Technologie informacyjne
przed 4 wykładem

Andrzej Giniewicz

25.03.2025

Dziś zajmiemy się podstawami naszego bezpieczeństwa w sieci.

1 Szyfrowanie i klucze

Szyfrem lub algorytmem szyfrującym będziemy nazywali ciąg operacji matematycznych, które mają na celu zapewnienie bezpieczeństwa, autentyczności i prywatności danych. Informacje, czyli tekst lub inne dane, reprezentowane jako ciągi liczb, przekształcone przez wybrany szyfr, nazywamy zaszyfrowanymi informacjami. Proces stosowania funkcji odwrotnej do funkcji szyfrującej, nazywa się deszyfrowaniem i pozwala odczytać oryginalne informacje. Aby informacja mogła być odczytana, należy wiedzieć, za pomocą jakiej funkcji została zaszyfrowana. Próbę odgadnięcia lub wyznaczenia funkcji szyfrującej, będziemy nazywać łamaniem szyfru. Jeśli o szyfrze myślimy jak o funkcji f, odszyfrowywanie będzie funkcją f^{-1}. W przykładzie poniżej informacja x zostaje zaszyfrowana do informacji y, która zostaje ponownie odszyfrowana do informacji x

$$y = f(x), \quad x = f^{-1}(y).$$

Dobre szyfry najczęściej mają następujące cechy:

- złamanie szyfru na obecnie dostępnych superkomputerach zajmuje niepraktycznie dużo czasu, np.: tysiące lat;
- zaszyfrowane dane przypominają losowy ciąg, co utrudnia znalezienie wzorców;
- zaszyfrowane dane nie pozwalają odgadnąć technologii, w której zostały zaszyfrowane.

Użyteczność funkcji szyfrującej, która nie ma parametrów, byłaby ograniczona, ponieważ wszystkie osoby znające tę funkcję mogłyby odczytać wszystkie wiadomości zaszyfrowane za jej pomocą. W tym celu zwykle wprowadza się parametr do funkcji szyfrującej, nazywany kluczem. Istnieją dwa rodzaje kluczy. Pierwszy rodzaj to klucze symetryczne, które pozwalają zarazem zaszyfrować, jak i odszyfrować wiadomość. Każda osoba znająca klucz

i metodę szyfrowania może odszyfrować i zaszyfrować wiadomość. Jeśli k to parametr oznaczający klucz, algorytm szyfrowania wykorzystujący klucz symetryczny możemy zapisać następująco

$$y = f(x,k), \quad x = f^{-1}(y,k).$$

Oznacza to, że osoba szyfrująca zna algorytm szyfrowania f, dane x i klucz k. Na ich podstawie wylicza zaszyfrowaną wiadomość y do innej osoby. Osoba ta, jeśli zna algorytm szyfrowania f i klucz k, może wiadomość odszyfrować. Zaletą tej metody jest to, że nawet jeśli zaszyfrowane dane y i metoda szyfrowania f wpadnie w niepowołane ręce, bez klucza k wciąż nie da się odczytać wiadomości.

Drugim sposobem szyfrowania jest klucz asymetryczny. W tym przypadku klucz do szyfrowania i odszyfrowywania wiadomości jest inny. Klucz do szyfrowania wiadomości nazywamy kluczem publicznym, natomiast klucz do deszyfrowania prywatnym. Jeśli klucz publiczny oznaczymy przez k_p, natomiast prywatny przez k_a, to schemat szyfrowania wygląda następująco

$$y = f(x,k_p), \quad x = f^{-1}(y,k_a).$$

Skąd nazwy kluczy: publiczny i prywatny? Zwykle klucz publiczny jest dystrybuowany do wielu osób, aby mogły zaszyfrować wiadomość, której adresatem jest konkretna osoba. Choć zaszyfrować wiadomość może wiele osób, to odczyta ją tylko ta, która ma klucz prywatny. Dlatego ważne jest, aby klucza prywatnego nie udostępniać nikomu.

