowadzeniu hasła, którym zabezpieczone zostały nasze partycje, możliwa jest normalna praca na danym dysku, tak jakby był to każdy inny dysk dostępny w systemie. Jeszcze do niedawna *TruCrypt* ustępował komercyjnym rozwiązaniom brakiem możliwości szyfrowania partycji systemowych. Jednakże wersja 5.0 i wyższe jest już pozbawiona tego ograniczenia. Do zaszyfrowania dysków możemy wykorzystać bardzo bezpieczny algorytm AES, który praktycznie zapewni naszym danym całkowite bezpieczeństwo.

Fizyczny dostęp innych osób do naszego komputera niesie ze sobą jeszcze kilka innych zagrożeń. Oddalając się od swego komputera przenośnego, oprócz założenia zapięcia fizycznego, pamiętajmy o bezwzględnym wylogowaniu się z systemu operacyjnego. Uniemożliwi to podejście obcej osobie i chwilowe skorzystanie z naszego systemu w jej tylko znanym celu. Znane są również przypadki osób podchodzących do pozostawionych na chwilę komputerów, które wtykają na chwilę w port USB specjalnie przygotowaną pamięć flash. Jeśli w systemie operacyjnym komputera, aktywna jest funkcja *Autoodtwarzania* (znana najczęściej jako autostart), komputer automatycznie zaczyna wykonywać pewną złośliwą procedurę zawartą na pendrivie (może to być instalacja trojana w systemie, pobranie plików, w których system przechowuje hasła, itd.). Dlatego, jak i z wielu innych powodów związanych z bezpieczeństwem naszego systemu, bezwzględnie należy wyłączyć tę funkcję w systemie operacyjnym. Przykładowo, w systemie Windows XP, wyłączymy globalnie tę funkcję za pomocą przystawki *Zasady grupy* (komenda *gpedit.msc*). W przystawce nawigujemy do widoku *Konfiguracja komputera/Szablony administracyjne/System* i aktywujemy opcję *Wyłącz funkcję Autoodtwarzanie*.

Korzystając z powyższych rad unikniemy przejęcia naszych danych w wyniku fizycznej ingerencji osób trzecich. Zastosowanie tych zasad tworzy jednocześnie kolejną warstwę ochronną w budowanej przez nas strategii obrony przed wrogimi sieciami i grasującymi w nich intruzami.

Wróg u bram

Korzystając z własnego komputera w skrajnie nieprzyjaznych warunkach, jakie z pewnością stanowi publicznie dostępna, otwarta sieć, należy pamiętać, by pozamykać wszelkie wrota, które potencjalnie mogą umożliwić intruzowi przeniknięcie do naszego systemu.

Jak można więc przedłużyć czas pracy swego komputera przenośnego na baterii, przyspieszyć działanie jego systemu operacyjnego, a zarazem znacząco zwiększyć jego bezpieczeństwo? Nic prostszego... Wystarczy tylko powyłączać wszelkie urządzenia i interfejsy, z których aktualnie nie korzystamy. Jeśli więc, przeglądamy Internet w kawiarence internetowej, a nasz laptop został przez obsługę podłączony do sieci za pomocą kabla sieciowego, wyłączmy kartę WiFi oraz Bluetooth. Oba te interfejsy, jeśli pozostają zawsze włączone, stanowią przecież pewną potencjalną furtkę dla włamywacza. Zazwyczaj użytkownicy zdają sobie sprawę z tego, że włączony interfejs WiFi może spowodować wyciek danych, natomiast zagrożenia związane z połączeniem Bluetooth są zazwyczaj ignorowane. Dzieje się tak

