Firewall nie powstrzyma prawdziwego smoka, czyli jak zadbać o cyberbezpieczeństwo

Przewodnik dla niefachowców

—

Wydanie III

Carey Parker

Helion

Apress

Tytuł oryginału: Firewalls Don't Stop Dragons:
A Step-by-Step Guide to Computer Security for Non-Techies, 3rd Edition

Tłumaczenie: Paweł Borkowski

ISBN: 978-83-283-5569-9

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/firsm3
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

ROZDZIAŁ 2

Fundamenty bezpieczeństwa cybernetycznego

Zanim przejdziemy do zagadnień bezpieczeństwa, musimy zdefiniować kilka podstawowych pojęć i terminów komputerowych. *Nie musisz* uczyć się ich na pamięć i nic się nie stanie, jeżeli pominiesz niektóre partie tego rozdziału. Na końcu książki znajduje się słowniczek, do którego możesz sięgnąć w razie nagłej potrzeby; możesz również powrócić do tego rozdziału, gdy zechcesz odświeżyć sobie pamięć. Aby jednak nasze dalsze rozważania miały sens, muszę Cię zapoznać z podstawami działania komputerów i internetu. Staram się tu przedstawić wszystkie rudymenty, więc gdy napotkasz coś, co już znasz, spokojnie możesz to pominąć albo przeczytać tylko pobieżnie. Pozwoliłem sobie również trochę ubarwić tekst zabawnymi dodatkami, aby nie był nużący. Tę książkę będą czytać przeróżni ludzie, dlatego nie mogę w pełni wytłumaczyć wszystkiego. W tym jednak rozdziale kładę solidne podstawy, na których możesz oprzeć swoją wiedzę.

Tu mieszkają smoki

Większość ludzi nie ma żadnego wyobrażenia o bezpieczeństwie komputerowym — jest to dla nich przedmiot zanadto abstrakcyjny i techniczny. Doszedłem do wniosku, że można objaśnić wiele jego aspektów, posługując się analogią do zamku feudała. Masz ludzi i kosztowności i musisz tego wszystkiego bronić przed rozmaitymi atakami. W dawnych czasach budowano w tym celu fizyczne przeszkody, takie jak mury i fosy. Okazuje się, że te same pojęcia dobrze pasują do bezpieczeństwa komputerowego. Mając to na uwadze i posługując się analogią do klasycznej, średniowiecznej warowni, porozmawiajmy o podstawach tego bezpieczeństwa.

Pasuję cię na…

Gratuluję! Twój król w swojej nieskończonej mądrości i wielkoduszności przyznał Ci władzę i rozległe połacie ziemi! Masz zaludnić i zabezpieczyć nowe obszary, w szczególności po to, aby przysporzyć dochodów podatkowych swojemu seniorowi. W tym celu otrzymałeś pewien zasób złota i surowców. Co dalej? Jak postąpisz?

Cóż, przede wszystkim powinieneś ustalić, co i kogo masz chronić. Na pewno będziesz musiał zabezpieczyć swoje złoto i inne kosztowności. Będziesz też musiał chronić zasoby naturalne na swoich włościach: grunty uprawne, kopalnie, kamieniołomy, lasy i źródła wody. Ponadto chcesz kontrolować dostęp do swoich ziem, a zwłaszcza szlaki wodne i lądowe. Bezpieczeństwo ludzi na Twoim terytorium jest również sprawą pierwszorzędnej wagi — nie dlatego, że jesteś dobrym człowiekiem, ale dlatego, że owi

ludzie są potrzebni do uprawy roli, pracy w kopalniach, wytwarzania dóbr, płacenia danin, jak też zasilania szeregów Twojej armii oraz gwardii przybocznej.

Następnie powinieneś określić, przed czym masz bronić swoich ludzi i zasobów. Niestety, zewsząd czyha wiele niebezpieczeństw. Nie tylko musisz uważać na chytrych rabusiów i wrogie wojska, lecz także strzec się dzikich zwierząt, groźnej zarazy, a nawet przebiegłych oszustów (o rety!). Warto też poznać siły i środki przeciwnika. Czy posiada on mocne oparcie finansowe? Jaką bronią się posługuje? Jakich sposobów walki używa? Wreszcie powinieneś rozpoznać motywy napastników. Czy są zachłanni, czy po prostu wygłodniali? Czy zamierzają poczynić jakieś kroki polityczne lub społeczne? Czy mają powody, by zaatakować właśnie Ciebie?

Posiadasz rozległe dobra, lecz ograniczone zasoby. Chcesz trzymać na dystans ciemnych typków, ale musisz zezwalać na handel i podróże. Istnieje wielu potencjalnych napastników, lecz prawdopodobieństwo ataku z każdej strony nie jest jednakowe. Podobnie będzie, gdy chodzi o ludzi i dobra pod Twoją ochroną — nie oszukujmy się, że nie cenisz ich w równym stopniu (np. Ty i Twoje złoto jesteście najważniejsi). Krótko mówiąc, musisz znaleźć jakiś kompromis. Bezpieczeństwo jest *zawsze* kwestią kompromisu. Teraz jednak, gdy przeprowadziliśmy analizę zagrożeń, posiadłeś dużo jaśniejsze pojęcie o tym, na co przeznaczyć swoje ograniczone zasoby.

Jako konsument z ograniczonym budżetem musisz ocenić grożące Ci niebezpieczeństwa i zdecydować, na co poświęcić swoje pieniądze i czas. Na szczęście większość tej pracy wykonałem za Ciebie w niniejszej książce!

Trzeba zauważyć, że jeśli agresorzy są znacznie lepiej od Ciebie dofinansowani albo posiadają dużo więcej zasobów, to prawdopodobnie stoisz na straconej pozycji. Przykładowo jeżeli uweźmie się na Ciebie rosyjska mafia bądź amerykańska Narodowa Agencja Bezpieczeństwa (NSA), bardzo trudno będzie Ci ją powstrzymać. W naszej analogii odpowiada to próbie obrony swoich włości przed smokiem. Jak sądzę, przed czerwcem 2013 r. wielu ludzi włożyłoby między bajki o smokach podejrzenie, że NSA prowadzi ogólną inwigilację — być może burzyło się przeciwko niej paru wariatów w cynfoliowych czepkach[1], ale to przecież nie mogła być prawda. Tymczasem, jak głosi porzekadło, nawet jeśli nie jesteś paranoikiem, to nie znaczy, że oni na Ciebie nie polują.

Gdyby nasz wyimaginowany rycerz uwierzył w istnienie smoków i postanowił, że musi się przed nimi bronić, co mógłby zrobić? Żaden mur nie powstrzyma latającej bestii. Również zwyczajna broń raczej nie przyda się przeciwko potężnemu stworowi. Z pewnością mógłbyś *spróbować* wznieść jakąś kopulastą twierdzę i zaopatrzyć się w zestaw przeciwsmoczego oręża, lecz prawdopodobnie w trakcie tych zabiegów stałbyś się bankrutem. A nawet gdyby udało się to osiągnąć, w jaki sposób wypróbowałbyś nowe środki obrony? Nie dość na tym: równie dobrze próba zbudowania tak silnej warowni mogłaby właśnie przykuć uwagę smoka! Po co ktokolwiek miałby się starać o takie zabezpieczenia, gdyby nie posiadał jakichś wyjątkowo cennych przedmiotów (np. mnóstwa złota i klejnotów)? Nie — jedyną nadzieję na ocalenie w obliczu takiego przeciwnika dawałoby ukrycie się w jakiejś głębokiej, mrocznej jaskini, zniknięcie mu z pola widzenia i niewychylanie głowy. Tylko cóż to byłoby za życie dla Twojej rodziny i poddanych?

Sednem tej książki (oraz inspiracją dla jej tytułu) jest to, że nie powinieneś próbować się bronić przed smokami. W myśl naszej analogii nie jesteś przecież władcą-rycerzem, ale człowiekiem z gminu. W porównaniu z bogaczami i wielkimi przedsiębiorstwami nie masz wiele do bronienia. Niemniej to, co posiadasz, należy do Ciebie i chciałbyś poczynić jakieś rozsądne i niezbyt kosztowne kroki w celu zabezpieczenia swojej rodziny i własności. Pomyśl o swoim obecnym mieszkaniu. Zapewne trzymasz w nim rzeczy warte wiele pieniędzy: ubrania, sprzęt elektroniczny, biżuterię i meble. Co jednak odgradza to wszystko od włamywaczy? Zapewne prosty zamek na klucz, kosztujący ok. 100 złotych w sklepie żelaznym. Czy można by go otworzyć wytrychem? Bez wątpienia tak (zdziwiłbyś się, jak łatwo otwiera się typowe zamki — nauczyłem się tego mniej więcej w kwadrans). Pomimo to na większości osiedli taki prosty zamek wystarcza.

[1] Cynfoliowy (właściwie aluminiowy) czepek — nakrycie głowy mające służyć do zabezpieczania mózgu przed promieniowaniem elektromagnetycznym, odczytywaniem myśli itp.; symbol przesadnej ostrożności, podejrzliwości lub manii prześladowczej — *przyp. tłum.*

Z tych samych względów nie potrzebujesz chronić swojego komputera i jego zawartości przed rosyjską mafią ani NSA. Ewentualnie mógłbyś to osiągnąć wyłącznie za cenę całkowitej izolacji. Jeżeli Cię to interesuje, mogłoby to wyglądać następująco. Najpierw kupujesz nowy komputer przenośny w dużym sklepie samoobsługowym. Zanim go uruchomisz, otwierasz obudowę i wyjmujesz wszystkie podzespoły odpowiadające za komunikację bezprzewodową, takie jak układy wi-fi i Bluetooth. Ustawiasz komputer w piwnicy bez okien, a jej ściany i sufit okrywasz siatką drucianą, aby nie przepuszczały sygnałów radiowych. *Przenigdy* nie podłączasz komputera do internetu i nie używasz żadnych urządzeń peryferyjnych (myszki, drukarki itp.) z kablem USB. Jaki miałbyś z tego pożytek? Komputer bez internetu jest dzisiaj prawie bezużyteczny. Ale nawet gdybyś poradził sobie w ten sposób, te drastyczne środki bezpieczeństwa i tak nie uchroniłyby Cię przed włamaniem do domu lub wręczeniem Ci nakazu przeszukania. Jeżeli jesteś dysydentem, sygnalistą w korporacji lub po prostu paranoikiem, to potrzebujesz innej książki. I najlepiej kup ją za gotówkę.

Chodzi jednak o to, że rosyjska mafia i NSA raczej nie będą celować *specjalnie* w Ciebie. Jak powiedzieliśmy już wcześniej, najpewniej będą Ci zagrażać oszuści korzystający z poczty elektronicznej, włamywacze próbujący dobrać się do Twoich rachunków bankowych oraz przedsiębiorstwa i władze prowadzące masową inwigilację. W tym zakresie możesz zrobić całkiem sporo, aby się obronić, nie poświęcając na to zbyt wiele czasu ani pieniędzy — i o tym właśnie traktuje ta książka.

Zapobieganie, wykrywanie i odzyskiwanie

Ogólnie zabezpieczanie obejmuje trzy etapy: przed, w trakcie i po, określane też jako zapobieganie (lub prewencja), wykrywanie oraz odzyskiwanie (lub przywracanie). Zapobieganie to próba uniknięcia przykrych wypadków; wykrywanie to definitywne ustalenie, że coś złego zaszło lub właśnie się dzieje; odzyskiwanie to naprawa lub łagodzenie zaistniałych szkód. Oczywiście ludzie z reguły skupiają się na prewencji, tak aby dwa następne etapy nie były potrzebne, żaden jednak plan bezpieczeństwa nie jest kompletny bez wszystkich trzech.

Wróćmy do naszego świeżo upieczonego władcy i obrony jego włości. W średniowieczu najpowszechniejszym środkiem obronnym był dostojny zamek. Niepraktyczne byłoby otaczanie całej krainy murem wysokim na 25 metrów, toteż panujący zwykle wznosił mury wokół miast, zwłaszcza tam, gdzie mieszkał on sam i jego rodzina. Zamki najczęściej stawiano na wzniesieniach, aby lepiej obserwować okolicę pod względem nadciągającego niebezpieczeństwa i mieć przewagę nad stroną atakującą. W czasie wojny ludność mogła się schronić w obrębie murów. Zamki na ogół miały bronić przed piechotą i konnicą. Nie istniały samoloty, więc niepotrzebna była obrona przeciwlotnicza, niemniej mury musiały być wystarczająco wysokie, żeby powstrzymać atakujących z drabinami, strzały z łuków i katapulty. Oprócz murów zamek często otaczała fosa, również utrudniająca dostęp napastnikom. Ponieważ trzeba było jakoś wchodzić i wychodzić, w murach musiało być co najmniej kilka przejść, które zabezpieczano wielkimi kratami z drewna bądź żelaza; czasami przypadało ich kilka na jedno przejście. Tych miejsc strzegły uzbrojone straże, które miały za zadanie kontrolować, komu wolno wejść i wyjść. Także mury i teren wewnętrzny były patrolowane przez strażników, próbujących rozpoznać, czy ktoś niepożądany nie przedostał się przez zewnętrzne bariery.

Zamki miały *obronę urzutowaną w głąb*, czyli były wyposażone w niejeden mechanizm powstrzymujący napastników. Mechanizmy te różniły się pomiędzy sobą, nie tylko ze względu na odmienne możliwości różnych przeciwników, lecz także po to, by zdywersyfikować całościowy system obrony na wypadek, gdyby napastnik zdołał sprytnie ominąć któryś z jego elementów. Niektóre składniki systemu miały charakter pasywny, np. mury i fosa; gdy raz je postawiono, prawie nie wymagały zabiegów. Inne środki obrony były aktywne, np. straż zamkowa. Strażnicy mogli samodzielnie myśleć, przyjmować rozkazy, a także na bieżąco oceniać jednostkowe zagrożenia i na nie reagować. Po otrzymaniu wyczerpujących instrukcji i przeszkoleniu nawet oni umieli całkiem skutecznie działać na własną rękę.

Okazuje się, że zabezpieczanie komputera pod wieloma względami przypomina budowę zamku. Główną bramą jest ruter internetowy, który oddziela Cię od świata zewnętrznego — zarówno od złych, jak i dobrych ludzi. Potrzebujesz połączenia ze światem, aby sprowadzać dla siebie wodę, żywność i inne zaopatrzenie,

a także sprzedawać towary; musisz jednak uważać, żeby nie przedostały się do wnętrza ciemne typki. Ruter ma w tym celu wbudowany mechanizm nazywany zaporą (ang. *firewall*). Przez analogię do zamku zapora pozwala ludziom z wewnątrz na wychodzenie i powrót, uniemożliwia zaś wstęp obcym, chyba że ich wpuścisz. Tak więc zapora pozwala komputerowi nawiązywać łączność z internetem (np. z witryną *google.com*) i wie, że ma przepuścić odpowiedź stamtąd (np. zwrot wyników wyszukiwania). Ale kiedy coś z internetu próbuje nawiązać kontakt z Twoim komputerem, wówczas zapora odmawia połączenia (lub po prostu ignoruje żądanie), chyba że na to pozwolisz wyraźnym poleceniem. Standardowo prawie wszystkie połączenia przychodzące są odrzucane przez zapory.

Oprogramowanie antywirusowe (ang. *antivirus* [AV] *software*) to coś w rodzaju zbrojnej straży. Aktywnie pilnuje systemu, a gdy wystąpi podejrzane zachowanie, stara się je powstrzymać. Często programy tego typu informują użytkownika o takiej sytuacji i pytają go, czy zezwala na daną czynność. Niemniej jeżeli zachodzi pewność, że dzieje się coś niewłaściwego, program antywirusowy zazwyczaj samodzielnie neutralizuje zagrożenie.

Jednakże nie wszystkie niebezpieczeństwa pochodzą z internetu. Również możliwe, choć nie tak samo prawdopodobne, jest uzyskanie fizycznego, osobistego dostępu do komputera. W takim przypadku Twoimi „murami obronnymi" są belki i cegły, a „fosą" — dobrze oświetlone podwórze z ciernistymi zaroślami przed oknem. Dopóki Twój komputer znajduje się w domu lub innym bezpiecznym miejscu, liczysz na to, że zamknięte drzwi, ściany itd. odstraszą złoczyńców. Jeżeli jednak posiadasz komputer przenośny i zabierasz go z domu, to zapewne masz znacznie słabsze zabezpieczenia fizyczne — może samochód, a może tylko specjalną torbę. W takiej sytuacji *Ty sam* pozostajesz najpewniejszym zabezpieczeniem, jeśli trzymasz komputer przy sobie, w torbie, najlepiej na ramieniu. Koniecznie powinieneś też ustalić hasło, tak żeby ktoś, kto ewentualnie ukradnie Ci sprzęt lub uzyska do niego bezpośredni dostęp, nie zdołał dostać się do Twoich danych. Powinieneś także zaszyfrować dysk twardy, zwłaszcza w komputerze przenośnym. W takim komputerze można się niepostrzeżenie dostać do danych bez zalogowania, więc zaszyfrowanie zawartości dysku stałego uniemożliwi jej odczytanie, jeżeli atakującemu uda się ominąć proces logowania.