Odwrotne wykorzystanie funkcji f, w którym y jest wiadomością, którą szyfrujemy za pomocą algorytmu f^{-1} oraz klucza prywatnego k_a, nazywamy podpisem cyfrowym wiadomości y. Podpis cyfrowy może zweryfikować każda osoba, która posiada odpowiedni klucz publiczny. Podsumowanie kluczy asymetrycznych znajduje się w tabeli poniżej.

	klucz publiczny	klucz prywatny
kto ma	im więcej tym lepiej	tylko jedna osoba
szyfrowanie	pozwala coś zaszyfrować	pozwala coś odszyfrować
podpis cyfrowy	pozwala sprawdzić podpis	pozwala coś podpisać

Istnieje wiele standardów szyfrowania, zarazem symetrycznego, jak i asymetrycznego. W przypadku podpisu asymetrycznego bardzo ważnym procesem jest weryfikacja poprawności klucza publicznego. Jeśli ktoś udostępni nam klucz publiczny i uwierzymy, że należy od danej osoby, każda wiadomość podpisana przez tę osobę, będzie zweryfikowana jako prawidłowa. Co jednak się stanie, jeśli uwierzymy, że klucz do kogoś należy, a w rzeczywistości został wygenerowany przez oszusta? W Internecie są tysiące a może i setki tysięcy kluczy publicznych podpisanych imionami i nazwiskami sławnych ludzi. Skąd mamy wiedzieć, który z tysięcy dostępnych Billów Gatesów jest tym prawdziwym? W praktyce wykorzystuje się dwa sposoby na sprawdzenie autentyczności kluczy:

- za pomocą urzędów certyfikacji,
- za pomocą sieci zaufania.

Sprawdzanie kluczy za pomocą urzędów certyfikacji jest bezpieczniejsze, ale bardziej kosztowne. Jest wykorzystywane tam, gdzie autentyczność podpisu jest bardzo ważna. Jednym ze standardów certyfikacji kluczy publicznych jest X.509. Jest to popularny standard, wykorzystywany między innymi do podpisu cyfrowego dokumentów w platformie ePUAP służącej do załatwiania spraw urzędowych w Polsce z wykorzystaniem tak zwanego profilu zaufanego. Certyfikacja wymaga weryfikacji tożsamości w urzędzie lub w inny pewny sposób (na przykład poprzez bank). Jednostka weryfikująca tożsamość następnie podpisuje klucz publiczny petenta. Jeśli otrzymamy od kogoś klucz publiczny, pobieramy klucz publiczny urzędu certyfikującego, dzięki czemu możemy sprawdzić podpis urzędu umieszczony pod otrzymanym kluczem publicznym i mieć pewność, że jest to ta osoba, za którą ktoś się podaje.

Do sprawdzania podpisów w wiadomościach e-mail nie stosuje się zwykle podpisów wystawianych przez urzędy certyfikacji, ponieważ koszt utrzymania takiego systemu byłby ogromny. Najczęściej używanym standardem do podpisywania i szyfrowania wiadomości o mniejszym znaczeniu strategicznym, jest standard OpenPGP. Jest to klasyczny przykład systemu opartego na sieci zaufania. Sieć zaufania to graf, w którym wierzchołkami są klucze, natomiast krawędzie informują nas o tym, że właściciel jednego klucza potwierdza autentyczność innego klucza. Krawędzie w grafie są skierowane, co oznacza, że zaufanie nie jest relacją symetryczną. Możemy komuś ufać, ale to nie znaczy, że on ufa nam. Wyróżnia się cztery poziomy zaufania, w stosunku do właścicieli kluczy.

1. Nieznane — wtedy nie wiadomo, czy osoba posługująca się kluczem, jest tym, za kogo się podaje. Jest to wartość domyślna dla nowego klucza;
2. Brak — wiemy, że właściciel klucza czasem podpisuje niezaufany klucz;
3. Częściowe — wiemy, że właściciel klucza rozumie konsekwencje wynikające z tego, że podpisuje czyjś klucz i sprawdza klucze przy podpisywaniu;
4. Pełne — wiemy, że właściciel bardzo dobrze zna koncepcje podpisywania kluczy i ufamy mu tak samo, jak sobie.