Rysunek 3. *Zagrożenia wykryte przez program Secunia Personal Software Inspector*

prawdopodobnie dlatego, że *Sinozęby* kojarzy się nam zazwyczaj z sieciami i urządzeniami o zasięgu co najwyżej kilku metrów. Jest to jednak nie do końca słuszne przekonanie. Urządzenia Bluetooth zostały podzielone na trzy klasy mocy. Podczas gdy urządzenia klasy 3 i 2 nie mają zasięgu większego niż odpowiednio 1 i 10 m, to już urządzenia klasy 1 są w stanie pracować na dystansach dochodzących do 100 m! Inną przyczyną ignorowania zagrożeń związanych z tym standardem komunikacyjnym może być to, że zazwyczaj jest on wykorzystywany do przyłączania *niewinnych* urządzeń peryferyjnych, takich jak myszki, klawiatury, słuchawki itd. Tymczasem, podobnie jak WiFi, *Sinozęby* może z powodzeniem posłużyć do utworzenia sieci komputerowej *ad hoc*. Jak wiadomo, sieć tego rodzaju pozbawiona jest centralnego urządzenia zapewniającego dodatkowe mechanizmy bezpieczeństwa (takiego jak *Access Point* w przypadku sieci WiFi), może więc zostać stosunkowo łatwo wykorzystana przez intruza do włamania. Nie zagłębiając się szczegółowo w tematy związane z bezpieczeństwem Bluetooth, warto tylko zauważyć, że urządzenie może pracować w trybie *Nonsecure mode* (jeden z 3 możliwych trybów pracy), który to nie zapewnia jakichkolwiek zabezpieczeń dla nawiązywania połączeń oraz samej transmisji. Zaś w pozostałych dwóch trybach są stosowane zabezpieczenia takie jak autoryzacja, autentykacja oraz szyfrowanie transmisji, natomiast ich skuteczność jest mocno dyskusyjna.

Należy więc zawsze, a już szczególnie w miejscach publicznych, wyłączać wszelkie niepotrzebne w danej chwili interfejsy komunikacyjne. Notebooki są zazwyczaj wyposażone w umieszczone na obudowie przełączniki umożliwiające szybkie włączanie i wyłączanie WiFi oraz Bluetooth, warto więc z nich korzystać. Wyłączenie karty WiFi, adaptera Bluetooth i innych urządzeń systemowych powinno również przedłużyć czas pracy naszego komputera przenośnego na baterii, jak i nieco odciążyć zasoby systemowe.

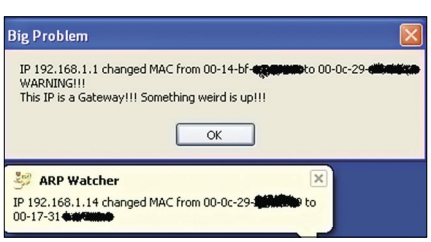
Pozamykanie furtek, przez które intruz mógłby przeniknąć do naszego systemu stanowi kolejną zbudowaną przez nas warstwę obronną strategii *DiD*. Zastanówmy się teraz jak powinniśmy przygotować do pracy w obcej sieci nasz system operacyjny oraz pracujące pod jego kontrolą aplikacje.

Mój system operacyjny jest moją twierdzą

Zbudowanie bezpieczeństwa systemu operacyjnego oraz pracujących w jego środowisku aplikacji jest oczywiście kluczową kwestią w strategii *Defence i Depth*. Ta warstwa obronna jest również najtrudniejsza w praktycznym wykonaniu ze wszystkich omówionych. Różnorodność systemów operacyjnych, aplikacji, usług i konfiguracji jest tak ogromna, że naprawdę trudno zapanować nad bezpieczeństwem własnego systemu. Można jednak wyróżnić kilka kwestii kluczowych dla bezpieczeństwa systemu wystawionego na próbę w obcej sieci komputerowej, uniwersalnych praktycznie dla wszystkich spotykanych obecnie rozwiązań.