To jest obrona urzutowana w głąb. Powinieneś zadbać o kilka warstw zabezpieczeń swojego komputera i zgromadzonych na nim danych. Im więcej warstw, tym będziesz bezpieczniejszy. Z tej książki dowiesz się, jak je tworzyć.

W tej książce nie poświęcimy wiele miejsca zagadnieniom wykrywania. Samodzielne ustalenie, że komputer jest atakowany lub niedawno uległ atakowi, to niełatwe zadanie. Co prawda można zakupić programy, które kontrolują (zwykle przez obserwację wychodzącego ruchu sieciowego), czy na komputerze osobistym nie zachodzą podejrzane działania; niemniej większość systemów wykrywania infiltracji (ang. *intrusion detection system* — IDS) jest przeznaczona dla właścicieli dużych serwerów publicznych. IDS-y są podobne do zapór; jednakże zapora przeważnie służy przede wszystkim przeciwdziałaniu infiltracji, podczas gdy IDS monitoruje czynności zachodzące w tle i transfer danych w poszukiwaniu oznak świadczących o tym, że atakujący już przeniknęli do komputera i próbują zrobić coś złego.

W naszej analogii straż zamkowa zajmuje się obserwowaniem ludzi przebywających w obrębie murów, zwracając uwagę na podejrzane zachowania i nieuprawnione kontakty z agentami z zewnątrz. W razie wykrycia intruzów bije się na alarm i pozostałe straże trwają w najwyższej gotowości, aż wszystkie zagrożenia zostaną rozpoznane i zneutralizowane. Jeżeli zwykła straż działa jak oprogramowanie antywirusowe, to oddziały elitarne przypominają raczej IDS; obie funkcje są zbliżone, a różnią się głównie zakresem i złożonością.

Wykrywanie nie jest (na razie) szczególnie przydatne w komputerach domowych, ale pełni ważną funkcję w zabezpieczaniu innych obszarów, z którymi mamy codzienną styczność. Na przykład specjalne taśmy i wklęsłe wieczka na artykułach żywnościowych informują nas o tym, czy słoik lub butelka były już otwierane. Papierowe lub foliowe naklejki na zamknięciach opakowań z lekami dostępnymi bez recepty (OTC) wprowadzono w bezpośrednim następstwie otruć tylenolem w Chicago na początku lat 80. ubiegłego wieku. Takie plomby umieszcza się nie po to, aby *zapobiec* manipulacji, lecz po to, aby ją *uwidocznić*. Widząc, że zamknięcie jest naruszone, wiemy, że ktoś nim manipulował, dlatego nie powinniśmy

używać tego produktu. Dawniej do zabezpieczania ważnej korespondencji używano pieczęci lakowych; nie chroniły one przed otwarciem listu, ale pozwalały stwierdzić, czy ktoś zrobił to wcześniej niż właściwy adresat.

Pomimo najbardziej wytężonych wysiłków możesz nie zapobiec wszystkim atakom, dlatego potrzebujesz także planu na wypadek, gdyby faktycznie zaszło coś złego. W niektórych sytuacjach, wiedząc o naruszeniu zabezpieczeń, można poczynić kroki w celu złagodzenia szkodliwych skutków: uruchomić program do usuwania złośliwego oprogramowania, pozmieniać hasła, zamknąć konta lub zdalnie usunąć swoje dane (jeżeli komputer lub inny sprzęt został ukradziony). Czasami jedynym wyjściem jest odrobienie strat i pójście dalej.

Terminologia informatyczna

Komputery są wszechobecne. Nie mam na myśli jedynie maszyn biurkowych i przenośnych. Niemal każde nowoczesne urządzenie elektroniczne mieści w sobie jakiś układ komputerowy, obecnie zaś wkraczamy w epokę łączenia ich wszystkich ze sobą: termostatów, telewizorów, odbiorników radiowych, a nawet opiekaczy do chleba (nie żartuję). Pomimo swojej wszechobecności komputery nie są przedmiotem należytego zrozumienia, a to z zasadniczego powodu: są one fenomenalnymi, skomplikowanymi tworami sztuki inżynierskiej!

Moim pierwszym komputerem był TI-99/4A firmy Texas Instruments (rysunek 2.1).

Rysunek 2.1. *Komputer TI-99/4A firmy Texas Instruments (ok. 1981 r.)*

Miał on tylko 16 KB pamięci. Pierwszy iPod mojej córki miał ponad 250 tys. razy więcej pamięci! W 1965 r. jegomość nazwiskiem Gordon Moore, współzałożyciel firmy Intel, napisał artykuł, w którym przewidywał, że moc obliczeniowa będzie się podwajać mniej więcej co dwa lata. Ta prognoza okazała się nader trafna i została później nazwana prawem Moore'a. Podwajanie jest wbrew pozorom bardzo potężną operacją. Podam klasyczny przykład. Załóżmy, że 1 stycznia podaruję Ci jeden grosz z obietnicą podwajania tej wartości przez resztę miesiąca. Tak więc 2 stycznia będziesz miał 2 grosze, a tydzień później — już 64. Po dwóch tygodniach posiadasz 81,92 złotego. To już coś, ale wciąż wydaje się niewiele. Jednakże w trzecim tygodniu Twój majątek przekracza 10 tys. złotych, a na koniec miesiąca stajesz się posiadaczem prawie 11 mln złotych! Wiem, że trudno w to uwierzyć, ale taka jest moc podwajania. Na podstawie prawa Moore'a możemy oszacować, że dzisiejsze komputery biurkowe są mniej więcej 65 tys. razy silniejsze od mojego małego TI-99/4A.

Mógłbym napisać cały tom o zasadach działania komputerów i może kiedyś to zrobię, ale na potrzeby tej książki przedstawię tylko najważniejsze pojęcia i terminy i omówię je bardzo ogólnie. Przypominam, że nie musisz tego wszystkiego zapamiętywać; chcę Cię tylko zaznajomić z podstawowymi rzeczami. Zawsze możesz sięgnąć do słowniczka, kiedy zapragniesz odświeżyć sobie pamięć.

Sprzęt i oprogramowanie

Nie sposób rozmawiać o komputerach, nie mówiąc o *sprzęcie* i *oprogramowaniu*. Sprzętem jest fizyczny komputer i wszystkie jego składniki, a więc zasadniczo to, co widoczne i namacalne. Do sprzętu zaliczają się też wszystkie rzeczy podłączone do komputera, ogólnie zwane **urządzeniami peryferyjnymi**, takie jak mysz, klawiatura, monitor ekranowy, drukarka, napędy dyskowe itd.

Oprogramowaniem jest kod komputerowy wykonywany na sprzęcie — złożony zestaw instrukcji dotyczących działania sprzętu w każdej możliwej sytuacji przewidzianej przez programistę, w szczególności w sytuacji wyjątkowej. Podstawowym programem, który steruje samym komputerem, jest **system operacyjny** (ang. *operating system* — OS). **Aplikacje** programowe to mniejsze, bardziej wyspecjalizowane jednostki oprogramowania przeznaczone do specjalnych czynności, takich jak redagowanie dokumentów, odtwarzanie muzyki lub poruszanie się po internecie. System operacyjny zajmuje się takimi sprawami jak uruchamianie i zatrzymywanie poszczególnych aplikacji, zarządzanie zbiorami danych, łączenie się z siecią oraz komunikacja z urządzeniami peryferyjnymi: klawiaturą, myszą, monitorem czy drukarką. OS to szczególny program, niezbędny do funkcjonowania komputera, aplikacje zaś to fakultatywne dodatki, przeznaczone do wykonywania konkretnych zadań.

W większości komputerów typu PC systemem operacyjnym jest Microsoft Windows. W maszynach Apple Macintosh system nazywa się macOS (dawniej Mac OS X). Przykładami aplikacji są: Microsoft Word, Adobe Reader, Mozilla Firefox, iTunes.

Sprzęt i oprogramowanie można sobie wyobrazić na kształt spektaklu teatralnego. Sprzętem jest scena, dekoracja, kurtyna, oświetlenie i nagłośnienie. System operacyjny stanowi jak gdyby połączenie scenariusza, reżyserii i obsługi scenicznej: steruje on całym przebiegiem przedstawienia, zapewniając, że aktorzy odgrywają właściwe role, i dostosowując otoczenie do sytuacji (rekwizyty, kostiumy, efekty świetlne i dźwiękowe). Wreszcie aktorzy to niejako aplikacje: wykonują poszczególne role na podstawie scenariusza i posługują się rekwizytami (dane i urządzenia peryferyjne) we współpracy z pozostałymi członkami zespołu.

Menedżer plików

Kiedy pracujesz na komputerze i chcesz przejrzeć listę plików, które się na nim znajdują, posługujesz się w tym celu **menedżerem plików** (ang. *file manager*). W systemie Windows nosi on nazwę Eksplorator Windows lub Eksplorator plików, a w Macintoshu — Finder. Gdy klikasz dwukrotnie katalog na pulpicie, otwierasz Mój komputer albo Macintosh HD, wtedy uruchamiasz menedżer plików. Może się to wydawać banalne, ale niektórzy nie wiedzą, że to się tak nazywa.

Bity i bajty

Wszystkie dane na komputerze — dokumenty, obrazy, a nawet utwory filmowe i muzyczne — są przechowywane w postaci bitów i bajtów. Zresztą dotyczy to również aplikacji programowych, a nawet samego systemu operacyjnego. Bity i bajty to podstawowe elementy świata cyfrowego. **Bit** jest najmniejszą porcją informacji w komputerze. Przyjmuje on jedną z dwóch wartości — zero albo jeden. Inaczej mówiąc, bit ma naturę dwójkową, czyli binarną (cząstka *bi* znaczy „dwa"). Bit oznacza się w skrócie małą literą *b*.

Aby tworzyć większe całości — takie jak różne wielkości liczbowe, znaki alfabetu, a także zabawne emotikony — potrzebujemy czegoś więcej od pojedynczego bitu. Następną pod względem wielkości porcją danych cyfrowych jest **bajt**, skrótowo oznaczany dużą literą *B*. Jeden bajt równa się ośmiu bitom. Tak więc skoro każdy z tych ośmiu bitów może przyjąć jedną z dwóch wartości, po dokonaniu obliczeń otrzymujemy 256 możliwych kombinacji ośmiobitowych: 00000000, 00000001, 00000010, 00000011 itd. aż do 11111111.

Do reprezentowania znaczących cząstek informacji używa się różnych sekwencji takich bitów; nazywamy to **kodowaniem**. Istnieje mnóstwo metod kodowania; w zasadzie można to robić dowolnie, pod warunkiem dokładnego określenia reguł, tak aby inni mogli *zdekodować* przekaz. Popularnym przykładem jest kodowanie ASCII (ang. *American Standard Code for Information Interchange* — amerykański standardowy kod do wymiany informacji). ASCII służy do kodowania znaków: liter, cyfr i innych symboli widniejących na klawiaturze komputerowej. Na przykład litera *A* ma w tym systemie kod 01000001[2]. Ponieważ chcemy rozróżniać duże i małe litery, potrzebujemy kodów dla jednych i drugich. Mała litera *a* ma kod 01100001[3]. Ogółem to wszystko, co możesz wpisać z użyciem klawiatury, ma jakąś reprezentację w ASCII. Przykładowo napis „witaj" wyglądałby następująco:

```
01110111011010010111010001100001011010 10
```

Osiem pierwszych bitów, 01110111, odpowiada literze *w* itd. Dla ludzi ten zapis wygląda zawile i odstręczająco, ale takim właśnie językiem posługują się na co dzień komputery.

Porozmawiajmy teraz o większych ilościach danych. Jeden bajt wystarcza do zakodowania jednego znaku z klawiatury, ale to jeszcze za mało. Aby kodować całe teksty, obrazy, filmy itp., potrzebujemy wielu bajtów. I jak posługujemy się skrótowymi nazwami dużych liczb dziesiętnych (tysiąc, milion, miliard itd.), tak samo używamy skrótów na oznaczenie dużych ilości bajtów. Te skrótowe terminy opierają się na standardowych przedrostkach miary: kilo- (tysiące), mega- (miliony), giga- (miliardy), tera- (biliony) itd. Tak więc kilobajt (KB) to tysiąc bajtów, megabajt (MB) — milion bajtów, a terabajt (TB) — bilion bajtów[4].

Pamięć

Aby komputer mógł przechowywać i przetwarzać wszystkie te bity i bajty, musi gdzieś je przechowywać. W komputerze istnieją różne wyrafinowane formy przestrzeni pamięciowej, ale dwiema najważniejszymi są pamięć o dostępie swobodnym/bezpośrednim (ang. *random access memory* — RAM) i dyski twarde. Kupując komputer, możesz przeczytać na pudełku ważne informacje o ich pojemności.

Najlepszą znaną mi analogią pomagającą zrozumieć, w jaki sposób funkcjonuje pamięć komputera, jest porównanie go do warsztatu garażowego. W garażu trzymasz wszystkie swoje narzędzia i materiały.

---

[2] W zapisie dwójkowym, co w systemie dziesiętnym odpowiada liczbie 65 — *przyp. tłum.*

[3] W systemie dziesiętnym 97 — *przyp. tłum.*

[4] Mniej więcej. Ponieważ komputery pracują w systemie dwójkowym, liczą według kolejnych potęg dwójki. Zapewne nigdy Ci się to nie przyda, ale gdy jakiś mędrek Ci powie, że 1 KB w rzeczywistości nie równa się 1000 bajtów, będzie miał rację… W istocie są to 1024 bajty. Dlaczego? Bo tak. Uwierz mi na słowo. W większości przypadków możesz po prostu przyjąć, że chodzi o 1000 bajtów, i na tym poprzestać. To samo dotyczy większych wartości (MB, GB, TB): traktuj je jak miliony, miliardy itd. — to z grubsza tyle samo.

Posługujesz się narzędziami do obróbki materiałów, albo tworząc nowe rzeczy, albo przerabiając stare. Jednakże nie korzystasz ze wszystkich narzędzi i materiałów jednocześnie — na ogół używasz nich pojedynczo, ewentualnie po kilka naraz. Gdy nadchodzi pora rozpoczęcia pracy, wyjmujesz potrzebne w danej chwili narzędzia i materiały i umieszczasz je na stole roboczym. Po zakończeniu pracy odkładasz na miejsce narzędzia i niezużyte materiały. Jeżeli próbujesz robić zbyt wiele rzeczy naraz, stwierdzasz, że powierzchnia robocza się zapełnia; po prostu nie możesz używać wszystkich swoich narzędzi i materiałów równocześnie — musisz któreś wybrać. Może da się położyć niektóre z nich na podłodze obok i wymieniać je w razie potrzeby, lecz nie będzie to zbyt efektywne.

Komputer działa na podobnej zasadzie. Dysk twardy jest niczym garaż — mieści w sobie wszystkie Twoje dane i programy gotowe do użytku. Gdy uruchamiasz określoną aplikację lub otwierasz któryś plik, jedne i drugie dane są kopiowane z dysku twardego do RAM-u, gdzie komputer może na nich pracować bezpośrednio i najefektywniej. Po zamknięciu aplikacji dane są kopiowane z powrotem z RAM-u na dysk. Dlatego właśnie dysk twardy jest dużo większy od RAM-u: musi pomieścić w sobie wszystko, nad czym akurat pracujesz albo nie, RAM natomiast musi przechować tylko to, nad czym właśnie pracujesz. Im więcej RAM-u, tym więcej rzeczy można obrabiać jednocześnie, tak jak na dużym stole warsztatowym. Gdy RAM się zapełni, komputer przenosi część jego zawartości na dysk twardy, aby zrobić miejsce, a w razie potrzeby dokonuje zamiany. Właśnie dlatego komputer staje się naprawdę opieszały, kiedy próbujesz otworzyć zbyt wiele aplikacji lub dużych zbiorów danych jednocześnie.

Gdy w garażu nazbiera Ci się za dużo rupieci, masz dwa wyjścia — zbudować większy garaż albo postarać się o jakąś dodatkową przestrzeń magazynową, taką jak przechowalnia na wynajem lub szopa z tyłu podwórza. Podobnie jeżeli chcesz robić więcej rzeczy naraz, potrzebujesz obszerniejszego stołu. Co się tyczy komputera, to rozwiązania są analogiczne. Aby przechowywać więcej danych, kupujesz pojemniejszy wewnętrzny dysk twardy bądź dodatkowy zewnętrzny. Jeżeli chcesz robić więcej naraz, musisz powiększyć RAM.