Klucz osoby B będziemy nazywać w pełni poprawnym dla osoby A, jeśli spełniony jest jeden z 3 warunków:

1. osoba A sama podpisała klucz osoby B,
2. istnieje ścieżka długości nie więcej niż 5 w sieci zaufania pomiędzy A i B taka, że wszystkie klucze są w niej w pełni zaufane,
3. istnieją trzy ścieżki długości nie więcej niż 3 w sieci zaufania pomiędzy A i B takie, że wszystkie klucze są w niej przynajmniej częściowo zaufane.

Jeśli spełniony jest warunek 3 powyżej, ale dla mniejszej liczby ścieżek, klucz nazywamy częściowo poprawnym. Klucze publiczne wraz z podpisami dystrybuowane są na serwery kluczy, aby każdy mógł sprawdzić, czy klucz danej osoby znajduje się w tej samej sieci zaufania, co jego. Niekiedy organizowane są wydarzenia polegające na tym, że osoby chcące potwierdzić swoją tożsamość spotykają się w jakimś miejscu i podpisują swoje klucze.

Angielska nazwa takiego wydarzenia to *key signing party*. Istnieje możliwość integracji systemu podpisów z przeglądarką poprzez dodatki do popularnych przeglądarek (na przykład Mailvelope) oraz dodatki do popularnych klientów pocztowych (na przykład Enigmail dla starszych wersji klienta Thunderbird) lub odpowiedniego klienta poczty (na przykład Thunderbird w wersji 78 lub nowszej).

Niezależnie od przyjętej zasady weryfikacji kluczy publicznych, należy pamiętać, aby:

- nigdy nikomu nie udostępniać swojego klucza prywatnego,
- nie przesyłać klucza prywatnego przez środki komunikacji przechowujące kopię wiadomości, na przykład e-mail, komunikatory, itp,
- nigdy nikomu nie podpisywać klucza, jeśli nie jesteśmy pewni jego tożsamości.

Stosowanym od niedawna rozwiązaniem, zyskującym dużą popularność, są sprzętowe klucze 2FA, które wspierają wiele różnych standardów w tym opisany SSH oraz OpenPGP. Posiadają one dodatkowe zabezpieczenia, które uniemożliwiają wykradzenie klucza prywatnego w inny sposób niż fizyczna kradzież klucza sprzętowego. Daje to dodatkowy poziom bezpieczeństwa, również do różnego rodzaju stron i aplikacji, które je wspierają, takich jak wiele interfejsów do serwerów poczty elektronicznej, portali tematycznych lub sieci społecznościowych. Jeśli zaczniemy korzystać z PGP warto też rozejrzeć się za dostawcą poczty e-mail, który takie rozwiązanie wspiera, dzięki czemu nasza poczta może być szyfrowana.

2 Protokół HTTPS

Protokół HTTPS jest bezpieczną, szyfrowaną wersją protokołu HTTP. Gdy przesyłamy dane przez protokół HTTP, na przykład login i hasło do banku, mogą one zostać przechwycone i odczytane przez osoby trzecie. Protokół HTTPS wykorzystuje szyfrowanie, aby temu zapobiec.

Jeśli twórca strony chce udostępniać szyfrowane połączenie, zgłasza się do dostawcy certyfikatu SSL. Dostawca certyfikatu weryfikuje w wersji minimum, czy dana osoba rzeczywiście zarządza domeną o podanym adresie. Takie certyfikaty nazywamy certyfikatami DV (ang. Domain Validation). Można też wystąpić o wersję certyfikatu dodatkowo potwierdzającą tożsamość firmy (OV, ang. Organization Validation), naszą tożsamość (IV, ang. Individual Validation) oraz rozszerzoną, co wiąże się z wyższą kwotą i ręczną weryfikacją wymagającą bezpośredniego kontaktu. Certyfikaty o rozszerzonej weryfikacji nazywają się EV (ang. Extended Validation). Częścią certyfikatu jest domena, której certyfikat dotyczy, dane osobowe, dane dostawcy certyfikatu, klucz publiczny danej firmy oraz inne dane, takie jak okres ważności. Wszystkie te informacje są podpisane cyfrowo przez dostawcę certyfikatu.