Przede wszystkim, system operacyjny oraz pracujące w nim aplikacje muszą zostać zaktualizowane zanim (podkreślam – zanim) komputer zostanie podłączony do nieznanej sieci. Praktycznie wszystkie obecnie używane systemy operacyjne wyposażone są w funkcje pozwalające na ich łatwe zaktualizowanie. W systemach z rodziny Windows wystarczy skorzystać z funkcji *Windows Update*, w systemach z rodziny Linux podobne rezultaty (w zależności od konkretnej dystrybucji) można osiągnąć poleceniami: *apt-get update*, *apt-get upgrade*, *yum update*, itp. Nie wolno wykonywać jakichkolwiek aktualizacji już w trakcie korzystania z nieznanej nam sieci komputerowej. W takim przypadku nie mamy przecież żadnej pewności, czy pobierane aktualizacje są rzeczywiście oryginalnymi poprawkami producenta. Nie jest to w żadnym razie wyłącznie teoretyczne zagrożenie. W Internecie dostępne jest specjalne narzędzie o nazwie *Evilgrade*, umożliwiające ingerencję w proces aktualizacji kilku popularnych aplikacji (np. dodatku Java, iTunes, OpenOffice'a i innych). Zasada działania jest prosta, oprogramowanie podszywa się pod legalny serwer aktualizacji i odpowiada na zapytania o aktualizacje wysyłane przez podatne na ten atak aplikacje. Jednak zamiast aktualizacji, intruz może w ten sposób zainstalować w systemie dowolny, złośliwy kod. *Evilgrade*, jako wielomodułowy *framework*, może być swobodnie modyfikowany, w celu obsługi innych aplikacji. Należy więc zwracać baczną uwagę na to, skąd nasze aplikacje pobierają aktualizacje.

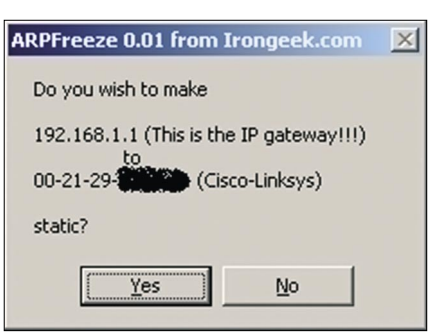
Mechanizmy aktualizacji wbudowane w system operacyjny mogą nie być w stanie dokonać aktualizacji oprogramowania pracującego w systemie. Tymczasem ze statystyk jasno wynika, że rośnie liczba exploitów wymierzonych nie tyle w sam system operacyjny, co w pracujące w nim aplikacje. Szczególnie głośno było w ostatnim czasie o dziurach w oprogramowaniu Adobe (Flash oraz Reader). Podobnie więc jak w przypadku systemu operacyjnego, wszystkie aplikacje muszą zostać zaktualizowane przed podłączeniem się do obcej sieci. Mechanizmy wbudowane w system operacyjny mogą w tym wypadku nie wystarczyć, przykładowo Windowsowy *Windows Update* jest w stanie aktualizować wyłącznie oprogramowanie firmy Microsoft. W celu zidentyfikowania w naszym systemie dziurawych, wymagających aktualizacji aplikacji, polecam darmowy (do użytku domowego) skaner *Secunia Personal Software Inspector*. Po zidentyfikowaniu i ocenieniu poziomu zagrożenia związanego z odnalezionymi lukami, program zaproponuje załatanie każdej z nich, podając bezpośrednie odnośniki do aktualnych wersji oprogramowania lub odpowiednich łatek (Rysunek 3). Znacznie



Rysunek 4. *Program DecaffeinatID wykrył zmianę adresu MAC odpowiadającego adresowi IP bramy, prawdopodobnie oznacza to próbę przeprowadzenia ataku Man in the middle*

uprości to proces przygotowania systemu do stawienia czoła nieznanej sieci.