Sieci przewodowe i bezprzewodowe

Kiedy komputery porozumiewają się pomiędzy sobą, robią to poprzez **sieć**. Inaczej mówiąc, sieć jest zbiorem połączonych komputerów, które komunikują się za pomocą wspólnego języka, czyli **protokołu**. Większość współczesnych sieci komputerowych używa tzw. protokołu internetowego (ang. *Internet Protocol* — IP). Sieci bardzo się różnią pod względem wielkości, ale występują w dwóch podstawowych formach: jako publiczne oraz prywatne. Komputerową siecią publiczną, którą wszyscy znamy i kochamy, jest ogromna, ogólnoświatowa pajęczyna nazywana internetem (od pierwotnej nazwy *Internetwork* — „międzysieć").

Istnieje też jednak nieprzeliczona liczba małych, prywatnych (bądź półprywatnych) sieci podłączonych do internetu. Zazwyczaj określa się je jako **komputerowe sieci lokalne** (ang. *local area network* — LAN). W pierwszej chwili jako właściciele LAN-ów przychodzą na myśl przedsiębiorstwa, ale jeżeli masz w domu ruter, do którego przyłączyłeś więcej niż jeden komputer lub inne urządzenie, to również posiadasz LAN.

Sieci mogą być albo przewodowe, albo bezprzewodowe, albo (najczęściej) takie i takie. Komputery są podłączone do LAN-u kablami typu Ethernet, które wyglądają jak przewody telefoniczne z większymi końcówkami plastikowymi po obydwu stronach. Komputery połączone bezprzewodowo korzystają z systemu wi-fi[5].

Na rysunku 2.2 przedstawiono standardowy kabel ethernetowy (połączenie przewodowe) oraz rozpoznawalny na całym świecie symbol wi-fi (połączenie bezprzewodowe).

[5] Wi-fi to po prostu chwytliwa nazwa, którą ktoś wymyślił. Miała brzmieć podobnie do hi-fi (ang. *high fidelity* — wysoka wierność [odtwarzania dźwięku]), ale w rzeczywistości nie oznacza „bezprzewodowej wierności" (ang. *wireless fidelity*). Jest po prostu dużo atrakcyjniejsza niż właściwe oznaczenie techniczne tego standardu — IEEE 802.11. (Niemniej autorytatywne źródła angielskojęzyczne, zarówno ogólne, jak i specjalistyczne, często objaśniają termin *wi-fi* właśnie jako skrót od *WIreless FIdelity — przyp. tłum.*).

Rysunek 2.2. *Kabel typu Ethernet (po lewej) oraz logo wi-fi (po prawej)*

Nie sposób rozmawiać o bezpieczeństwie cybernetycznym, jeżeli nie wie się paru podstawowych rzeczy o metodach komunikacji międzykomputerowej. Poświęcam tej tematyce więcej miejsca w dalszej części bieżącego rozdziału.

Szerokość pasma

Transmitując dane, chcielibyśmy wiedzieć, z jaką prędkością mogą się przemieszczać. Miarą tej prędkości są „bity na sekundę" (ang. *bits per second* — b/s)[6], najczęściej megabity na sekundę (Mb/s), a czasami gigabity na sekundę (Gb/s). Wielkość tę określa się jako **szerokość pasma**. Najczęściej napotykamy ją przy dwóch okazjach: kiedy podpisujemy umowę z operatorem internetowym (ang. *Internet service provider* — ISP) albo kiedy oglądamy sprzęt sieciowy, np. ruter bezprzewodowy.

Najlepiej wyobrazić sobie szerokość pasma przez podobieństwo do wody płynącej w rurach. Przez grubszą rurę można przepuścić więcej wody w krótszym czasie. Internet jest często przedstawiany jako układ rur (albo przewodów) właśnie przez analogię do wody. Jeżeli woda jest dostarczana do domów z głównego ujęcia w danej miejscowości i następnie odprowadzana do kanalizacji, to dane w internecie krążą podobnie, przynajmniej pod względem prędkości. Od ujęcia biegną duże rury, które doprowadzają wodę na osiedla, dalej mniejsze (powolniejsze), które dochodzą do budynków, i wreszcie najcieńsze, do których podłącza się prysznice, baterie kuchenne itd.

Bardzo podobnie wygląda usługa internetowa. Łącza domowe są najpowolniejsze (najcieńsze rury). Przewody od budynków do osiedlowej skrzynki rozdzielczej są dużo szybsze. Połączenia skrzynki rozdzielczej z siedzibą operatora internetowego są jeszcze szybsze, a łącza między nim a następnym operatorem — najszybsze (najgrubsze „rury").

W dalszej części książki opowiem o tym, jak internet transportuje wszystkie te bity i bajty.

Bluetooth

Bluetooth to zabawna nazwa[7] poręcznego systemu łączności bezprzewodowej. Służy on głównie wyeliminowaniu irytujących kabli. Pierwotnie był używany przede wszystkim do łączenia z komputerem lokalnych urządzeń peryferyjnych, takich jak myszki i klawiatury, ale zyskał na popularności jako system transmisji dźwięku. Przykładowe zastosowania to samochodowe zestawy głośnomówiące do telefonów komórkowych, przenośne głośniki i oczywiście słuchawki bezprzewodowe. Bluetooth jest też używany w nowoczesnych układach zdalnego sterowania, ponieważ urządzenia nie muszą „widzieć się" wzajemnie, czego wymaga powszechniejsza łączność w podczerwieni (ang. *infrared* — IR). Na rysunku 2.3 przedstawiono oficjalny symbol Bluetooth.

[6] W literaturze fachowej występuje też jednostka o nazwie „bod" (ang. *baud*), 1 bd = 1 b/s — *przyp. tłum.*

[7] Dosłownie „sinozęby" — *przyp. tłum.*

Rysunek 2.3. *Logo Bluetooth*

Klient i serwer

Kiedy dwa komputery porozumiewają się ze sobą, najczęściej jeden z nich żąda od drugiego, żeby coś zrobił. Strona żądająca nazywa się **klientem**, a odpowiadająca — **serwerem**. Ten sam komputer może być raz klientem, a raz serwerem, niemniej w obecnej dobie internetu prawie wszystkie żądania pochodzą od komputerów lokalnych (klientów) i są kierowane do dużych komputerów w ogólnoświatowej sieci publicznej (serwerów). Żądania mogą być np. takie: „pokaż mi ten film z kotem grającym na fortepianie", „znajdź wszystkie strony internetowe z wizerunkiem Scarlett Johansson", „udostępnij to szałowe zdjęcie wszystkim moim znajomym".

Chmura

Jest to jedno z najczęściej używanych (i nadużywanych) określeń we współczesnej terminologii komputerowej, ukute przez dzisiejszy przemysł i rzucane na lewo i prawo. Co ono oznacza? Gdy ktoś mówi o *chmurze*, ma po prostu na myśli to wszystko, co istnieje lub dzieje się gdzieś w internecie.

Kiedy inżynierowie rysują schematy sieci komputerowych, często posługują się piktogramem chmury, aby oznaczyć jakieś bliżej nieokreślone zgrupowanie przedmiotów „gdzieś tam"… Nie wiemy, co tam jest, i nawet nie chcemy wiedzieć. Rzeczy wnikają z jednej strony w tę mgławicę i wyłaniają się po drugiej stronie; w środku czasami ulegają zmianom, a czasami wychodzą takie same. Wygląda to jak internet, prawda?

Dzisiaj wszystkie nasze komputery i inne urządzenia są połączone przez internet, a łącza stały się tak szybkie, że faktycznie możemy wysyłać dane do obróbki, zamiast przetwarzać je lokalnie na swoim sprzęcie. Kiedy wysyłamy swoje dane do internetu, aby gdzieś tam zostały poddane obróbce, nazywa się to **obliczeniami w chmurze** (ang. *cloud computing*). Przykładem może być Google Docs: zamiast uruchamiać Microsoft Word na własnym komputerze (i modyfikować plik na lokalnym dysku twardym), redagujemy dokument w przeglądarce internetowej, a wszystko to dzieje się na jakimś odległym komputerze należącym do Google'a. Kiedy trzymasz kopie swoich danych w miejscu takim jak Dropbox lub Google Drive, jest to **przechowywanie w chmurze** (ang. *cloud storage*); pliki znajdują się na lokalnym dysku twardym, a równocześnie na serwerze Dropboksa lub Google'a.

Neutralność internetu

Jeżeli nie spadłeś z Księżyca, to na pewno słyszałeś o **neutralności internetu**. Z pewnością widziałeś też wielu polityków i rzeczników prasowych trąbiących o tym, dlaczego zniszczy ona internet i handel elektroniczny albo przeciwnie — dlaczego je ocali. O co więc chodzi?

Omawiane pojęcie oznacza, że żadna osoba ani firma nie może mieć przywilejów w internecie. W tej grze powinny panować reguły jednakowe dla wszystkich jej uczestników. Brzmi to całkiem nieźle, prawda? Spójrzmy więc na rzeczywisty przykład i sprawdźmy, jak on się ma do tej definicji.

Netflix to popularny serwis filmowy — tak popularny, że według niektórych szacunków odpowiada za ponad jedną trzecią całego ruchu internetowego w godzinach szczytu! Jak łatwo zgadnąć, transfer tylu

bitów może bardzo obciążać serwery. Jeżeli operator internetowy musi dokupić sprzętu, aby sprostać temu całemu zapotrzebowaniu, to czy Netflix nie powinien mu zapłacić trochę więcej pieniędzy z tytułu tych kosztów?

Kusi nas odpowiedź: owszem, powinien. Ale to śliski grunt. Sedno sprawy leży w tym, że operatorzy internetowi sprzedają pewne usługi, a jeżeli nie są w stanie wywiązać się z obietnic, to muszą zainwestować trochę środków w infrastrukturę. Jeżeli wymaga to podniesienia opłat za usługi, to muszą je podnieść, być może tworząc przedziały cenowe, tak aby tylko użytkownicy korzystający z najszerszego pasma płacili najwięcej. Nie możemy jednak żądać od przedsiębiorców świadczących popularne usługi, żeby pokrywali zwiększone koszty; w przeciwnym razie przerodzi się to w wyzysk, a do udziału w grze zostaną dopuszczone jedynie te firmy, które będzie na to stać. Netflix i podobne młode firmy rozkwitły przede wszystkim dlatego, że mogły konkurować na jednakowych zasadach. Drobni gracze zawsze chcą regulacji dla czystej gry, ponieważ w przeciwnym razie nigdy nie mogliby rywalizować z zasobnymi, znanymi i potężnymi korporacjami. Gdy jednak sami stają się potężną korporacją, chcą się uwolnić od uregulowań, aby ustawiać sprawy po swojemu i spychać na bok konkurencję.

Neutralność internetu nie jest pojęciem nowym. Obowiązuje przez cały czas, przynajmniej do tej pory. Trzeba ją zachować, ażeby mógł się narodzić kolejny Google, Netflix czy Facebook. Niestety, w czasie powstawania tej książki rząd USA osłabił przepisy, które miały zapewniać grę według jednakowych reguł.

Internet rzeczy

Wyrażenie **internet rzeczy** (ang. *Internet of Things* — IoT) dotyczy współczesnej dążności do tego, żeby z internetem mogły się łączyć używane powszechnie przedmioty: zabawki, urządzenia gospodarstwa domowego, samochody, wodomierze, a nawet żarówki i termostaty. Dzięki temu można nimi sterować ze smartfonu lub z komputera, nawet przebywając poza domem. Oczywiście to oznacza, że mogą nimi sterować również osoby niepożądane, jeśli znajdą i wykorzystają lukę w oprogramowaniu.

Takie przedmioty są prawie zawsze związane z jakimś rodzajem usługi chmurowej. Nieustannie „telefonują" one do siedziby producenta lub innej firmy, aby zapewniać te niesłychane udogodnienia internetowe. Mówiąc o internecie rzeczy, często przywołuje się takie produkty jak Amazon Echo i Google Home — niewielkie, połączone z internetem urządzenia, które reagują, kiedy wypowiada się słowo „Alexa" (nazywane **słowem wybudzającym**). Za ich pośrednictwem można zapytać o prognozę pogody, poznać najświeższe informacje, zamówić towary z Amazona, a nawet sterować innymi tego typu urządzeniami domowymi. Jednakże w związku z tym rodzą się pewne oczywiste pytania o prywatność. Zajmę się nimi w dalszym ciągu książki.

Poznaj swojego wroga

Idę o zakład, że słyszałeś już większość z powyższych terminów informatycznych, nawet jeżeli nie wiedziałeś, co dokładnie znaczą. Na ogół jednak ludzie są znacznie mniej obznajomieni z terminologią z dziedziny bezpieczeństwa. Gruntowniej zajmę się tą tematyką w dalszych rozdziałach, a na razie chcę pobieżnie przedstawić garść pojęć, abym mógł do nich przynajmniej przelotnie nawiązywać, nie tracąc z Tobą kontaktu.

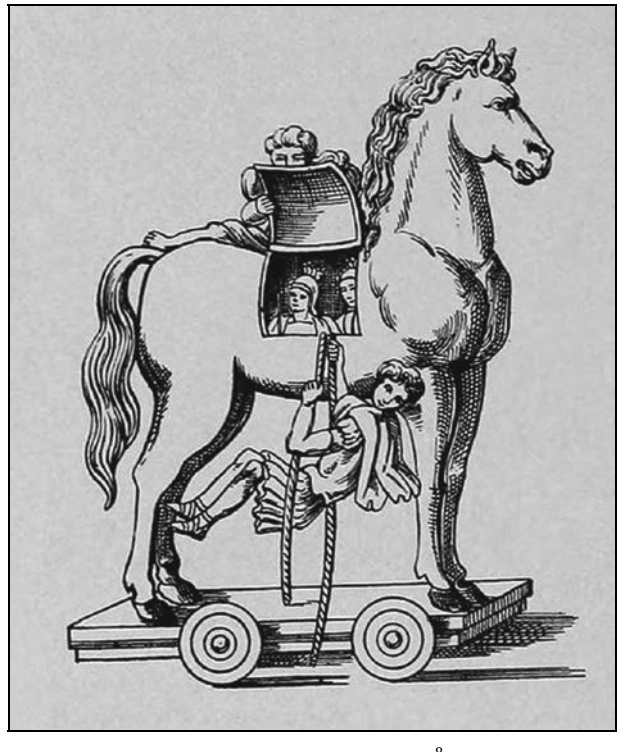
Złośliwe oprogramowanie

Wyraz *malware* jest skrótem od *malicious software* („złośliwe oprogramowanie") i ogólnie oznacza wszystkie programy, które źle się zachowują. Większość tej książki jest poświęcona temu, jak unikać takich programów. Ochrona komputera i unikanie zarażeń zabezpiecza nie tylko Ciebie, lecz także wszystkie znane Ci osoby (a przynajmniej te, które figurują w Twoim komputerowym spisie adresów).

Jak łatwo zgadnąć, istnieje wiele odmian złośliwego oprogramowania, a ponadto poszczególne programy tego typu mają zwykle wielorakie składniki i funkcje. Poniżej zestawiam najpowszechniejsze dzisiaj odmiany.

Wirusy i robaki. Te nazwy słyszała większość ludzi i zapewne one pierwsze przyszły Ci do głowy, gdy przeczytałeś definicję złośliwego oprogramowania. **Wirus** jest to program rozpowszechniany przez zarażone pliki, które z reguły użytkownik musi otworzyć, aby się zarazić. **Robak** to szczególny gatunek wirusa: może się powielać i samodzielnie przemieszczać na inne komputery przez sieć, wykorzystując błędy w usługach, które są często udostępniane na odległość. Tak jak wirus biologiczny, wirus komputerowy przenosi się do osób, które znasz i z którymi się kontaktujesz. W celu zarażania może wykorzystać spis adresów z programu pocztowego, historię przeglądarki i inne informacje z komputera.

Koń trojański (trojan). Jest to szkodliwy program „przebrany" lub ukryty w „porządnym" oprogramowaniu. Nazwa pochodzi oczywiście od klasycznej opowieści o koniu, którego Grecy użyli do zdobycia miasta Troja. We wnętrzu wielkiej drewnianej figury konia ukryli doborowy oddział wojowników (rysunek 2.4). Postawili figurę u bram miasta jako przynętę, po czym odpłynęli, pozorując porażkę. Mieszkańcy Troi wprowadzili konia do miasta, a po zapadnięciu zmierzchu wojownicy wyszli z jego wnętrza i otworzyli od środka bramy miejskie. Wówczas greckie wojska, które tymczasem powróciły pod osłoną nocy, mogły wejść do miasta i je zająć.



Rysunek 2.4. *Klasyczne wyobrażenie słynnego konia trojańskiego*[8]

[8] Źródło: Henry René d'Allemagne, *Histoire des jouets*, 1902.

Komputerowy koń trojański działa na podobnej zasadzie. Otrzymujesz coś, co wydaje się normalnym programem lub dokumentem, ale kryje w sobie szkodliwy kod. Kiedy uruchomisz taki program lub otworzysz dokument, szkodnik się aktywizuje i zaraża Twój komputer.