Gdy wchodzimy na stronę przez HTTPS, dzieją się następujące rzeczy:

1. Nasza przeglądarka informuje serwer, jakie wersje szyfrowania wspiera oraz wysyła do serwera losową, znaną sobie liczbę;

2. Serwer z puli dostępnych wersji szyfrowania wybiera najlepszą obsługiwaną przez siebie i odpowiada, przesyłając do przeglądarki wersję szyfrowania, certyfikat SSL oraz losową wybraną przez siebie i zapamiętaną liczbę;

3. Nasza przeglądarka sprawdza podpis pod certyfikatem z bazą znanych i zaufanych dostawców certyfikatów — baza ta jest częścią przeglądarki i jest aktualizowana z każdą aktualizacją przeglądarki. Jeśli podpis się zgadza, sprawdzana jest domena oraz data ważności zapisana w certyfikacie. Jeśli coś się nie zgadza, jesteśmy informowani, że połączenie nie jest bezpieczne;

4. Nasza przeglądarka losuje kolejną liczbę, tak zwany sekret. Sekret jest szyfrowany przy pomocy klucza publicznego serwera, który jest prawidłowo podpisany przez dostawcę certyfikatu. Sekret po przesłaniu, jest odszyfrowywany przez serwer jego kluczem prywatnym.

5. Teraz i przeglądarka i serwer mają trzy informacje: po jednej losowej liczbie wysłanej na początku transmisji oraz sekret. Z tych trzech informacji oba urządzenia wyliczają klucz sesji, który sam w sobie nie jest przekazany przez Internet;

6. Komunikacja pomiędzy przeglądarką a serwerem odbywa się dalej za pomocą szyfrowania symetrycznego z wyliczonym kluczem sesji.

Jak widać, do szyfrowania jest użyty algorytm symetryczny, ale aby ustalić klucz szyfrowania symetrycznego, stosowane jest szyfrowanie asymetryczne i podpisy cyfrowe z urzędem certyfikacji pomiędzy.

Bardzo ważne jest, aby nie akceptować wyjątków w certyfikatach. Jeśli otrzymamy od przeglądarki informację o tym, że certyfikat nie jest ważny, możemy kontynuować na własną odpowiedzialność, ale pamiętajmy, że ktoś może podszywać się pod dostawcę danej usługi. Jeśli zobaczymy ostrzeżenie od przeglądarki mówiące, że certyfikat nie jest ważny, otwórzmy go, sprawdźmy jego dane i odezwijmy się do administratora strony. Najczęściej możemy sprawdzić, kto nim jest, używając komendy `whois` lub stosując różnego rodzaju bazy firm i książki telefoniczne.

Do niedawna certyfikaty były kosztowne. Dziś każdy może poprosić o certyfikat SSL z weryfikacją domeny (certyfikat DV) i otrzymać go za darmo. Inicjatywa oraz narzędzia służące do uzyskania takiego certyfikatu nazywa się *Let's Encrypt*. Ze względu na powszechność certyfikatów, trwają rozważania nad uniemożliwieniem łączenia się ze stronami internetowymi, które nie posiadają certyfikatu, choćby wydanego przez *Let's Encrypt* lub dowolnego innego dostawcę. Musimy pamiętać, że ma to zalety oraz wady. Po pierwsze, część stron się nie dostosuje i może zniknąć z powierzchni Ziemi, a raczej stać się niedostępna, po drugie darmowy certyfikat stanie się nowym brakiem certyfikatu, czyli zaufanie do certyfikatów wystawionych przez *Let's Encrypt* będzie raczej niskie. Oprócz tych wad dużą zaletą takiego rozwiązania jest to, że nawet słabo weryfikowany certyfikat od *Let's Encrypt* zapewnia mocne szyfrowanie, o wiele trudniej więc będzie przeprowadzić wiele rodzajów cyber-ataków. Tymczasem, warto sprawdzać, przez kogo został wystawiony certyfikat. Bank raczej nie będzie miał swoich kluczy podpisanych przez tego dostawcę, więc pomimo „kłódki" w pasku adresu, warto się zastanowić przed wpisaniem swojego hasła.