Zaktualizowaliśmy więc system operacyjny oraz wszelkie zainstalowane aplikacje. Nie straszny więc nam jest już żaden znany exploit. Świetnie, ale co z exploitami typu *Zero-day*? Przecież w trakcie konferencji poświęconej bezpieczeństwu informatycznemu, istnieje całkiem spore prawdopodobieństwo, że z tej samej sieci będzie korzystać specjalista, który niedawno odkrył nową dziurę w systemie operacyjnym lub jakiejś usłudze, stworzył nowy exploit i będzie chciał go przetestować na obecnej publiczności. Prostym rozwiązaniem może się okazać powyłączanie wszelkich serwerów i usług sieciowych pracujących na naszym komputerze przenośnym. Często zdarza się przecież, że informatycy i programiści instalują na swym przenośnym sprzęcie całą masę testowych serwerów: WWW, bazodanowych oraz związanych z różnego rodzaju usługami zarządzania sprzętem i oprogramowaniem. Przed podłączeniem się do nieznanej sieci, należy bezwzględnie powyłączać wszelkie tego typu, niepotrzebne w danym momencie serwery. W celu sprawdzenia, jakie porty zostały otwarte w naszym systemie przez zainstalowane w nim usługi wystarczy wydać proste polecenia: *netstat -a* (w systemach z rodziny Windows) lub *lsof -i* (w systemach z rodziny Linux). Dobrym pomysłem będzie też przeskanowanie portów TCP oraz UDP za pomocą programu *Nmap* uruchomionego z poziomu innej maszyny, przykładowe polecenie może wyglądać następująco: `nmap -p T:0-65535,U:0-65535 adres_IP_sprawdzanego_komputera`. Wszelkie odkryte w ten sposób serwisy należy wyłączyć przed podłączeniem się do obcej sieci. W przypadku jeśli z jakichś względów serwis nie może zostać wyłączony, należy zainstalować wszelkie dostępne dla niego w danej chwili poprawki. Jeśli usługa potrzebna nam jest tylko lokalnie, należy za pomocą zapory ogniowej odfiltrować port tak, by był dostępny wyłącznie z adresu *127.0.0.1* (*localhost*).



Rysunek 5. *Program ARPFreeze pozwala na stworzenie statycznych wpisów w tablicy ARP*

Kolejną kwestią związaną z konfiguracją systemu operacyjnego, na jaką należy zwrócić szczególną uwagę, są udostępnione na przenośnym komputerze udziały sieciowe. Kwestię tę omówię głównie na przykładzie systemów z rodziny Windows, jednak podobny problem może wystąpić w systemach z rodziny Linux (w tym wypadku szczególną uwagę należy zwrócić na konfigurację *Samby* oraz *NFS*).

Być może w ostatnim czasie zdarzyło się, że prywatne zdjęcia zawarte na komputerze przenośnym zostały przeniesione na stacjonarny komputer domowy za pomocą udostępnionego katalogu? W trakcie udostępniania udziału nie martwiliśmy się jednak o żadne zabezpieczenia, w końcu miało to być chwilowe udostępnienie w obrębie naszej sieci domowej. Jednak jeśli zapomnimy o takim udostępnionym bez zabezpieczeń folderze i podłączymy komputer do obcej sieci komputerowej, każdy inny użytkownik tej sieci będzie w stanie pobrać zawartość udostępnionego katalogu. Znane są również przypadki złośliwego oprogramowania rozprzestrzeniającego się właśnie poprzez automatycznie wyszukiwane, niezabezpieczone udziały sieciowe.