Oprogramowanie szpiegujące (ang. *spyware*)**.** Jest to złośliwe oprogramowanie stworzone po to, aby śledzić użytkownika — albo sprawdzać, co robi, albo poszukiwać wartościowych informacji na jego komputerze, a następnie donosić o tym ciemnym typkom. Może chodzić o hasła do kont, kontakty lub dane personalne, które posłużą do podszycia się pod kogoś (kradzież tożsamości).

Oprogramowanie szantażujące (ang. *scareware*)**.** Czasami ciemne typki próbują bezpośrednio zabrać komuś pieniądze. Tego rodzaju złośliwe oprogramowanie może ukradkiem wyrządzić jakąś szkodę w komputerze, a następnie oferować jej naprawienie (za opłatą). Niekiedy taki program podszywa się pod darmowy wykrywacz wirusów itp., ale w rzeczywistości on sam jest *przyczyną* problemu, który potem proponuje rozwiązać. W innych przypadkach oprogramowanie szantażujące obserwuje aktywność użytkownika w internecie, czekając na jakieś kłopotliwe zachowanie, np. oglądanie witryn pornograficznych lub pobieranie treści z nielegalnych źródeł; wówczas program wyświetla fałszywe ostrzeżenie o naruszeniu prawa, grożąc zdemaskowaniem, chyba że zapłaci się grzywnę.

Oprogramowanie wymuszające (ang. *ransomware*)**.** Wraz z pojawieniem się walut cyfrowych, takich jak bitcoin, nastąpiła istna eksplozja szczególnej odmiany szkodliwego oprogramowania, jaką są programy wymuszające. Infekują one komputer w taki sposób, że faktycznie kradną dane i zatrzymują je dla okupu, ukradkiem szyfrując dyski twarde; wskutek tego dane stają się całkowicie nieczytelne, ale łatwo można je odzyskać za pomocą prostego klucza deszyfrującego. Jest to tak, jak gdyby przestępcy wkradli się do domu, umieścili wszystkie kosztowności w domowym sejfie, a następnie pozostawili kartkę z informacją: „Jeżeli chcesz otrzymać kod dostępu, musisz wpłacić 10 tys. dolarów na nasze konto w banku szwajcarskim". W zasadzie nadal masz wszystko, co miałeś… tyle że nie możesz z tego korzystać. Sprytne, prawda? Gdy wniesiesz opłatę, otrzymasz klucze deszyfrujące i odzyskasz dane.

■ **Uwaga** W rozdziale 5. opowiem, jak zaszyfrować dysk twardy, aby uniemożliwić dostęp do plików na wypadek kradzieży sprzętu. Jednakże taki zabieg nie zabezpieczy komputera przed oprogramowaniem wymuszającym… Nic nie stoi na przeszkodzie, by plik został zaszyfrowany dwukrotnie!

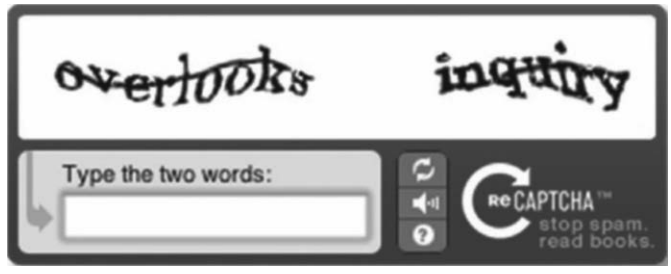
Potencjalnie niepożądane programy (ang. *potentially unwanted program* — PUP)**.** Jest to bodajże najmniej niebezpieczna forma szkodnictwa, aczkolwiek bywa dość irytująca i uciążliwa. Tego rodzaju oprogramowanie najczęściej towarzyszy „darmowym" programom, które pobieramy z internetu: dostajemy bezpłatną aplikację, ale doczepia się do niej PUP, a dostawca otrzymuje pieniądze od sprzedawców niechcianego oprogramowania za to, że instaluje się ono na czyimś komputerze. Większość instalatorów ostrzega o niechcianych dodatkach, ale trzeba pogrzebać głębiej, bo takie informacje niełatwo znaleźć. Jeżeli znajdziesz konfigurację instalacyjną, która uwidoczni zbędne programy, na ogół będziesz mógł się ich pozbyć.

Podstępniejsza odmiana PUP-a nazywa się **oprogramowaniem reklamowym** (ang. *adware*). Po zainstalowaniu wyświetla ono różnorakie reklamy. Za każdą pokazaną lub kliknięta reklamę płaci się „odsyłaczowe", co przynosi dochód. Czasami takie programy zbierają też informacje z komputera, aby odsprzedać je handlowcom.

Bot (skrót od „robot")**.** Jest to program automatyzujący czynności wykonywane normalnie przez człowieka. Boty nie zawsze powodują szkodę. Są np. używane przez wyszukiwarki, takie jak Google i Bing, do „przeczesywania" internetu w poszukiwaniu nowych, interesujących witryn, aby można je było uwzględniać w wynikach wyszukiwania. Inne boty służą do nieco mniej szczytnych celów, takich

jak pokonywanie ludzi w rozgrywkach internetowych, rejestrowanie się w konkursach lub zakładanie fałszywych kont pocztowych do rozsyłania śmieciowych wiadomości (czyli spamu).

Z tego powodu wiele witryn internetowych pokazuje użytkownikom bardzo zniekształcone wizerunki liter i cyfr, a następnie każe je przepisać do specjalnej rubryki. Te irytujące sprawdziany noszą nazwę CAPTCHA[9] (rysunek 2.5).



Rysunek 2.5. *Przykład internetowego formularza typu CAPTCHA*

Mają one zapobiegać automatycznemu wykonywaniu przez boty tego wszystkiego, co robi człowiek. Specjalnie tworzą problemy, które powinny być łatwe do rozwiązania przez człowieka, ale bardzo trudne dla programów komputerowych.

Jeśli chodzi jednak o złośliwe oprogramowanie, to boty mogą być używane do robienia w *Twoim* imieniu takich rzeczy, jakich normalnie byś *nie zrobił*; np. rozsyłają wśród Twoich znajomych wiadomość elektroniczną z reklamą tabletek na powiększenie męskich genitaliów. Niektóre ciemne typki starają się budować wielkie sieci zarażonych w ten sposób komputerów. Taka sieć (ang. *botnet*) jest w istocie armią zdalnie sterowanych maszyn, podszywających się pod właściciela, lecz pracujących dla kogoś innego; co gorsza, prawowity właściciel komputera może się o tym nigdy nie dowiedzieć. Jednym z powszechnych zastosowań sieci botów jest zasypywanie żądaniami wybranej witryny internetowej, tak aby zablokować jej serwery; tego rodzaju atak nosi nazwę „rozproszona odmowa usługi" (ang. *distributed denial of service* — DDoS). Sprawcy robią to dlatego, że nie lubią właściciela danej witryny, ewentualnie chcą od niego wymusić pieniądze „za ochronę".

Jeszcze gorsze jest to, że wszystkie nowe, wspaniałe urządzenia ze świata internetu rzeczy także są komputerami — a każdy komputer podłączony do ogólnoświatowej sieci pozostaje narażony na ataki. Ponieważ zaś owe urządzenia są na ogół wytwarzane bardzo tanio, ich zabezpieczenie jest słabe albo wcale nie istnieje. Urządzenia IoT wprost zachęcają do tworzenia sieci botów.

Kopanie kryptowalut. Wraz z nagłym powstaniem „kryptowalut", takich jak bitcoin, pojawiła się swego rodzaju gorączka ich „wydobywania" (ang. *mining*). Polega ono na przeprowadzaniu bardzo złożonych operacji, wysoce obciążających komputer; z biegiem czasu staje się to coraz trudniejsze, tak aby podaż cyfrowych kryptowalut nie wymknęła się spod kontroli. Nie trzeba było długo czekać, żeby ciemne typki przekształciły swoje sieci botów w ogromne zespoły wydobywcze. Na szczęście dla użytkowników skutkuje to jedynie wyższymi opłatami za prąd, ponieważ wprzęgnięcie komputera w takie skomplikowane operacje wymaga sporej mocy.

Rootkit. Jest to szczególnie nieprzyjemny gatunek szkodliwego oprogramowania, który często atakuje systemy operacyjne. Celowo ukrywa się zarówno przed użytkownikiem, jak i przed programami do wykrywania wirusów itp. Czasami wręcz blokuje lub niszczy programy zabezpieczające, uniemożliwiając im działanie. Co gorsza, rootkity często znajdują sposób na ukrycie kopii swojego kodu, tak że nawet jeśli

[9] Akronim nazwy *Completely Automated Public Turing test to tell Computers and Humans Apart* — „całkowicie zautomatyzowany publiczny test Turinga do rozróżniania komputerów i ludzi". Test Turinga (od nazwiska Alana Turinga) ma na celu ustalenie, że porozumiewamy się z istotą ludzką, a nie z maszyną.

się znajdzie i usunie aktywną kopię, to za chwilę uruchamia się następna. Rootkity częstokroć przygotowują na komputerze swoisty przyczółek — bezpieczne lądowisko dla kolejnych napastników. Przedstawione w tej książce metody pomagają wydatnie ograniczyć ryzyko związane z takim (i wszelkim innym) złośliwym oprogramowaniem.

Błędy sprzętowe

Ostatnimi laty rozpowszechniło się nowe zagrożenie, mianowicie ataki sprzętowe. Zamiast wyszukiwać luki w systemach operacyjnych, przeglądarkach internetowych lub innych aplikacjach, włamywacze nauczyli się sprytnie wykorzystywać słabe punkty centralnych jednostek przetwarzających (ang. *central processing unit* — CPU), czyli procesorów.

Dwa tego rodzaju błędy, które przyciągnęły uwagę środków przekazu (i słusznie), nazwano Spectre i Meltdown. Aby maksymalnie zwiększyć moc obliczeniową układów komputerowych, producenci firm Intel i AMD obmyślili metody pozwalające procesorowi na wcześniejsze obliczenie różnych możliwych wyników, a następnie, po zadecydowaniu o dalszym toku przetwarzania, podanie gotowej odpowiedzi. Wymagało to wstępnego pobierania wszystkich danych potrzebnych do takich obliczeń. Okazuje się, że ten mechanizm nie został należycie zabezpieczony i wroga aplikacja mogła zajrzeć w owe dane bez pozwolenia, przez co wyciekały informacje. Jeżeli były to prywatne dane, mogły zostać użyte do niecnych celów.

Jeżeli brzmi to zawile, to dlatego, że jest zawiłe. Takie słabe punkty i wymierzone w nie ataki były nadzwyczaj subtelne. Ponieważ jednak Intel i AMD wytwarzają procesory prawie dla każdego komputera na świecie, w rezultacie narażony był niemal każdy: Macintosh, PC, a także Linux (który jest głównym systemem operacyjnym dla większości dużych serwerów internetowych). W tym wypadku dało się załatać luki niskopoziomowymi modyfikacjami programowymi. Z pewnością jednak nadejdzie taki czas, że środki programistyczne nie pomogą, a wówczas będzie można jedynie wyrzucić komputer i kupić nowy. Na zaprojektowanie, wyprodukowanie i wdrożenie do użytku układów komputerowych potrzeba wielu miesięcy, toteż gdy ujawni się tego rodzaju błąd, nowy sprzęt może być dostępny w sprzedaży dopiero po długim czasie.

Eksploity

Eksploit (ang. *exploit*) to ogólna nazwa pewnego rodzaju szpary w cybernetycznej zbroi — słabego punktu, przez który mogą przenikać złe rzeczy. Eksploity to na ogół błędy w systemie operacyjnym bądź aplikacji, takiej jak przeglądarka internetowa, czytnik PDF lub wtyczka do przeglądarki. Chodzi po prostu o jakiś defekt w kodzie, którego twórca (taki jak ja) coś pomylił i przeoczył[10]. Nietrudno o coś takiego, nawet u doświadczonych programistów, i po części właśnie dlatego mamy dzisiaj tyle problemów ze szkodliwym oprogramowaniem.

Eksploit zerodniowy (ang. *zero-day exploit*) to słaby punkt, który pozostawał nieznany ogółowi, a w szczególności twórcy danego programu. To zasadniczo znaczy, że ciemne typki znalazły go wcześniej niż inni. Trzeba zauważyć, że wiele błędów utrzymuje się latami, zanim ktoś je odkryje. Luka nazwana Shellshock, ujawniona we wrześniu 2014 r., to jeden z najgorszych błędów tego typu — czaił się w oprogramowaniu od 1989 r.!

[10] W literaturze informatycznej występuje najczęściej określenie eksploita nie jako samej „szczeliny" czy wady oprogramowania, lecz jako szkodliwego programu, który wykorzystuje takie luki i błędy istniejące w innych programach — *przyp. tłum.*

Jak działa internet

Internet jest fascynującym osiągnięciem techniki (a faktycznie połączeniem wielu różnych technik, które współdziałają mniej czy bardziej płynnie). Całe tomy poświęcono na objaśnienie jego działania, ale ja chcę się w tym miejscu skupić na przepływie danych. Trzeba to bowiem zrozumieć, zanim przejdziemy do zagadnień chronienia danych, które krążą w sieci.

Kiedy przeglądasz strony internetowe, wysyłasz pocztę elektroniczną, zamieszczasz filmy w YouTubie albo oglądasz je w Netfliksie, wówczas przenosisz dane między swoim komputerem a inną jednostką w internecie — często jakimś dużym serwerem należącym do Amazona, Google'a czy Netfliksa, a czasami komputerem podobnym do Twojego (np. prowadząc z kolegą rozmowę przez Skype). Dane mogą podróżować w dwóch kierunkach — z internetu i do niego. Kiedy więc umieszczasz film w YouTubie, nazywamy to **wysyłaniem** lub **ładowaniem** (ang. *uploading*), a kiedy kupujesz utwór muzyczny w sklepie iTunes, żeby odtworzyć go na swoim komputerze, wówczas jest to **pobieranie** lub **ściąganie** (ang. *downloading*).

Ale jak to się faktycznie odbywa? Trafne pytanie! W rzeczywistości bardzo płynnie. Jak już wspomniałem, dane składają się z bitów i bajtów. Wykonując idealną kopię bitów, tworzysz idealną kopię danych. Aby dokonać transferu danych z jednego komputera na drugi, trzeba po prostu znaleźć sposób na powielenie bitów w tej samej kolejności na drugim komputerze. Powiedzmy, że chcesz komuś wysłać dokument Microsoft Word: nie musisz fizycznie przesyłać swoich bitów, tylko ich *kopie*. Gdy to zrobisz, plik będzie istniał zarówno na Twoim, jak i cudzym komputerze, a obydwie jego postacie będą w stu procentach jednakowe.

Jak dokładnie się to robi? Znowu trzeba by napisać cały tom, aby przedstawić istotę rzeczy, dlatego znacznie ją uprościmy. Internet działa bardzo podobnie do przedsiębiorstwa pocztowego. Musi ono dostarczyć przesyłkę z punktu A do punktu B i posługuje się w tym celu szerokim zestawem sposobów i środków, których większości w ogóle nie widzimy i nie znamy. Wiemy tylko tyle, że jeśli zaadresowany i ofrankowany list wrzucimy do skrzynki, to firma zajmie się resztą! Jeżeli chcemy, żeby adresat coś nam odesłał, musimy też podać właściwy adres zwrotny. Po prostu magia — list jakimś sposobem opuszcza naszą skrzynkę i na koniec trafia do skrzynki pocztowej odbiorcy, prawda?

Popatrzmy więc, co się dzieje za kulisami, gdy wrzucasz list do skrzynki. Co pewien czas, zwykle raz dziennie, listonosz przyjeżdża sprawdzić skrzynkę. Jeżeli znajdzie w niej list, wyjmuje go i odkłada na stos poczty wychodzącej. Na koniec dnia zabiera ten stos do sortowni, która sprawdza wszystkie adresy odbiorców i rozdziela pocztę do pojemników w zależności od miejsca przeznaczenia. Poczta miejscowa może być rozwieziona już nazajutrz przez tego samego listonosza, podczas gdy zamiejscowa prawdopodobnie zostanie umieszczona w ciężarówce lub samolocie i przewieziona do odległej placówki pocztowej, która dostarczy ją jako miejscową. Początkowy stos może zostać rozdzielony i rozesłany na różne sposoby, nawet do tego samego miejsca przeznaczenia. To zależy od stopnia załadowania ciężarówki lub samolotu, od dostępności tych środków transportu, a nawet od zmieniających się cen paliwa. Wybrana trasa i metoda transportu może też zależeć od tego, jaką usługę opłacił nadawca (przekaz pieniężny, list ekonomiczny lub priorytetowy itd.). Po drodze może nastąpić wiele przystanków i zmian środka transportu. I znowu jako nadawca nie musisz wiedzieć, jak to się odbywa — interesuje Cię jedynie to, żeby przesyłka w rozsądnym czasie dotarła do adresata.