3 Rodzaje ataków

Niekiedy zdarza się, że osoby trzecie przeprowadzają na nas atak mający na celu niepożądane działanie. Wyróżniamy cztery główne rodzaje ataków:

1. rekonesans,
2. uzyskanie dostępu,
3. odmowa usługi,
4. infekcja.

Rekonesans polega na skanowaniu sieci w poszukiwaniu słabych punktów oraz na podsłuchiwaniu. Może służyć do kradzieży informacji lub umożliwienia dalszych ataków. Ofiarami takiego rodzaju ataków najczęściej padają serwery udostępniające usługi w sieci, przy czym im więcej usług jest „wystawionych na świat", tym łatwiej znaleźć w nich jakąś lukę. Serwery to jednak nie jedyny cel rekonensansu — ofiarą może paść nasz komputer, nasze urządzenie mobilne, nasz router bezprzewodowy lub inny punkt dostępowy do WiFi albo co ciekawe, również urządzenia inteligentnego domu i komputery pokładowe samochodów. Każde urządzenie jakkolwiek połączone z siecią jest narażone. Co robić, by się bronić przed tym rodzajem ataku? Poniżej kilka rad.

1. Stosujmy mocne hasła. Hasło do routera WiFi jest jednym z ważniejszych haseł w waszych domach.
2. Wykonujmy aktualizacje systemu operacyjnego na wszystkich urządzeniach[1], w tym na routerach (proces ten jest opisany w instrukcji urządzenia).
3. Nie udostępniajmy usług, których nie musimy udostępniać.

Uzyskanie dostępu jest kolejnym rodzajem ataku. Jego ofiarą najczęściej padają usługi internetowe, czyli różnego rodzaju portale. Atak może odbyć się poprzez złamanie lub podsłuchanie hasła. Innym popularnym rodzajem ataku mającym na celu uzyskanie dostępu jest atak typu „man in the middle", w którym atakujący sprawia, że pakiety wędrują przez jego komputer, zanim trafią we właściwe miejsce. Tego typu atak często jest wykonywany w kawiarniach i restauracjach. Innym rodzajem ataku jest „phishing", w którym rozsyłane są e-maile łudząco przypominające na przykład e-maile z Poczty Polskiej, informujące o konieczności zapłaty cła za przesyłkę. Bądźmy bardzo uważni na wiadomości przychodzące. Nie każdy otrzyma spadek od księcia egzotycznego kraju[2]. Co robić, aby bronić się przed tym rodzajem ataku? Poniżej kilka rad.

[1] Przypominam, że jako studenci Politechniki Wrocławskiej mogą Państwo pobrać najnowszą wersję systemu Windows z programu Microsoft Azure `https://wmat.pwr.edu.pl/studenci/studia/oprogramowanie/microsoft-azure`. Nowe wersje systemu Linux zawsze można sprawdzić na stronie `https://distrowatch.com/` lub na stronie swojej dystrybucji. Najnowsza wersja systemu macOS jest dostępna z firmy Apple o ile kwalifikujemy się do darmowej aktualizacji.

[2] Nie wszystkie phishingi są beznadziejnie głupie — czasem na uczelniach pojawiają się realnie wyglądające maile o konferencjach.

1. Stosujmy mocne, różne hasła. Nie używajmy tego samego hasła na różnych portalach. Zastanówmy się nad zastosowaniem menadżera haseł, który będzie pamiętał je za nas.