Przed podłączeniem się do obcej sieci należy więc koniecznie sprawdzić, co udostępnia nasz komputer oraz odpowiednio zmodyfikować ustawienia systemowe w tym zakresie. W systemach Windows, w tym celu wystarczy uruchomić *Zarządzanie komputerem* (komenda `compmgmt.msc`) i wybrać pozycję *Foldery udostępnione*. Należy zweryfikować wszelkie udziały oraz związane z nimi uprawnienia. Udziały, których nazwa zakończona jest znakiem $, to tzw. udziały administracyjne, czyli takie, do których dostęp mają wyłącznie administratorzy systemu. W przypadku, gdy któreś z kont administracyjnych zabezpieczone jest słabym hasłem, udziały administracyjne stanowią szczególne zagrożenie. Przykładowo domyślnie włączony udział *C$* pozwala na sieciowy dostęp dowolnemu użytkownikowi do całej partycji systemowej *C:*! Przykładowo, polecenie `net use z: \Adres_IP_lub_Nazwa_komputera\C$ /user:administrator hasło_administratora` pozwoli zdalnemu użytkownikowi na zamapowanie całej naszej partycji *C:* jako dysk *Z:* w jego lokalnym systemie. W tym miejscu należy więc przypomnieć o konieczności ustawiania silnych haseł, szczególnie dla kont administracyjnych. Przed podłączeniem komputera do sieci obcej, najbezpieczniejsze będzie jednak zupełne wyłączenie dostępu do wszelkich udziałów. Można to uzyskać wyłączając po kolei każdy udział za pomocą opcji *Zatrzymaj udostępnianie* i/lub wyłączyć wyjątek *Udostępnianie plików i drukarek* w konfiguracji systemowej zapory sieciowej. Można też odinstalować całkowicie protokół *Udostępnianie plików i drukarek w sieciach Microsoft Networks* we właściwościach bieżącego połączenia sieciowego. W celu sprawdzenia konfiguracji udziałów udostępnionych w systemach z rodziny Linux, należy przeanalizować konfigurację zawartą w odpowiednich dla danej dystrybucji plikach konfiguracyjnych, w szczególności w pliku `smb.conf`.

Zabezpieczając własny system, warto również skorzystać z szeregu specjalizowanych aplikacji. Oprócz obowiązkowego oprogramowania antywirusowego oraz zapory sieciowej, istnieje szereg aplikacji dedykowanych do obrony systemów pracujących w skrajnie nieprzyjaznych warunkach. Przykładem takiej aplikacji jest *DecaffeinatID*, prosty system IDS, będący w stanie wykrywać groźne ataki typu *ARP Spoofing* (Rysunek 4). Jest to możliwe dzięki temu, że program monitoruje:

- zmiany w tablicy ARP,
- zdarzenia w logu bezpieczeństwa,
- zdarzenia w logu zapory sieciowej systemu Windows.

Przykładowo, jeśli program zauważy, że adres fizyczny zapamiętany w tablicy ARP dla adresu IP odpowiadającego bramie uległ zmianie, zostanie wyświetlone ostrzeżenie o prawdopodobnie odbywającym się ataku, mającym na celu przechwycenie naszego ruchu sieciowego.

Innym przykładem oprogramowania stworzonego specjalnie z myślą o obronie systemów pracujących w potencjalnie niebezpiecznej sieci, jest *ARPFreeze*. Program ten umożliwia stworzenie statycznej tablicy ARP (Rysunek 5), dzięki czemu uodporni nasz system od ataków zatruwających tablicę ARP i w konsekwencji również od ataków typu *Man in the middle*.