Trasowanie internetowe działa bardzo podobnie. Każdy komputer w internecie ma niepowtarzalny adres, nazywany **adresem protokołu internetowego**, w skrócie IP. Składa się on z czterech liczb rozdzielonych kropkami, np. 74.125.228.46 lub 72.21.211.176.

Aby ludziom łatwiej było zapamiętywać te liczby, przypisujemy im umowne nazwy, takie jak „google.com" lub „amazon.com"; są to **nazwy domen**. Gdy przeglądarka internetowa lub aplikacja pocztowa ma użyć jednej z takich nazw, komputer wywołuje usługę o nazwie DNS (ang. *Domain Name System/Service* — system/usługa nazw domen), która zamienia nazwę na adres IP.

Ilekroć zatem każemy swojemu komputerowi wysłać jakieś dane przez internet, on zawija je w pakiet, nakleja docelowy adres IP, po czym umieszcza je w swego rodzaju cyfrowej skrzynce pocztowej, czekając na ich pobranie. Automatycznie dodawany jest adres IP nadawcy, tak aby komputer docelowy mógł odesłać odpowiedź. Gdy dane zostaną odebrane, przechodzą przez szereg specjalizowanych komputerów nazywanych

Ciekawostka

Każda z czterech liczb składających się na adres IP należy do przedziału 0 – 255. Gdy zsumować wszystkie warianty, otrzymamy ponad 4 mld niepowtarzalnych adresów, lecz… ta pula już ulega wyczerpaniu! Istnieje rozszerzony schemat adresowania, stopniowo wprowadzany w celu uratowania sytuacji, o nazwie **IPv6** (czyli protokół internetowy w wersji 6, która zastąpi obecną wersję 4). IPv6 pozwala zapisać naprawdę niewyobrażalnie wiele adresów:

340 282 366 920 938 463 463 374 607 431 768 211 456

Ta liczba rzeczywiście robi wrażenie. Podobno każdy atom na planecie Ziemia mógłby mieć własny adres IPv6, a jeszcze pozostałoby dosyć liczb dla 100 takich planet!

ruterami, które ustalają, jak przekazać informację z jednego miejsca w drugie. Dokładna trasa może być za każdym razem inna, co wynika z obciążenia ruterów, kosztów naliczanych przez poszczególnych operatorów oraz wszelkich szczególnych warunków, których mógł zażądać komputer nadawcy. Więcej o tym powiemy za chwilę.

W kapryśnym internecie nie występuje coś takiego jak na poczcie, mianowicie dostarczanie dużych rzeczy w jednym pakiecie. Zasadniczo każda przesyłka ma rozmiary zwykłego listu. Dlaczego? Cóż, kiedy w grę wchodzą bity i bajty, można rozłożyć wszystko na kawałki i bezbłędnie zrekonstruować po drugiej stronie! Jako że poszczególne kawałki mogą się przemieszczać różnymi trasami, ich kolejność na drugim krańcu bywa zaburzona. Jak sobie z tym poradzić? Kiedy dzieli się coś dużego na małe pakiety, każdemu z nich przypisuje się numer, poczynając od zera. Po drugiej stronie można według tych numerów poskładać dane we właściwej kolejności.

Wróćmy do naszej analogii pocztowej. Powiedzmy, że chcesz komuś wysłać kopię słownika oksfordzkiego, ale możesz to robić tylko po jednej kartce. Jak byś postąpił? Cóż, trzeba by najpierw skopiować wszystkie kartki i włożyć każdą kopię do oddzielnej koperty, a na każdej z kopert umieścić adres odbiorcy. Zamiast naklejać wszędzie znaczki, zapłaciłbyś poczcie jakiś umowny ryczałt, a ona zajęłaby się resztą. Kartki są już ponumerowane, więc jeśli przyjdą nie po kolei, adresat bez trudu je uporządkuje.

Nagle jednak uświadamiasz sobie, że Twoja skrzynka pocztowa nie pomieści wszystkich tych listów jednocześnie. Co teraz? Cóż, trzeba je wysyłać w partiach, np. po 100 sztuk. Kiedy pocztowiec opróżni skrzynkę, możesz dołożyć kolejną partię. Odbiorca otwiera wszystkie koperty i układa kartki według paginacji. Po otrzymaniu ostatniego listu będzie miał kompletny tom!

Niestety, przedsiębiorstwo pocztowe (tak jak internet) nie działa doskonale. Czasami przesyłki giną. Jak sobie z tym poradzić? Wystarczy poprosić odbiorcę, żeby co pewien czas wysłał informację o tym, co otrzymał do tej pory. Jeżeli stwierdzi brak niektórych kartek, będzie mógł poprosić o ich ponowne wysłanie.

Tak w wielkim skrócie wygląda transfer danych przez internet, tyle że zamiast tygodni zabiera ułamki sekund! Komputer nadawcy dzieli plik lub wiadomość, lub cokolwiek innego na małe porcje, nazywane **pakietami**. Każdy pakiet zostaje opatrzony dwoma adresami IP — nadawcy i odbiorcy. Następnie pakiety są numerowane, tak aby komputer odbiorczy wiedział: (a) w jakiej kolejności je poskładać oraz (b) czy któryś pakiet nie zaginął i nie powinien zostać wysłany powtórnie. Jak widać, to nie takie trudne!

Do czego potrzebujesz tej całej wiedzy? Objaśnię to w dalszych rozdziałach. Wrócimy do tej analogii, kiedy będziemy mówili o prywatności, uwierzytelnianiu i szyfrowaniu.

Metody pracy

Skoro już zapoznaliśmy się z podstawami działania komputerów oraz internetu, czas zająć się naprawdę ciekawymi rzeczami! Zdaję sobie sprawę, że normalni ludzie mogą nie podzielać mojej wielkiej fascynacji mechanizmami bezpieczeństwa cybernetycznego, zrobię jednak, co w mojej mocy, żeby Cię przekonać o ich skuteczności. Jedną z ważnych nauk płynących z tej książki jest to, że można zaufać matematyce. Środki masowego przekazu i kultura popularna lubią przedstawiać łamanie zabezpieczeń, haseł i kodów jako czynność nadzwyczaj łatwą. W rzeczywistości nowoczesne komputerowe algorytmy bezpieczeństwa są bardzo solidne i niemal nie do obejścia, jeżeli prawidłowo się je zastosuje (kluczową rolę odgrywa spójnik „jeżeli"). Pomimo miliardów dolarów wydanych na superkomputery w takich instytucjach jak NSA i GCHQ[11] instrumenty stworzone przez kryptografów trzymają się zadziwiająco mocno (na szczęście). W tym rozdziale omówimy procedury i narzędzia, które pozwalają nam robić zakupy i załatwiać sprawy w banku przez internet, a także przesyłać prywatne wiadomości i chronić swoje dane komputerowe przed osobami postronnymi.

Szyfrowanie i kryptoanaliza

Jakie problemy staramy się tu rozwiązać? Do czego przede wszystkim potrzebujemy narzędzi kryptograficznych? Rozważmy klasyczny przykład prywatnego dziennika. Chciałbym zapisywać swoje myśli i przechowywać notatki w taki sposób, żebym wyłącznie ja sam mógł je zawsze odczytać. Można po prostu gdzieś schować diariusz, licząc na to, że nikt go nie znajdzie. Jest to **zabezpieczanie przez ukrywanie** (ang. *security through obscurity*): coś jest bezpieczne tylko dlatego, że jego istnienie pozostaje nieznane. W świecie kryptografii taki sposób nigdy nie wystarcza, przynajmniej nie jako podstawowy środek bezpieczeństwa. W istocie potrzebujemy swoistego mechanizmu, dzięki któremu słowa byłyby całkowicie niezrozumiałe dla osób postronnych, nawet w wypadku kradzieży dziennika, a mimo to w pełni czytelne dla ich autora.

Jak się zapewne domyślasz, w takiej sytuacji potrzebujemy **szyfrowania**. Musimy jakimś sposobem przekształcić zapisane wyrazy w inną postać (reprezentację), która będzie czystym nonsensem dla osób postronnych. W kryptografii tekst pierwotny nazywa się **tekstem jawnym** lub **otwartym**, a jego zmienioną postać wyjściową — **szyfrogramem** lub **kryptogramem**. Aby przekształcić jeden w drugi, należy użyć **szyfru**. Jest to tajny kod lub algorytm, który odwzorowuje litery tekstu otwartego na litery, cyfry lub inne symbole szyfrogramu. Tego rodzaju szyfry nazywają się **podstawieniowymi**, ponieważ za każdą literę normalnego alfabetu podstawia się jeden znak „alfabetu" szyfrowego.

Jest to klasyczny „sekretny pierścień deszyfrujący" z dawnych lat. Dla nieobeznanych z tym przedmiotem: są to dwa przyległe kółka, osadzone na wspólnym trzpieniu; na krawędzi jednego i drugiego znajduje się ciąg znaków, tak że obracając kółkami, można różnorako przyporządkowywać wzajemnie litery lub liczby. Jeżeli ciąg jest jednakowy na obydwu kółkach, nazywamy to **szyfrem przesuwającym**. Powiedzmy, że na obu kółkach umieszczono po prostu angielski alfabet we właściwym porządku, tak że jeśli dopasujemy literę *A* na jednym kółku do litery *A* na drugim, to wszystkie litery będą sobie identycznie przyporządkowane: *B* do *B* itd. aż do końca alfabetu. To nie jest żaden szyfr, więc przekręćmy jedno kółko… Załóżmy, że teraz *A* odpowiada *N*. To znaczy, że *B* odsyła do *O*, *C* do *P* itd. Ponieważ kółka są okrągłe, następną literą za *Z* jest *A* i ciąg zaczyna się od początku. Jest to szczególny szyfr przesuwający, znany jako *ROT13*, co w skrócie oznacza „rotację o 13 pozycji", gdyż w alfabecie litera *N* znajduje się 13 miejsc za literą *A*. Ponieważ angielski alfabet składa się z 26 liter, podwójne zaszyfrowanie czegoś za pomocą ROT13 daje w rezultacie tekst pierwotny (jako że 13 + 13 = 26).

[11] *Government Communications Headquarters* (Rządowe Centrum Łączności) — brytyjski odpowiednik amerykańskiej NSA.

Zabezpieczanie przez ukrywanie — przykład niewystarczalności

Zabezpieczanie przez ukrywanie występuje w świecie realnym częściej, niż powinno. Ilekroć chodzi o coś ważnego, w ogóle nie powinno mieć miejsca. Oto prawdziwy przykład tego, że stosowanie środków bezpieczeństwa jest równie ważne jak niewidoczne rozwiązania techniczne. Młoda, obiecująca firma wprowadziła na rynek nową, „inteligentną" żarówkę, sterowaną przez wi-fi. Miał to być element internetu rzeczy, a więc podłączania wszystkich urządzeń do sieci, tak by użytkownicy mogli nimi sterować ze smartfonu lub z komputera. Zamysł był taki, że po uruchomieniu pierwszej żarówki (do czego trzeba uwierzytelnić ją przez wi-fi, aby włączyła się do domowej sieci) kolejne porozumiewały się z „główną" żarówką i automatycznie podłączały do sieci bezprzewodowej. Co za wygoda! Te cudowne aparaciki tworzyły prywatną sieć typu „siatka" lub „krata" (ang. *mesh network*) do porozumiewania się pomiędzy sobą. Ponieważ sygnał bezprzewodowy rozchodzi się we wszystkie strony, włamywacze mogą go łatwo podsłuchać. Inżynierowie owej firmy wiedzieli o tym, dlatego zastosowali szyfrowanie „wojskowe", aby zapobiec podsłuchowi. Niestety, jako klucza szyfrującego — od którego zależy sukces całej operacji — użyli ustalonej, niezmiennej wartości! Właśnie tak: *wszystkie ich produkty działały z tym samym kluczem*. Pozostawał on jednak ukryty w pamięci żarówek, któż więc mógłby go stamtąd wydobyć? Oczywiście włamywacze. Wzięli jedną z takich żarówek, podłączyli druty do wewnętrznego układu komputerowego i wyciągnęli z niego klucz. Teraz włamywacz potrzebuje tylko podejść do cudzego mieszkania dostatecznie blisko, żeby „usłyszeć" komunikujące się pomiędzy sobą żarówki, a następnie może rozszyfrować łączność, aby poznać identyfikator i hasło do domowej sieci bezprzewodowej. Firma liczyła na to, że nikt nie będzie zadawał sobie trudu i grzebał w jej produktach, aby znaleźć klucz kodowy — typowe zabezpieczanie przez ukrywanie. Gdy klucz wyszedł na jaw (a więc przestał być ukryty), powstał haczyk na wszystkich nabywców tych żarówek. Firma opublikowała poprawkę do swojego oprogramowania, lecz teraz klienci muszą się zatroszczyć o zaktualizowanie kupionych żarówek w celu usunięcia słabego punktu… a to mało prawdopodobne.

Na rysunku 2.6 pokazano, jak to działa. Widać całe odwzorowanie alfabetu oraz metodę szyfrowania na przykładzie słowa „witaj".

Mój ulubiony popkulturowy przykład sekretnego pierścienia deszyfrującego pochodzi z klasycznego filmu *A Christmas Story*[12]. Główny bohater Ralphie Parker właśnie otrzymał przesyłkę z sekretną odznaką deszyfrującą i od teraz należał do Tajnego Koła Sierotki Ani. Na zakończenie każdej audycji z radiowego cyklu przygodowego pt. *Little Orphan Annie* (*Sierotka Ania*) lektor Pierre Andre podawał tajną, zaszyfrowaną wiadomość, którą mogły odcyfrować tylko dzieci posiadające odznakę. W tym przypadku szyfr odwzorowywał litery na liczby, więc na jednym kółku widniał alfabet, a na drugim — sekwencja liczb (rysunek 2.7)[13].

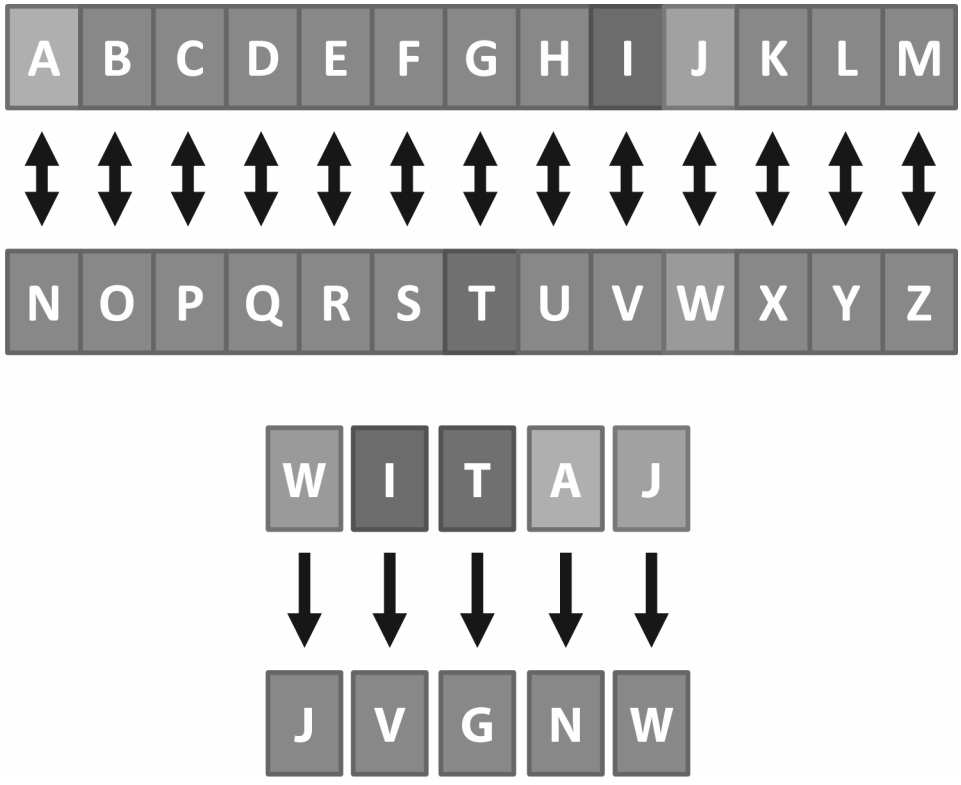
Aby rozszyfrować wiadomość, trzeba było znać ustawienie kółek, i Pierre poinformował swoich słuchaczy, żeby przekręcili tarcze na B-2. Innymi słowy, literze *B* odpowiadała liczba 2; to najprostsza możliwa zamiana, ponieważ *B* jest drugą literą alfabetu. Tak więc *A* reprezentuje 1, a *Z* — 26. Pierwsza wiadomość, którą otrzymał Ralphie jako członek tajnego koła, wyglądała następująco[14]:

2-5-19-21-18-5-20-15-4-18-9-14-11-25-15-21-18-15-22-1-12-20-9-14-5

[12] W Polsce wyświetlany pt. *Prezent pod choinkę — przyp. tłum.*

[13] Jest to moja osobista odznaka deszyfrująca, która pochodzi z A Christmas Story House and Museum (Dom i Muzeum *Prezentu pod choinkę*) w Cleveland w stanie Ohio. Jeżeli jesteś miłośnikiem tego filmu, koniecznie odwiedź to miejsce (*http://www.achristmasstoryhouse.com*)!