2. Starajmy się nie korzystać z Internetu w otwartych sieciach, takich jak hotspoty w restauracjach i innych miejscach publicznych. Możliwe, że ktoś ustawił taką samą nazwę punktu dostępowego, jak właściciel, a w rzeczywistości siedzi dwa stoliki dalej i czeka na łowy. Jeśli już musimy skorzystać z sieci, używajmy tylko protokołu HTTPS.

3. Czytajmy strony informujące o wyciekach danych, na przykład portale takie, jak `https://niebezpiecznik.pl/`. Jeśli z jakiejś firmy wycieką dane, natychmiast zmieńmy hasło i sprawdźmy, czy konieczne są dodatkowe działania, na przykład blokada karty płatniczej lub zastrzeżenie dokumentu.

4. Jeśli otrzymamy podejrzany e-mail, skontaktujmy się z potencjalnym nadawcą w inny sposób. Dokładnie sprawdźmy też adres, z którego wysłana jest wiadomość.

Odmowa usługi jest rodzajem ataku, w którym powodujemy, że dostęp do usługi będzie niemożliwy. Najczęściej odbywa się to poprzez zmasowany ruch sieciowy z różnych źródeł — zasoby komputera serwera zostaną przez to wyczerpane i nie będzie mógł odpowiadać na właściwe zapytania. Taki rodzaj ataku nazywa się DDoS (ang. Distributed Denial of Service). Istnieją całe farmy botów, które wykonują takie ataki. Najczęściej ofiarą takich ataków padają duże serwisy internetowe, ale nie tak dawno mógł paść jego ofiarą każdy — poprzez bramkę SMS. Atakujący pisał skrypt, który z różnych darmowych bramek internetowych, wysyłał tysiące SMSów na jeden numer. Może to spowodować oprócz notorycznie zapchanej skrzynki, której nie nadążamy kasować, zapchanie sieci. Przed tego rodzaju atakiem jako osoby fizyczne nie musimy się bronić, ale warto mieć świadomość jego istnienia, ponieważ może się zdarzyć, że to nam jakaś strona odmówi usługi.

Ostatnim rodzajem ataku jest infekcja. Atakujący po uzyskaniu dostępu lub poprzez naruszenie zaufania, może spowodować, że na komputerze pojawi się złośliwe oprogramowanie. Może to być na przykład wirus lub koń trojański. Jeśli oprogramowanie takie zostanie niezauważone, będzie śledzić nasze ruchy w sieci. Często może też spowodować, że nasz komputer będzie wykorzystywany do dalszego rozpowszechniania złośliwego oprogramowania w sieci lub jako furtka do kolejnych ataków. Co robić, aby bronić się przed tym rodzajem ataku? Poniżej kilka rad.

1. Wykonujmy aktualizacje systemu operacyjnego i całego używanego oprogramowania, szczególnie używanego do korzystania z sieci.

2. Zainstalujmy sprawdzony program antywirusowy i dbajmy o regularną aktualizację samej aplikacji antywirusa i bazy wirusów. Jeśli program dostarcza dodatek do przeglądarki, włączmy go. Nigdy nie instalujmy więcej niż jednego antywirusa. Jeśli zamierzamy zmienić program antywirusowy, najpierw odinstalujmy stary, potem zainstalujmy nowy — bazy wirusów mogą być rozpoznane jako złośliwe oprogramowanie.

3. Skanujmy antywirusem wszystkie pobrane pliki, ręcznie lub automatycznie, zależnie od dostępnych opcji. Raz na miesiąc wykonujmy skanowanie systemu w poszukiwaniu wirusów.

4. Wybierzmy system operacyjny, na którym zainfekowanie jest trudne.

5. Nie korzystajmy z konta administratora, jeśli nie ma takiej potrzeby — załóżmy konto zwykłego użytkownika, który ma mniejsze uprawnienia, więc ewentualny wirus mniej „popsuje".