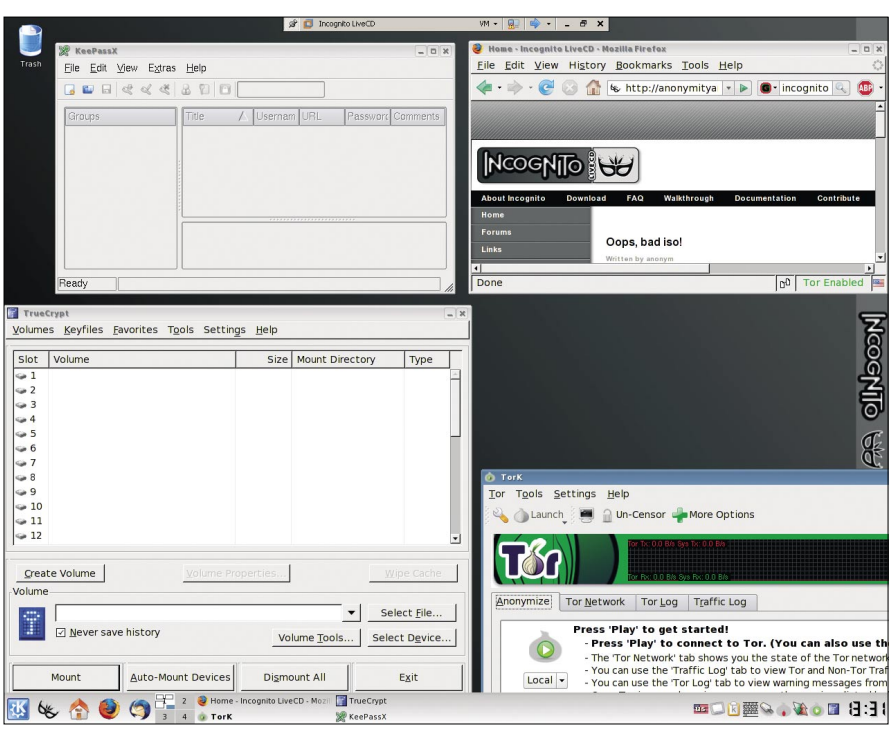
Zamiast łatać i zabezpieczać własny system operacyjny oraz zainstalowane w nim dziesiątki aplikacji i serwisów, można również zastosować zupełnie inną strategię. Można przyjąć zasadę, że w trakcie korzystania z niebezpiecznych obcych sieci, będziemy zawsze korzystać ze specjalnie przygotowanego, super bezpiecznego systemu operacyjnego typu Live CD. Obecnie, najciekawszy tego typu system stanowi specjalistyczna dystrybucja Linuxa – *Incognito*. Jest to dystrybucja, którą można uruchomić bezpośrednio z płyty CD lub pamięci flash, zbudowana na bazie *Gentoo Linux*. Jest to system specjalnie zaprojektowany do bezpiecznego i anonimowego zarazem korzystania z sieci publicznych. Co najciekawsze, istnieje również możliwość uruchomienia wirtualnej instancji tegoż systemu bezpośrednio pod systemem operacyjnym Windows. Jest to możliwe, dzięki zintegrowaniu dystrybucji z emulatorem o otwartym kodzie – *QEMU*. Wszystkie aplikacje sieciowe zawarte w tej dystrybucji, takie jak przeglądarki internetowe, klienty pocztowe, programy IM, itd. natychmiast po uruchomieniu systemu są już specjalnie skonfigurowane. Każde połączenie wychodzący będzie anonimizowane z wykorzystaniem sieci Tor. Należy pamiętać, że wykorzystanie sieci Tor zapewnia wyłącznie wysoki stopień anonimowość, jednak nie oferuje w żadnym razie szyfrowania połączeń. System *Incognito* został jednak wyposażony w szereg dodatkowych narzędzi oferujących szyfrowanie, takich jak program *GnuPG*, pozwalający na szyfrowanie poczty elektronicznej. Stosowanie tego systemu operacyjnego może znacząco zwiększyć nasze bezpieczeństwo w trakcie korzystania z nieznanej nam sieci. Warto również zwrócić uwagę, że ta dystrybucja Linuksa pozwala również na obchodzenie mechanizmów filtracji (filtracji URL, filtracji IP, itp.) treści. Jeśli więc w danej sieci korzystanie z pewnych zasobów internetowych jest zabronione, *Incognioto* prawdopodobnie umożliwi nam dostęp do wszystkich zasobów.

Po zbudowaniu systemu operacyjnego – twierdzy, nasza strategia *Defens in Depth*, jest już niemal kompletna. Zbudujmy jednak jeszcze ostatnią linię obronną – zabezpieczmy dodatkowo same dane, tak by nawet ich przejęcie, nie dało intruzowi najmniejszych korzyści.

Pancerne dane

W przypadku gdyby wszystkie dotychczas omówione linie obronne zostały przełamane przez intruza i nasze dane dostałyby się w niepowołane ręce, sprawmy by nasze pliki stały się jednocześnie ostatnią linią obrony. Wszelkiego rodzaju dane można, zazwyczaj stosunkowo prostymi metodami zabezpieczyć tak, że praktycznie każdy intruz połamie sobie na nich zęby.