[14] Jak widać z rysunku, odznaka deszyfrująca nie była prawdziwym szyfrem przesuwającym, ale dla potrzeb ilustracyjnych upraszczam zagadnienie.



Rysunek 2.6. *Szyfr przesuwający ROT13*

Rysunek 2.7. *Odznaka deszyfrująca sierotki Ani z filmu Prezent pod choinkę*

Za pomocą swojej odznaki Ralphie z wysiłkiem odcyfrował przekaz. Wiemy, że 2 oznacza *B*, więc to będzie pierwsza litera wiadomości. Na piątym miejscu w alfabecie stoi *E*, zatem to będzie druga litera. Literą o numerze 19 jest *S* itd., aż otrzymujemy taki napis:

B-E-S-U-R-E-T-O-D-R-I-N-K-Y-O-U-R-O-V-A-L-T-I-N-E

W tym momencie Ralphie powoli odczytał wiadomość, dzieląc ją na słowa. „Pamiętaj… żeby… wypić… ovaltine". Ovaltine? Parszywa reklama?[15].

Teraz odwróćmy cały proces i zabawmy się w ciemnego typka. Przejąłeś tajną wiadomość i chcesz poznać jej treść. Jak zabrałbyś się do złamania szyfru? Czynności mające na celu poznanie szyfru noszą nazwę **„kryptoanaliza"**. Współcześnie szyfrowaniem zajmują się komputery i samodzielne złamanie szyfru w zasadzie wykracza poza możliwości zwykłego śmiertelnika, dawniej jednak szyfrowano ręcznie i łamano szyfry także ręcznie.

Zacznijmy kryptoanalizę od dokładnego przyjrzenia się szyfrogramowi. Najpierw musimy przyjąć pewne założenia. Załóżmy, że tekst jawny został napisany po angielsku oraz że każdy symbol kryptogramu odpowiada jednej literze angielskiego alfabetu. Te przypuszczenia mogą być błędne, ale jednym z najpotężniejszych narzędzi w arsenale łamacza kodów jest jak największa wiedza o tekście pierwotnym. Posiadanie uprzedniej wiedzy, nawet tylko prawdopodobnej, pozwala znacznie zmniejszyć wysiłek konieczny do rozszyfrowania tekstu.

Następnie powinniśmy zbadać szyfrogram w poszukiwaniu wzorców lub wskazówek. Widzimy liczby z zakresu 1 – 25. Ponieważ w języku angielskim używa się 26 liter, przyjmiemy, że mamy do czynienia z prostym szyfrem podstawieniowym, odwzorowującym litery od *A* do *Z* na liczby od 1 do 26.

W tym momencie zaczyna się robić ciekawie. Ponieważ założyliśmy, że tekst jawny napisano po angielsku, do złamania szyfru możemy spożytkować swoją wiedzę o tym języku. Okazuje się, że najczęściej występującą w nim literą jest *E*. Skąd to wiadomo? Cóż, większość ludzi nie ma powodów, by się tym interesować, ale łamacz szyfrów powinien znać takie statystyki. Gdy więc wziąć stosunkowo długi szyfrogram pochodzący z angielskiego tekstu jawnego, można mieć sporą dozę pewności, że najczęściej powtarzający się symbol odpowiada literze *E*. Następne pod względem częstości litery języka angielskiego to kolejno *T*, *A* i *O*. Zliczanie symboli użytych w szyfrogramie i próba dopasowania ich do kolejnych liter nazywa się **analizą częstotliwości**; tak więc częstość występowania danego znaku w kryptogramie (a więc jego liczebność w stosunku do innych symboli) pomaga odgadnąć odpowiadającą mu literę angielską.

Nasz szyfrogram jest dość krótki, zróbmy jednak analizę częstotliwości. Zliczając poszczególne wielkości liczbowe, stwierdzamy, że najczęściej powtarzają się 5, 15 i 18 — po trzy razy. Załóżmy więc, że jedna z liczb odpowiada literze *E*. Sprawdźmy każdą z nich. Przypuśćmy najpierw, że literze *E* odpowiada 15. Teraz zrobimy kolejne założenie, aby zobaczyć, czy nam się poszczęści: miejmy nadzieję, że ktokolwiek układał ten szyfr, nie wysilał się zanadto i po prostu oznaczył litery kolejnymi liczbami. Jeżeli więc $E = 15$, to $F = 16$, $G = 17$ itd. Według tego przyporządkowania łamacz podstawia wszystkie litery i otrzymuje poniższą wersję tekstu jawnego:

R-U-I-K-H-U-J-E-T-H-Y-D-A-O-E-K-H-E-L-Q-B-J-Y-D-U

Hm, nie wygląda to dobrze, ale przynajmniej wyeliminowaliśmy jedno z założeń. Jako ludzie leniwi trzymajmy się ich nadal i po prostu spróbujmy innego przyporządkowania. W szyfrogramie trzy symbole występowały po trzy razy, więc skoro 15 nie odpowiada literze *E*, to może 5 albo 18 będą pasować.

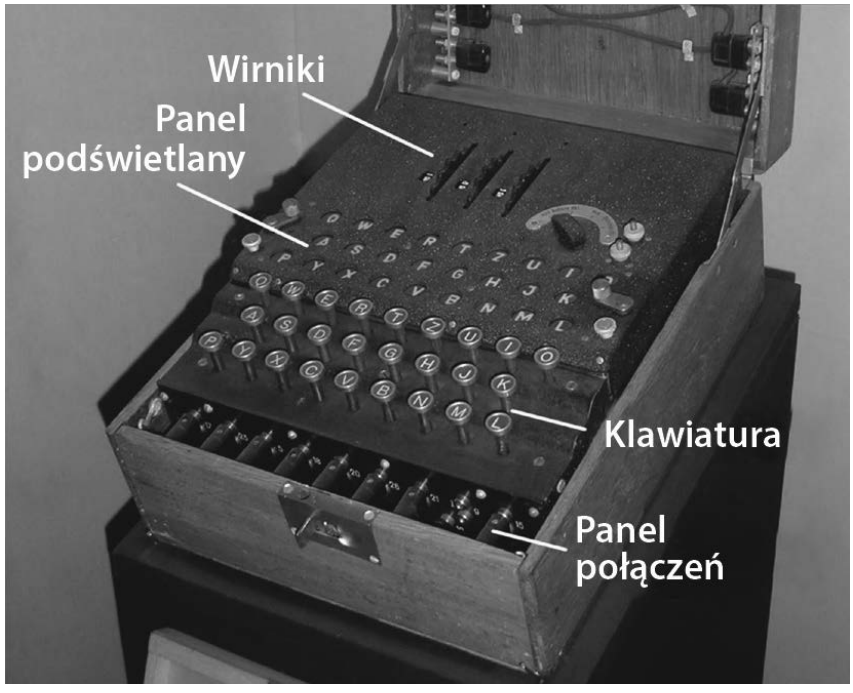
Jeżeli przyjmiemy, że $E = 5$, to zgodnie z pozostałymi założeniami otrzymujemy tekst:

B-E-S-U-R-E-T-O-D-R-I-N-K-Y-O-U-R-O-V-A-L-T-I-N-E

Udało się! Właśnie rozszyfrowaliśmy wiadomość! Hura! Gdyby szyfrogram zawierał również odstępy międzywyrazowe, moglibyśmy posłużyć się inną statystyką do pomocy. Najczęściej występującymi jednoliterowymi wyrazami w języku angielskim są zaimek *I* („ja") i przedimek nieokreślony *a*. Najczęstszym wyrazem trzyliterowym jest przedimek określony *the*. Wyrazy angielskie najczęściej zaczynają się od litery *S*. Znając więc granice wyrazów, zyskalibyśmy dużo więcej informacji, dzięki którym moglibyśmy ustalić odwzorowanie i złamać szyfr.

[15] Ovaltine — słodki napój na bazie wody i mleka z dodatkiem różnych składników, np. słodu, kakao, proszku jajecznego, serwatki, przeznaczony do picia na gorąco przed snem. Producent napoju w USA sponsorował audycje dla dzieci z cyklu o sierotce Ani i reklamował w nich swoje towary — *przyp. tłum.*

Oczywiście współczesna kryptoanaliza jest dużo bardziej skomplikowana. Dzisiaj do szyfrowania danych używa się komputerów i wysoce złożonych algorytmów. Niemniej wykonane przez nas ćwiczenie pozwala się zorientować, w jaki sposób atakujący mógłby próbować złamać kod. Jeden z najsłynniejszych takich ataków został dokonany w trakcie drugiej wojny światowej, kiedy Anglik Alan Turing i jego koledzy z Bletchley Park odcyfrowali (udoskonalając metody pierwotnie opracowane przez Polaków)[16] kody maszyny szyfrującej Enigma (rysunek 2.8) używanej przez Niemców. Jednakże twórcy i łamacze kodów odgrywają istotną rolę w całej historii, a ich działalność sięga wstecz co najmniej do Mezopotamii z 1500 r. przed Chr.[17].



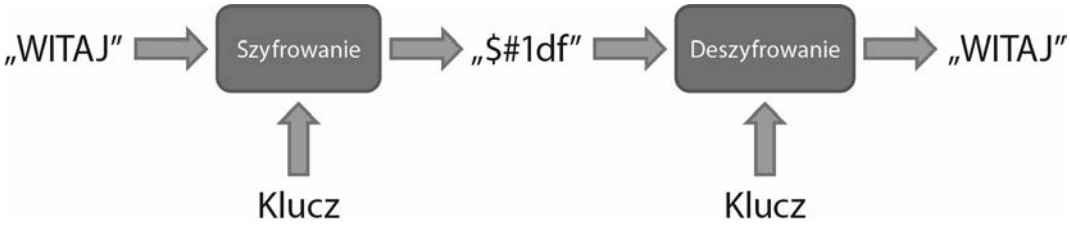
Rysunek 2.8. *Niemiecka maszyna szyfrująca Enigma z drugiej wojny światowej (zdjęcie Karsten Sperling)*

Nowoczesna kryptografia

Współczesne szyfry opierają się na pojęciu tajnego klucza. Bierzemy tekst jawny oraz jakiś klucz tekstowy (coś w rodzaju hasła) i przepuszczamy je przez algorytm szyfrujący. Rezultat wygląda całkiem niezrozumiale. W odróżnieniu od naszego prostego szyfru podstawieniowego, który omawialiśmy powyżej, szyfrogram może nie wynikać z bezpośredniego odwzorowania znaku na znak, a nawet może w ogóle nie mieścić się w zbiorze znaków języka angielskiego. Jeżeli jednak wziąć ten sam tajny klucz i zastosować algorytm odwrotny (deszyfrujący), to otrzyma się pierwotny tekst otwarty. Tego rodzaju szyfrowanie nazywa się **symetrycznym**, ponieważ zarówno do szyfrowania, jak i deszyfrowania służy ten sam klucz (rysunek 2.9).

[16] Zwłaszcza trzech matematyków: Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego — *przyp. tłum.*

[17] Pracę Turinga wspaniale przedstawiono w oscarowym filmie *The Imitation Game* (w Polsce pt. *Gra tajemnic* — *przyp. tłum.*). Jeżeli historia kryptoanalizy fascynuje Cię tak samo jak mnie, to gorąco polecam książkę: Simon Singh, *Księga szyfrów*, tłum. Piotr Amsterdamski, Świat Książki, Warszawa 2003.



Rysunek 2.9. *Przebieg szyfrowania symetrycznego*

Trzeba podkreślić, że same algorytmy szyfrujące i deszyfrujące są upublicznione i dobrze znane. To znaczy, że proces przekręcania i przywracania (odkręcania?) tekstu *nie jest tajny*. Dawniej twierdzono, że byłoby bezpieczniej, gdyby utajnić algorytmy. Intuicyjnie wydaje się to słuszne, tak jak u magika, który nie zdradza sposobu, w jaki robi swoje sztuczki. Ale w tym sedno — nie jest to prawdziwa magia, jeśli istnieje sztuczka. Skoro można rozszyfrować wiadomość tylko na podstawie znajomości metody jej zaszyfrowania, to cały proces zależy od tego, że ów sekret nigdy nie zostanie ujawniony ani odkryty — nie tylko w przypadku jednej osoby, ale każdego, kto kiedykolwiek go użył, a więc i każdego komunikatu lub pliku kiedykolwiek zaszyfrowanego za pomocą tego algorytmu. W dzisiejszym świecie to nie wystarcza. Każdy wartościowy schemat kodowania musi pozostawać bezpieczny, nawet jeśli wszystkie szczegóły jego działania są powszechnie znane. Ponadto dzięki temu eksperci mogą dokładnie zanalizować i sprawdzić algorytm.

Jeżeli używasz szyfru do zakodowania osobistych danych, takich jak prywatny dziennik, to szyfr symetryczny działa całkiem dobrze. Wybierasz i zapamiętujesz hasło, którego używasz jako tajnego klucza do zakodowania notatek w diariuszu. Klucz jest znany tylko Tobie i jeżeli wybrałeś mocne hasło, tekst pozostaje nieczytelny dla osób postronnych. Ale znowu trzeba wziąć pod uwagę przestrogę, którą tu wtrąciłem. Musisz wybrać mocne hasło. Omówię to szerzej w jednym z dalszych rozdziałów, a na razie powiem tyle: komputery są tak potężne, że mogą zgadywać miliony, a nawet miliardy haseł na sekundę, aby dobrać się do Twojego dziennika, więc jeżeli wybrałeś imię swojej wnuczki albo nazwę ulubionej drużyny piłkarskiej, to nie wystarczy.

Szyfrowanie symetryczne można sobie wyobrazić na podobieństwo kufra z solidną kłódką: masz do niej klucz i tylko Ty możesz ją otworzyć. Nieważne, czy inni przejmą kufer — dopóki nie zdobędą klucza, nie dostaną się do zamkniętego wewnątrz dziennika. Nie powinno nawet mieć znaczenia, czy znają budowę mechanizmu zamknięcia. Aby ta analogia w pełni pasowała do współczesnej kryptografii, trzeba dodać, że kufer musi być idealnie szczelny, a kłódka rzeczywiście niemożliwa do otworzenia wytrychem. Najważniejszy zatem jest klucz. Jeżeli masz go u siebie i nie istnieją inne jego egzemplarze, tylko Ty możesz otworzyć kłódkę, a więc i dostać się do zawartości.

Możliwość zamknięcia diariusza w kufrze to dobra rzecz, niemniej w świecie realnym zdarzają się inne sytuacje wymagające zabezpieczenia. Według pojęć kryptografii omówiliśmy przypadek *danych w spoczynku*, ale co powiedzieć o *danych w ruchu*, czyli o ich przesyłaniu? W tym nowym scenariuszu istotnie zwiększa się liczba ludzi, którzy potrzebują dostępu do informacji — wtedy była to jedna osoba, teraz jest więcej niż jedna. Dodaliśmy też wymóg, że przesyłamy te dane na pewną odległość, za pośrednictwem osób postronnych, którym niekoniecznie ufamy. Aby posłużyć się w tym celu szyfrem symetrycznym, należałoby przekazać tajny klucz zamierzonemu odbiorcy. Ale jak to zrobić bezpieczną metodą? Nie można go po prostu wysłać, gdyż ktoś mógłby go po drodze przechwycić. Można by go podyktować przez telefon, ale jeśli działa podsłuch? Trzeba by spotkać się twarzą w twarz i wyszeptać klucz do ucha, to zaś może się okazać niewygodne albo wręcz niewykonalne.

Na szczęście w połowie lat 70. ubiegłego wieku grupa naprawdę bystrych badaczy wymyśliła całkiem nowe podejście do szyfrowania, które zrewolucjonizowało bezpieczną komunikację i szyfrowanie w ogóle. W istocie rzeczy wynaleźli kłódkę z dwoma kluczami — publicznym do zamykania i prywatnym do otwierania. Nazywa się to **szyfrowaniem asymetrycznym**, ponieważ do szyfrowania i deszyfrowania służą różne klucze. W tym schemacie kopie klucza publicznego można rozdawać jak popadnie, podczas

gdy klucz prywatny należy wyłącznie do właściciela. Każdy, kto chce wysłać wiadomość, używa publicznego klucza odbiorcy do jej zakodowania, a następnie odbiorca stosuje swój klucz prywatny do jej zdeszyfrowania. Błyskotliwe i eleganckie rozwiązanie! Dzięki tej metodzie dwie osoby mogą się bezpiecznie porozumiewać bez konieczności fizycznej wymiany jednego wspólnego klucza.