6. Obserwujmy komputer w poszukiwaniu nietypowego i niestandardowego zachowania, którego nie widzieliśmy wcześniej.

7. Przed kliknięciem linku w wiadomości e-mail sprawdźmy, czy e-mail pochodzi od tej osoby, za którą podaje się autor wiadomości. Sprawdźmy dokładnie adres oraz wszelkie elementy, które mogą sugerować kradzież tożsamości lub podszywanie się pod kogoś. Jeśli ktoś stosuje podpis cyfrowy, sprawdzajmy zawsze jego poprawność.

4 Zdalne logowanie i przekierowanie ruchu

Kolejnym obok HTTPS i podpisów cyfrowych zastosowaniem kluczy jest zdalne logowanie. Na zajęciach będziemy korzystać ze standardu OpenSSH. Jest to system kluczy asymetrycznych, w którym na zdalnym komputerze umieszcza się klucz publiczny, a klucz prywatny pozostawia na komputerze lokalnym. Korzystając z tego protokołu, można zalogować się na zdalny komputer bez podawania hasła do konta. Zwykle natomiast zakłada się hasło na klucz prywatny, aby choć w minimalny sposób zabezpieczyć połączenie na wypadek wykradnięcia lub wycieku klucza prywatnego. Jest to system, z którego będziemy wielokrotnie korzystać na zajęciach.

SSH oprócz logowania do powłoki tekstowej pozwala na inne funkcje, na przykład przekierowanie portów oraz tunelowanie. Przekierowanie portów to jedna z metod udostępniania portów usług na routerach, poprzez przesłanie ruchu z portu routera na inny port innej maszyny do niego podłączonej. Tunelowanie pozwala ustawić pośrednika pomiędzy komputerem lokalnym a zdalnym, dzięki czemu zdalny komputer widzi adres IP i możliwości pośrednika, a nie naszego komputera lokalnego. Tunelowanie pozwala przekierować ruch konkretnej aplikacji, jego konfiguracja jest więc nieco trudniejsza, niż w przypadku alternatyw, którą jest na przykład VPN.

Jeśli możliwość tunelowania SSH jest niewystarczająca, warto zastanowić się nad skorzystaniem z serwera VPN, który cały ruch sieciowy kieruje poprzez inną maszynę, łącząc się z nią w sposób bezpieczny. Jeśli VPN ma zapewniać bezpieczeństwo, powinien to być własny serwer VPN, który stosunkowo łatwo uruchomić we własnym mieszkaniu, za pomocą mikrokontrolera Raspberry Pi oraz darmowych narzędzi typu PiHole oraz PiVPN. Dzięki temu mamy pewność, że ruch sieciowy jest tak samo bezpieczny, jak nasza sieć domowa. Jeśli korzystamy z innych serwerów VPN, musimy ufać dostawcy tej usługi — nasze połączenie jest wtedy tak zaufane, jak ufamy pośrednikowi, przez którego przesyłamy komplet

danych. Nieuczciwy lub słabo zabezpieczony dostawca VPN to umożliwienie ataku typu „man in the middle" na nasze własne życzenie. Zastosowanie serwerów VPN nie ogranicza się jednak do bezpieczeństwa. Często stosowane są, aby obejść ograniczenia regionalne narzucone na różne strony, sklepy lub platformy streamingowe. Jeśli ruch przechodzi przez serwer VPN w USA, zapytania do strony będą wyglądać, jakby pochodziły z USA, przez co wyświetli się strona przeznaczona dla tego właśnie regionu. Każdorazowo należy jednak rozpatrzeć legalność takiego postępowania — zależy ona od warunków korzystania z serwisu. Przy takim rozwiązaniu wciąż można zainstalować na komputerze własny serwer VPN, najpopularniejszym rozwiązaniem są wtedy kupowane u różnych dostawców wirtualne serwery (tak zwane VPS, „Virtual Private Serwer"), na których można zainstalować dowolne oprogramowanie. Jakiekolwiek ustawienia serwerów VPN są na poziomie systemu operacyjnego, oznacza to, że nie tylko przeglądarka, ale wszystkie programy, będą mogły korzystać z bezpiecznego połączenia.