Praktycznie wszystkie programy, których używamy na co dzień, generują domyślnie dane niezabezpieczone w żaden sposób. Przejęcie takiego dokumentu przez osoby trzecie pozwala więc na swobodny odczyt, modyfikację i dalsze rozpowszechnianie cudzych plików. Większość użytkowników zdaje sobie przecież sprawę z tego, że dzisiejsze aplikacje są wyposażone w najrozmaitsze opcje zabezpieczania danych, zazwyczaj poprzez ich szyfrowanie, jednak mało kto korzysta z tej funkcjonalności. Możemy szyfrować (korzystając z funkcjonalności samego oprogramowania lub łatwo dostępnych rozszerzeń) dane tworzone przez najpopularniejsze pakiety biurowe, pliki w formacie PDF, pliki zawierające bazy danych i wiele innych. Wystarczy tylko odnaleźć odpowiednią opcję w używanym przez nas programie lub doinstalować odpowiednią wtyczkę. Jeśli opcja szyfrowania jest rozbudowana o opcje wyboru algorytmu szyfrującego oraz długości klucza, warto poświęcić chwilę na dokonanie odpowiedniego



Rysunek 6. *Środowisko systemu Incognito zostało przez twórców skonfigurowane do bezpiecznej i anonimowej pracy w dowolnej sieci komputerowej*

wyboru. Często zdarza się tak, że program domyślnie oferuje bardzo słaby algorytm szyfrujący. Przykładowo w oprogramowaniu Microsoft Word oraz Excel w wersjach 97-2003, domyślnie stosowane jest bardzo słabe szyfrowanie z kluczem zaledwie 40-bitowym. Stworzono więc oprogramowanie (np. *Elcomsoft Advanced Office Password Breaker*), które jest w stanie rozszyfrować każdy taki zaszyfrowany domyślnym algorytm plik. Długość hasła oraz jego złożoność nie mają w tym wypadku najmniejszego znaczenia, gdyż program sprawdza każdą z możliwych (240 możliwości) kombinacji klucza. Nowoczesny pecet jest w stanie przejrzeć wszystkie możliwości już nawet w ciągu 24 godzin. Należy więc zawsze wybierać spośród dostępnych algorytmów szyfrowania te najbardziej bezpieczne. Obecnie, jednym z najbezpieczniejszych jest przykładowo algorytm AES z 256-bitowym kluczem. Należy również zawsze stosować długie i skomplikowane hasła, gdyż większość pozostałych metod otwierania zaszyfrowanych plików opiera się na sprawdzaniu wszystkich możliwych kombinacji hasła.

Warto również zastanowić się nad szyfrowaniem korespondencji przesyłanej za pomocą poczty elektronicznej. W tym przypadku możemy wykorzystać, dostępny w formie dodatku dla większości najpopularniejszych programów pocztowych, program *Pretty Good Privacy* (PGP, pol. całkiem niezła prywatność). PGP pozwala szyfrować i deszyfrować wiadomości poczty elektronicznej, podpisywać je cyfrowo oraz weryfikować tożsamość nadawcy (pod warunkiem, że ten także korzysta z PGP).

W trakcie korzystania z nieznanej nam sieci, można również rozważyć szyfrowanie rozmów VoIP. Program Zfone, który jest dostępny w postaci dodatków do wielu popularnych programów umożliwiających rozmowy VoIP (X-Lite, Gizmo, XMeeting, Google Talk VoIP, Yahoo Messenger's VoIP client, Magic Jack i inne) zabezpiecza przeprowadzane rozmowy za pomocą protokołu ZRTP. Program ten nie wspiera niestety protokołu Skype, który nie został nigdy oficjalnie upubliczniony.

Dane zabezpieczone odpowiednio silnymi algorytmami szyfrującymi, będą dla intruza bezużyteczne, warto więc wyrobić sobie nawyk szyfrowania najważniejszych plików. Szyfrowanie plików stanowi ostatni element wielowarstwowej strategii obronnej, jaką proponuję przyjąć w trakcie korzystania z niebezpiecznych sieci publicznych.