Można to sobie przedstawić następująco. Powiedzmy, że Alicja chce wysłać jakieś poufne dokumenty do swojego kolegi Boba na drugim końcu kraju[18]. Wprawdzie mogłaby wsiąść w samolot i doręczyć je osobiście, lecz byłby to sposób kosztowny i niewygodny; dlatego Alicja zamierza wysłać je zwykłą pocztą. Ma zgrabne pudełko zamykane na kłódkę, tyle że nie może po prostu wysłać klucza Bobowi — bądź co bądź ktoś po drodze mógłby zrobić sobie kopię. Jako kobieta inteligentna Alicja wie, że nie musi polegać na mechanizmie zabezpieczenia symetrycznego, ale może skorzystać z metody asymetrycznej. W tym celu prosi Boba, żeby przysłał jej otwartą kłódkę, po czym używa jej do zamknięcia pudełka. Nie potrzebuje klucza, gdyż każdy może zamknąć kłódkę, po prostu ją zaciskając. Jednakże tylko Bob będzie mógł ją otworzyć, ponieważ tylko on ma klucz. Jeżeli Alicja byłaby dość bystra, mogłaby też włożyć do pudełka jedną ze swoich kłódek, tak aby Bob odesłał jej dokumenty z użyciem tej samej metody.

Jak to wszystko odnosi się do naszych komputerów? Jak mówiliśmy w tym rozdziale, ilekroć wysyłamy wiadomość elektroniczną, oglądamy film na YouTubie, robimy zakupy w sklepie internetowym, opłacamy rachunki przez internet albo po prostu krążymy po sieci, tym samym wysyłamy dane i odbieramy je z internetu. Dane te zostają podzielone na kawałki zwane **pakietami** i te pakiety odbywają podróż z naszego do innego komputera (albo w odwrotnym kierunku). Po drodze mogą przechodzić przez dziesiątki komputerów, ruterów, przełączników i serwerów. Należy pamiętać, że takie cyfrowe przesyłki są podobne raczej do pocztówek niż do listów — to znaczy, że każdy człowiek (bądź komputer) po drodze, który na nie spojrzy, zobaczy całą ich treść.

W niektórych przypadkach można się z tym pogodzić, ale oczywiście bywają sytuacje — np. korzystanie z banków i sklepów — wymagające bezpiecznej łączności. Jednym z protokołów komunikacyjnych używanych w internecie jest protokół przesyłania hipertekstu (ang. *Hypertext Transfer Protocol* — HTTP). Widziałeś ten skrót wiele razy w adresach sieciowych, takich jak *http://yahoo.com/*. Jeżeli jesteś spostrzegawczy, zauważysz, że czasami nie jest to http, ale https; dodatkowa litera *S* znaczy *secure*, czyli „bezpieczny". Kiedy przeglądarka internetowa komunikuje się przez HTTPS, powinna wyświetlać dodatkowy wskaźnik — taki jak ikonka kłódki, która informuje, że łączność z daną witryną jest zabezpieczona. Wówczas niezależnie od tego, jakimi drogami pakiety przemieszczają się po internecie, tylko komputer docelowy może je odcyfrować.

Uwierzytelnianie oraz integralność wiadomości

Hura, znamy szyfrowanie asymetryczne! A więc problem z głowy? Niezupełnie. To nie wystarcza do tego, żeby nikt nie podejrzał treści naszego komunikatu. Przywołajmy analogię z udziałem Boba i Alicji. Skąd Alicja wie, że faktycznie wysyła dokumenty do Boba? Gdybym był sprytnym szpiegiem, mógłbym się zainstalować między Alicją a Bobem i grać wobec nich obojga rolę drugiej strony; byłby to atak typu „człowiek w środku" (ang. *man-in-the-middle attack*). Sedno sprawy leży w przechwytywaniu komunikacji między Alicją a Bobem. Załóżmy, że szpieg przeniknął do przedsiębiorstwa pocztowego i zyskał dostęp do całej korespondencji między nimi dwojgiem. Gdy Bob wysyła otwartą kłódkę do Alicji, szpieg przejmuje przesyłkę i podmienia kłódkę na swoją. Nie posiada klucza do kłódki Boba, ale nie jest mu potrzebny. Gdy Alicja wysyła do Boba poufne dokumenty, nieświadomie zamyka pudełko na kłódkę szpiega. Ten znowu przejmuje przesyłkę i otwiera ją swoim kluczem. Jeżeli chce być naprawdę przebiegły, może skopiować dokumenty, po czym zamknąć pudełko na kłódkę Boba (którą sobie uprzednio zachował). Bob otrzymuje pudełko, otwiera je swoim kluczem i błędnie zakłada, że materiały pozostały utajnione wobec osób postronnych.

[18] Alicja i Bob to postacie dobrze znane w świecie kryptografii. Imion tych używa się w scenariuszach komunikacyjnych zamiast określeń „strona A" i „strona B".

Jako człowiek w środku szpieg może powodować wszelkiego rodzaju szkody. Przykładowo mógłby nie tylko kopiować treść komunikatów i zawartość przesyłek, lecz także ją *zmieniać*. Powiedzmy, że Bob poprosił Alicję o przysłanie 10 tys. złotych gotówką. Przechwyciwszy wiadomość, szpieg zamienił kwotę na 20 tys. Gdy Alicja wysyła pieniądze, szpieg zabiera połowę, a pozostałe 10 tys. wysyła dalej do Boba, który dostanie dokładnie tyle, ile chciał, i nikt się nie zorientuje w oszustwie. Co więcej, szpieg mógłby zastąpić banknoty falsyfikatami i zgarnąć całość dla siebie!

Jak rozwiązać ten problem? Potrzebujemy teraz jakiegoś sposobu na to, by Alicja bez cienia wątpliwości przekonała Boba nie tylko o tym, że wyłącznie ona jedna mogła nadać przesyłkę, lecz także o tym, że zawartość nawet w najmniejszym stopniu nie uległa zmianie. W tym celu powinniśmy zastosować, oprócz kluczy prywatnych i publicznych, nowe narzędzie o nazwie **kryptograficzna funkcja skrótu**[19] (wiem, że brzmi to bardzo technicznie… ale po prostu zdaj się na mnie).

Przede wszystkim dla uproszczenia pomówmy tylko o wysyłce dokumentu od Alicji do Boba. Alicja ma zbiór kartek, które chce wysłać Bobowi w bezpieczny sposób, zapewniający, że nikt ich nie przejmie i nie podmieni po drodze. Jakiego narzędzia do tego potrzebujemy?

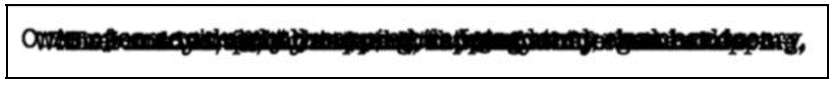
Powiedzmy, że istnieje aparat do dokumentów, który skutecznie scala wiele stronic w jedną. Układa wszystkie karty w stos i prześwietla je magicznym promieniem, w istocie chwytając cień całego tekstu na stronach i łącząc go w jeden, złożony obraz „rentgenowski". Nazwijmy takie urządzenie „papierentgenem".

Przekonajmy się na prostym przykładzie, jak działa ten wspaniały aparat. Na rysunku 2.10 widać pięć zdań mniej więcej równej długości.

Once upon a midnight dreary, while I pondered, weak and weary,
Over many a quaint and curious volume of forgotten lore--
While I nodded, nearly napping, suddenly there came a tapping,
As of some one gently rapping, rapping at my chamber door.
"'Tis some visiter," I muttered, "tapping at my chamber door--
Only this and nothing more."

Rysunek 2.10. *Pięć zdań*

Teraz umieśćmy je kolejno jedno na drugim (rysunek 2.11).



Rysunek 2.11. *Pięć zdań jedno na drugim*

To jest papierentgenowski obraz wszystkich pięciu zdań — scalenie ich wszystkich, ułożonych kolejno na sobie. Obraz taki wykazuje kilka interesujących własności.

Po pierwsze, jest całkowicie niepowtarzalny i daje się przewidzieć na podstawie danych wejściowych. Jedynym sposobem na uzyskanie dokładnie takiego obrazu papierentgenowskiego jest użycie dokładnie tych samych wyrazów w tej samej kolejności. Gdyby zmienić, dodać bądź usunąć choćby jeden znak, obraz wynikowy także uległby zmianie.

Po drugie, z tego obrazu nie da się odczytać pierwotnych pięciu zdań. Mamy do czynienia z konwersją „stratną" — w trakcie tworzenia obrazu informacja się gubi. Taka konwersja przebiega więc jednokierunkowo:

[19] Spotyka się też nazwę „funkcja mieszająca" — *przyp. tłum.*

mając dane wejściowe (pięć zdań), zawsze można odtworzyć wynik (obraz papierentgenowski), ale znając wynik, nie można odzyskać danych wejściowych.

Wreszcie w tym procesie powstaje coś o niewielkich, stałych rozmiarach. Jeżeli poddalibyśmy takiemu procesowi zbiór kartek jakiejś książki, to w wyniku otrzymamy jedną stronicę, niezależnie od liczby stronic wejściowych. Ściskamy więc cały tom do rozmiarów pojedynczego arkusza.

Tak więc nasz aparat papierentgenowski może przetworzyć dowolny zbiór stronic w jeden niepowtarzalny obraz ich wszystkich — w pojedynczą stronę, która reprezentuje dziesiątki albo i setki stron wejściowych.

A teraz podarujmy to sprytne urządzenie Bobowi i Alicji! Dzięki niemu Alicja mogłaby prześwietlić swój dokument i dołączyć do niego obraz wynikowy. Po odebraniu przesyłki Bob może zastosować swój aparat do prześwietlenia otrzymanego dokumentu, a następnie porównać uzyskany obraz z obrazem przysłanym przez Alicję. Jeżeli są identyczne, Bob ma pewność, że dokument w żadnym szczególe nie został zmieniony. Gdyby szpieg w jakikolwiek sposób zaingerował w treść dokumentu — usunął jedną kartę, użył korektora biurowego, wymienił kartę lub dodał nową — aparat papierentgenowski wytworzyłby odmienny obraz. Toteż nawet jeżeli szpieg mógłby przechwycić i obejrzeć przesyłkę, w żaden sposób nie zdołałby niepostrzeżenie zmienić dokumentu.

Zasadniczo w taki sposób działa kryptograficzna funkcja skrótu. Wprowadza się porcję tekstu, aby w wyniku otrzymać krótki ciąg znaków. Gdy w tekście wejściowym zmienić choć jedną literę, wynik całkowicie się zmieni. W praktyce niemożliwe jest też znalezienie innego zestawu wyrazów, dla którego funkcja skrótu dawałaby taki sam wynik.

Sprawdźmy powyższą teorię. Gdy potraktujemy całą tę książkę (w oryginalnej postaci angielskojęzycznej) jako dane wejściowe, po zastosowaniu popularnej kryptograficznej funkcji skrótu o nazwie SHA-256 otrzymamy poniższy wynik:

4a939d318741a70f67af9e3fbb28d5f2ebeccc799c0ee6bf0de59628bbcc7178

A oto wynik po zamianie tylko *jednego znaku*:

1fd4094a7780cdc18c54c339bc4011669656455e7a64a32b4769aafa6516e6b7

Czy widać jakiekolwiek podobieństwo między nimi? Nie. Są całkowicie, wyraźnie różne. To jest nawet lepsze od naszego papierentgena — jedna drobna zmiana na wejściu prowadzi do ogromnej zmiany na wyjściu.

Jeżeli już wprowadziłem Cię w należycie paranoiczny stan, to spostrzeżesz, że tu nadal kryje się pewien problem. Dlaczego szpieg, oczywiście mający dostęp do każdej przesyłki, nie mógłby po prostu wymienić obrazu papierentgenowskiego, który Alicja dołączyła do dokumentu? Mógłby zmienić treść, wytworzyć obraz nowego dokumentu i dołączyć *tenże* obraz do przesyłki. W tym momencie wraca do gry kryptografia klucza publicznego i również w tym miejscu załamuje się analogia do zwykłej kłódki.

Teraz musimy sobie wyobrazić innego rodzaju kłódkę, jaka w rzeczywistości nie istnieje; nazwijmy ją *superkłódką*. Ma ona dwa otwory na klucze: jeden do zamykania, a drugi do otwierania. Klucze do obsługi tej specjalnej kłódki zawsze występują w parach. Jeden z nich jest kluczem publicznym, który można kopiować i rozdawać wszystkim chętnym, drugi zaś — kluczem prywatnym, który nie ma innego egzemplarza i należy tylko do właściciela. Kłódkę można zamknąć jednym bądź drugim z nich, ale potem da się ją otworzyć tylko drugim z pary. Ten sam klucz nie może służyć do obydwu czynności: jeden zamyka, a drugi otwiera. Pasują dowolne dwa klucze, co stanowi o uroku superkłódki, ale muszą należeć do tej samej pary. Nadążasz?

Superkłódkę można kupić w każdym dobrym sklepie, ale żeby otrzymać parę kluczy, trzeba udać się do wyjątkowego ślusarza — oczywiście superślusarza. Wykona on dwa pasujące klucze: publiczny i prywatny. Zachowa również egzemplarz klucza publicznego i bezpłatnie zrobi jego kopię dla każdego, kto zechce. Wreszcie ślusarz ręczy za to, że wykonał klucze specjalnie dla Ciebie, i może udowodnić, że wręczył Ci osobiście pojedynczy klucz prywatny. W gruncie rzeczy superślusarz potwierdza i poręcza Twoją tożsamość.

Dobrze… Zakładając, że podążałeś za tokiem myśli i przyswoiłeś ją sobie, możemy teraz powiedzieć dwie ważne rzeczy. Po pierwsze, jeżeli zamknę superkłódkę należącym do kogoś kluczem publicznym,

to ów ktoś będzie jedynym na świecie człowiekiem, który potrafi ją otworzyć, ponieważ jedynie on posiada klucz prywatny. A zatem wiem niezawodnie, że gdybym zamknął tę specjalną kłódkę jednym z publicznych kluczy Alicji (który mógłbym dostać od ślusarza), wtedy byłbym pewien, że Alicja, i tylko ona, mogłaby ją otworzyć. Po drugie, gdybym otrzymał coś zamkniętego na kłódkę, która dałaby się otworzyć kluczem publicznym Alicji, to by znaczyło, że musiała ją zamknąć sama Alicja — miałbym więc pewność, że cokolwiek znajduje się w zamkniętym pudełku, naprawdę pochodzi od Alicji[20].

Teraz mamy wszystkie narzędzia potrzebne do rozwiązania problemu i jesteśmy na ostatniej prostej. Wytrzymaj jeszcze chwilę…

Raz jeszcze zacznijmy od początku i zobaczmy, jak działa nasz nowy system. Alicja zamierza wysłać Bobowi jakieś poufne dokumenty. Chce zagwarantować, że nikt inny ich nie przeczyta, nawet jeśliby zdołał przechwycić je po drodze. Chce również zapewnić, by bez cienia wątpliwości Bob wiedział, że to Alicja je wysłała. Wreszcie na wszelki wypadek chce też umożliwić Bobowi sprawdzenie, czy dokumenty nie zostały w żaden sposób zmienione.

Tak więc Alicja i Bob kupują sobie po aparacie papierentgenowskim i superkłódce. Obydwoje zabierają swoje prywatne klucze do domu i zamawiają przez internet albo kupują u ślusarza po egzemplarzu publicznego klucza korespondenta. Alicja wkłada do pudełka tajne materiały, a następnie prześwietla je aparatem. Uzyskany obraz wkłada do drugiego, mniejszego pudełka, które następnie zamyka na jedną ze swoich superkłódek za pomocą klucza prywatnego. Ponieważ pudełko zostało zamknięte kluczem prywatnym Alicji, każdy może je otworzyć jednym z jej bezpłatnych kluczy publicznych. W tym momencie nie chodzi o ochronę zawartości (czyli obrazu papierentgenowskiego), lecz o poświadczenie, że to Alicja prześwietliła dokumenty, a więc też nadała przesyłkę. Teraz Alicja wkłada małe pudełko wraz z dokumentami do dużego i zamyka je na drugą superkłódkę, używając publicznego klucza Boba. Od tej chwili duże pudełko może otworzyć wyłącznie Bob. Alicja ufnie powierza paczkę nowemu listonoszowi, który jest szpiegiem.

Gdy Bob otrzymuje pudełko, otwiera je swoim kluczem prywatnym. Wyjmuje mniejsze pudełko, zawierające obraz papierentgenowski, i otwiera je kluczem publicznym Alicji. Ponieważ superkłódka dała się otworzyć za pomocą tego klucza, Bob wie, że to Alicja zamknęła mniejsze pudełko na superkłódkę. Następnie wyciąga swój aparat papierentgenowski i prześwietla odebrane dokumenty. Obraz pokrywa się z tym, który przysłała Alicja! Teraz Bob wie, że nawet jeśli pudełko zostało w jakiś sposób naruszone, to jego zawartość się nie zmieniła.