Podsumowanie

Czytelnik może dojść do wniosku, że zaproponowana strategia wymaga zbyt wiele zachodu i jest zbyt skomplikowana, by można ją było stosować przy każdej okazji korzystania z zasobów informatycznych nieznanej nam sieci. Jest to jednak przekonanie błędne. Po pierwsze, bezpieczeństwo naszych prywatnych lub firmowych danych jest warte tego zachodu. Po drugie, przygotowanie *pancernego* systemu wystarczy wykonać tylko raz, a potem należy już tylko dbać o jego aktualność i stosować się do przedstawionych zasad bezpiecznego korzystania z obcych sieci. Zaproponowana procedura, zainspirowana strategią *Defence in Depth* jest naprawdę skuteczna i prawidłowo wykonana, zapewni niemal stuprocentowe bezpieczeństwo naszych danych. Jednoczesne przełamanie wszystkich pięciu warstw ochronnych, jakie utworzymy wokół naszych danych jest, nawet dla wytrawnego crackera, praktycznie niemożliwe. Jest wielce prawdopodobne, że włamywacz napotykając na kolejne zabezpieczenia, po prostu obierze sobie za cel jakiś inny, słabiej zabezpieczony system.

Na koniec chciałbym wspomnieć o zupełnie odmiennej metodzie zapewniającej bezpieczną pracę w sieci obcej. Jeśli tylko dysponujemy możliwością wykonania połączenia typu *remote vpn* do sieci (domowej lub firmowej), w której będziemy mogli zdalnie zalogować się do jakiegoś komputera, takie rozwiązanie może z powodzeniem zastąpić naszą rozbudowaną strategię obronną. Jeśli uda nam się utworzyć bezpieczny tunel do zdalnego komputera i na nim pracować, to potencjalny intruz nasłuchujący w sieci obcej będzie w stanie wyłącznie przechwycić transmisję szyfrowaną, a my pozostaniemy w pełni bezpieczni.

W Sieci

- *http://hcsl.pl/* - Hard – Hard Core Security Lab,
- *http://www.cert.org/* – Computer Emergency Response Team,
- *http://www.remote-exploit.org/backtrack.html* – BackTrack,
- *http://www.wallofsheep.com/* – Wall of Sheep project,
- *http://www.usatoday.com/tech/conventions/2005-08-01-hacker-conference_x.htm* – Hackers demonstrate their skills in Vegas,
- *http://pl.kensington.com/* – Oficjalna strona firmy Kensington,
- *http://www.truecrypt.org/* – Strona domowa projektu TruCrypt,
- *http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf* – Wireless Network Security 802.11, Bluetooth and Handheld Devices,
- *http://secunia.com/vulnerability_scanning/personal/* – Secunia Personal Software Inspector,
- *http://www.irongeek.com/i.php?page=security/decaffeinatid-simple-ids-arpwatch-for-windows* – DecaffeinatID: A Very Simple IDS,
- *http://www.irongeek.com/i.php?page=security/arpfreeze-static-arp-poisoning* – ARPFreeze: A tool for Windows to protect against ARP poisoning,
- *http://anonymityanywhere.com/incognito/* – Incognito Live CD,
- *http://www.torproject.org/* – Tor on-line,
- *http://www.elcomsoft.com/* – ElcomSoft Co.Ltd.,
- *http://www.pgpi.org/* – The International PGP Home Page,
- *http://zfoneproject.com/* – The Zfone Project,
- *http://www.irongeek.com/* – Irongeek.

Wojciech Smol
Autor jest absolwentem wydziału Automatyki, Elektroniki i Informatyki Politechniki Śląskiej w Gliwicach. Ukończył studia na kierunku informatyka, o specjalności Bazy danych, sieci i systemy komputerowe. Pracuje jako administrator sieci i systemów komputerowych w firmie Mostostal Zabrze Holding S.A.
Kontakt z autorem: *wojciech.smol@mz.pl* lub *wojciech.smol@gmail.com*.
Strona domowa autora: *http://hcsl.pl/*.