Dotarliśmy do celu! Zasadniczo takie same mechanizmy znajdują dzisiaj zastosowanie w zabezpieczaniu niemal całej komunikacji internetowej. Istnieje wiele różnych algorytmów oraz ich skomplikowanych kombinacji, ale podstawowe zasady pozostają bez zmian. Obydwa klucze, publiczny i prywatny, są w niewidoczny sposób ustalane przez komputer użytkownika (klient) i komputer odległy (serwer). Chociaż można by utworzyć taką parę kluczy i zarejestrować je w oficjalnej agencji (czyli u ślusarza z naszej analogii), większość przeciętnych ludzi tego nie potrzebuje. Potwierdzamy swoją tożsamość podczas zakładania konta internetowego, a potem używamy identyfikatora lub adresu elektronicznego w połączeniu z hasłem.

Uwierzytelnianie, autoryzacja, ewidencjonowanie

Podstawy bezpieczeństwa mamy już prawie za sobą, ale musimy poświęcić jeszcze chwilę trzem sprawom: uwierzytelnianiu (ang. *authentication*), autoryzacji lub nadawaniu uprawnień (ang. *authorization*) oraz ewidencjonowaniu (ang. *accounting*). Powyżej omówiliśmy uwierzytelnianie, więc pomówmy krótko o dwóch pozostałych.

Posiadając już mechanizmy do jednoznacznej identyfikacji użytkownika (uwierzytelnianie), możemy ograniczyć dopuszczalny dla niego zakres czynności. Na przykład pracownicy dużych przedsiębiorstw otrzymują osobiste identyfikatory, które po przyłożeniu do czytnika otwierają wejścia do różnych obszarów

[20] Z tego wynika tzw. niezaprzeczalność (ang. *nonrepudiation*). Ten wymyślny termin prawniczy oznacza w zasadzie tyle, że Alicja nie może wiarygodnie zaprzeczyć, iż coś podpisanego „cyfrowo" jej kluczem prywatnym pochodzi od niej.

na terenie zakładu. Taki identyfikator zapewnia uwierzytelnienie pod warunkiem, że pozostaje w posiadaniu jedynie tej osoby, której został przydzielony. Można jej zamknąć bądź otworzyć wstęp na określone obszary w ten sposób, że identyfikator będzie odblokowywał tylko niektóre wejścia. Dzięki temu można podzielić teren na strefy o różnym stopniu dostępności. Wiedza o tym, że tylko garstka ludzi ma wstęp na dany obszar, pozwala zacieśnić krąg podejrzanych np. w wypadku kradzieży.

Tego systemu można również używać do rejestrowania, kto wchodzi do strefy o ograniczonym dostępie i przez jaki czas tam przebywa. To jest trzecia zasada — ewidencjonowania. Gdy z pracowni o ograniczonym dostępie zginie nowy sprzęt laboratoryjny, wtedy straż przemysłowa może sprawdzić, kto przebywał w tym pomieszczeniu w czasie zgłoszonego zdarzenia.

Nowsze nie musi być lepsze

W dziedzinie bezpieczeństwa utrzymuje się nieustające napięcie między skłonnością do używania najnowszej, najwspanialszej techniki a nieufnością wobec wszystkiego, co nie przeszło wystarczającej próby czasu. Powiedzmy, że Twój zamek oblega rozwścieczona zgraja, a ja oferuję Ci nowoczesne, magiczne pole siłowe, które według moich zapewnień wytrzyma więcej od każdego muru z kamieni. Czy od razu zburzysz mury zamku i zainstalujesz pole siłowe, polegając wyłącznie na moim słowie? Raczej nie. A gdybym pokazał Ci tomy wyników z laboratorium, w którym porównywałem swoje pole z murem kamiennym pod względem wytrzymałości na symulowane ataki? Jeżeli naprawdę troszczysz się o swoje bezpieczeństwo, to też nie wystarczy. Niemniej gdyby moja oferta rzeczywiście przewyższała to, co obecnie posiadasz, jej zlekceważenie byłoby błędem. Jak byś zatem postąpił?

Cóż, prawdopodobnie zastosowałbyś nowe pole siłowe *oprócz* istniejących murów i wypróbował je w trakcie prawdziwego najazdu prawdziwych wrogów. Najpewniej też postępowałbyś tak przez dłuższy czas, zanim całkowicie zdałbyś się na to nowe rozwiązanie. Kamienne mury znasz i pokładasz w nich zaufanie. Wiesz, jak zostały zbudowane i jak należy je budować, ponieważ uczestniczyłeś w tym wielokrotnie. Znasz ich słabe miejsca i obmyśliłeś, jak je podeprzeć. Ale to nowe pole siłowe… nigdy go nie używano. Nie wiadomo, jak sprawdzi się w warunkach rzeczywistych. A jeśli twórca przeoczył coś istotnego? Może pole działało świetnie w kontrolowanym środowisku laboratoryjnym, ale zawiedzie w rzeczywistym świecie, w którym wiele zmiennych wymyka się ludzkiej kontroli, np. nieustający i nieograniczony dostęp do magicznej energii.

To samo dotyczy bezpieczeństwa. Nowe schematy szyfrowania, systemy uwierzytelniania i metody zabezpieczeń na ogół są traktowane nieufnie, dopóki nie popracują co najmniej przez parę lat. Dzięki temu niezależne zespoły specjalistów mają czas na wypróbowanie nowości w rzeczywistym świecie. Zaproponowanie nowego algorytmu szyfrującego, który na papierze jest matematycznie poprawny, to cenna rzecz, ale całkiem czymś innym jest zastosowanie go w sprzęcie i oprogramowaniu.

Wiedza o narzędziach i procesach bezpieczeństwa cybernetycznego jest o wiele szersza, ale ten rozdział zapoznał Cię z najważniejszymi pojęciami i koncepcjami z tej dziedziny.

Prywatność i śledzenie

Nie sposób omawiać bezpieczeństwa komputerowego, nie wspominając o prywatności. Jak mówiliśmy we wcześniejszych partiach bieżącego rozdziału, ciemne typki mające dostęp do Twoich prywatnych danych mogą dużo łatwiej złamać Twoje hasła lub podszyć się pod Ciebie (kradzież tożsamości). Choćby z tych względów należy bardzo ostrożnie udostępniać informacje o sobie takim serwisom jak Google, Facebook, Instagram, Twitter, LinkedIn itp.

Ale w prywatności chodzi o coś więcej niż świadome i dobrowolne ujawnianie. Naprawdę trzeba się bać o to, co każdego dnia rozpowszechniamy bezwiednie. Kartami kredytowymi i debetowymi wygodnie płaci się za nabyte towary, zarówno przez internet, jak i w budynkach sklepowych. Niemniej MasterCard, Visa i American Express wiedzą, gdzie i co kupujemy oraz ile pieniędzy wydajemy. Więksi detaliści również przechowują takie informacje.

Po skandalu z Cambridge Analytica nikogo nie powinno dziwić, ile informacji na nasz temat gromadzą serwisy społecznościowe w rodzaju Facebooka i LinkedIn. Zapewne też zdajesz sobie sprawę, że Google wie jeszcze więcej od każdego z nich. Google to nie jest wyszukiwarka internetowa, serwis pocztowy ani magazyn dokumentów… Google to przedsiębiorstwo reklamowe i kropka. Ponad 90% jego dochodów pochodzi z reklam, które mogą kosztować więcej, ponieważ są dobrze dopasowane. A są dobrze dopasowane dlatego, że Google wie niewyobrażalnie dużo o nas wszystkich.

Jako konsument powinieneś uświadomić sobie jedno:

Jeżeli produkt jest darmowy, to najpewniej Ty nim jesteś.

To znaczy, że wszystkie „bezpłatne" serwisy internetowe muszą gdzieś zarabiać. Jeżeli oferują coś bezpłatnie, to muszą zarabiać na czymś innym.

Może nie jesteś świadom tego, że wiele z tych przedsiębiorstw odsprzedaje innym Twoje dane. Takie firmy nazywamy **maklerami danych**. Widziałem szacunki, według których jest ich od 2500 do 4000 w samych Stanach Zjednoczonych. Działają one w zasadzie bez uregulowań prawnych (przynajmniej w czasie pisania tej książki… wkrótce może się to zmienić). Nie posiadasz swoich danych, a przeważnie nawet nie możesz się z nimi zapoznać. Zastanawiałeś się, dlaczego w różnych sklepach proponują „karty lojalnościowe"? Ilekroć przedkładasz taką kartę, pozwalasz sprzedawcy powiązać wszystkie Twoje zakupy z Twoją osobą. Te informacje prawie na pewno zostaną użyte do przedstawienia Ci lepiej dopasowanych ofert, a prawdopodobnie też odsprzedane innym podmiotom.

Do najcenniejszych konsumentów zaliczają się kobiety, które niedawno zaszły w ciążę. Młodzi rodzice wydają mnóstwo pieniędzy i wyrobienie w nich przywiązania do marki na tym etapie jest dla sprzedawców niezwykle ważne. W lutym 2012 r. magazyn „Forbes" opublikował reportaż o tym, jak Target trafnie przewidział, że pewna kobieta w jednym z gospodarstw domowych zaszła w ciążę, na podstawie rodzajów zamawianych przez nią produktów: bezzapachowego olejku i mydła, dużych ilości wacików, nawilżanych chusteczek oraz szczególnych suplementów witaminowych. Kierując się „wysokim prawdopodobieństwem ciąży", Target z własnej inicjatywy wysłał owej klientce talony na produkty dla dzieci. Na nieszczęście „kobieta" okazała się kilkunastoletnią uczennicą szkoły średniej mieszkającą z rodzicami, a jej ojciec jeszcze o niczym nie wiedział. Co do niektórych szczegółów wymienionych w reportażu wysunięto wątpliwości, lecz nie zmienia to faktu, że cała sytuacja wynikła z masowego gromadzenia i kojarzenia danych. W takim świecie obecnie żyjemy, a dzieje się coraz gorzej.

Wprawdzie deklarowanym celem zbierania tych informacji i tworzenia dokładnych profili osobowych jest dostarczanie reklamodawcom rzekomo anonimowych zestawień demograficznych, lecz trzeba zdawać sobie sprawę, że nie mamy żadnej realnej kontroli nad handlem tymi danymi. Możemy spróbować „zgłosić rezygnację", tyle że zastosowanie się do naszego życzenia — nie tylko w tej chwili, ale na zawsze — zależy od dobrej woli tych działających poza prawem przedsiębiorstw. Nie dość na tym: trzeba wiedzieć, że skoro ktoś przechowuje te wszystkie informacje, to rząd i jego agendy również zyskują do nich dostęp i zapewne nawet nie potrzebują nakazu sądowego, aby je otrzymać. Zresztą niektóre z tych danych możesz sprawdzić sam. Twój adres IP pozwala stwierdzić, kto jest Twoim operatorem internetowym (ISP) i gdzie fizycznie się znajdujesz (przynajmniej z dokładnością do kraju i miasta)[21].

Aby do reszty Cię zgorszyć, muszę powiedzieć coś jeszcze: nawet jeżeli opłacisz jakąś usługę, to nie masz pewności, że operator nie zechce dodatkowo zarabiać na Twoich danych osobowych. Kilka lat temu wyszło na jaw, że amerykańskie przedsiębiorstwa telekomunikacyjne AT&T oraz Verizon Communications generowały specjalne informacje pozwalające śledzić aktywność użytkowników w internecie. Ilekroć ktoś przeglądał sieć za pomocą smartfonu, obydwie firmy opatrywały wszystkie jego żądania znacznikiem (czasami określanym jako *supercookie*), widocznym dla każdej odwiedzanej przezeń witryny. Znacznik okresowo się zmieniał, dzięki czemu AT&T i Verizon mogły sprzedawać abonamenty na aktywność internetową użytkowników. Ale nawet gdy serwisy nie płacą za takie informacje, mogą używać owego identyfikatora do śledzenia. Jeżeli mają jakiś inny sposób na niezależne ustalanie tożsamości użytkowników,

[21] Z takiej usługi można skorzystać pod różnymi adresami, m.in.: *http://kodit.pl/geolokalizacja*, *http://www.digipedia.pl/ip/*, *https://pl.infobyip.com/*, *http://www.ip.dbox.pl/pl/*, *https://speedtestonline.pl/geolokalizacja-sprawdzenie-adresu-ip/*.

to na jedno wychodzi. Dobra wiadomość jest tylko taka, że śledzenie odbywa się jedynie w trakcie korzystania z internetu za pośrednictwem sieci komórkowej i jedynie wówczas, kiedy łączność jest nieszyfrowana. Jeżeli korzystamy z witryn obsługujących HTTPS, to łączność podlega ochronie i żadne identyfikatory śledzące nie mogą być dodawane.

Wskutek ostrego protestu konsumentów obydwa przedsiębiorstwa w końcu umożliwiły swoim użytkownikom zgłoszenie rezygnacji ze śledzenia. Amerykańska Federalna Komisja Łączności (ang. *Federal Communications Commission* — FCC) nawet obciążyła Verizon grzywną w wysokości 1,3 mln dolarów (dla takiej firmy to tyle co nic). Wszystko to jednak dowodzi, że nawet kosztowna usługa nie gwarantuje, iż świadczący ją podmiot nie będzie chciał zarobić na naszych danych jeszcze więcej.

A oto jeszcze jedna nieprzyjemna historia. Michael Price w portalu Salon[22] opisuje swój nowy, wspaniały, „inteligentny" telewizor, który zakupił w miejsce starego, zawodnego i „tępego". Nowy odbiornik oferował wszystkie wspaniałe funkcje: przeglądarkę internetową, pocztę elektroniczną, media społecznościowe, strumieniowe serwisy telewizyjne, aplikacje, gry. Autor popełnił jednak błąd i przeczytał warunki podane drobnym drukiem.

> „[…] teraz boję się z niego korzystać. Wy też zaczęlibyście się bać, gdybyście przebrnęli przez 46-stronicowy opis polityki prywatności. To urządzenie zbiera zdumiewającą ilość danych. Rejestruje, gdzie, kiedy, w jaki sposób i jak długo korzystacie z telewizora. Ustawia znaczniki pozwalające stwierdzić, »kiedy odebrano dane treści lub określoną wiadomość elektroniczną«. Zapamiętuje »używane aplikacje, odwiedzane witryny internetowe i sposoby korzystania z treści«. Ignoruje żądania »nie śledź« w ramach celowej polityki".

Jest jeszcze gorzej: w ten odbiornik wbudowano mikrofon i kamerę, które pozwalają na rozpoznawanie głosu i twarzy. W polityce prywatności zapisano: „Prosimy pamiętać, że jeżeli w wypowiadanych przez użytkownika słowach zawarte są osobiste lub inne delikatne informacje, informacje te znajdą się wśród utrwalanych danych i zostaną przekazane innemu podmiotowi".

Oczywiście żyjemy w epoce wirtualnych asystentów, takich jak Siri Apple'a i Alexa Amazona. Świadomie kupujemy produkty, które przez cały czas nasłuchują naszego głosu, tak że za ich pośrednictwem możemy poznać najświeższe doniesienia lub prognozę pogody, zamówić towary, a nawet włączać i wyłączać różne urządzenia.

W takim świecie obecnie żyjemy — pełnym inteligentnych aparatów, które śledzą każdy nasz ruch wirtualny i fizyczny i przekazują te informacje jakimś nieokreślonym „innym podmiotom". W miarę jak rozwija się internet rzeczy i coraz więcej tępych urządzeń nabiera znamion inteligencji, niebezpieczeństwo śledzenia nas i naruszania naszej prywatności wzrasta skokowo.

Prawdziwy problem związany z zarabianiem na naszych danych tkwi w tym, że większość ludzi po prostu nie zdaje sobie sprawy z tego, co naprawdę się dzieje, i nie ma prawie żadnej kontroli nad gromadzonymi informacjami. Potrzebujemy więcej przejrzystości oraz możliwości „zgłaszania rezygnacji"[23] ze zbierania danych, nawet jeśli taki wybór będzie kosztował. Ludzie powinni mieć wybór i powinien on być świadomy. Trzeba, żebyśmy jako konsumenci i obywatele mobilizowali swoich przedstawicieli politycznych do działania w naszym interesie. Przedsiębiorstwa muszą zapewniać bezpłatny i łatwy dostęp do naszych profili informacyjnych (podobnie jak kredytodawcy muszą dostarczać bezpłatne kopie raportów kredytowych) oraz umożliwiać ich zmianę bądź likwidację, gdy tego zażądamy. Poszedłbym nawet dalej: trzeba się „zapisywać" na wszelkie zbieranie danych, lecz w istocie uzyskanie takiej zgody odbywa się zbyt łatwo. Ile razy naprawdę przeczytałeś umowę licencyjną użytkownika końcowego

[22] Patrz: *https://www.salon.com/2014/10/30/im_terrified_of_my_new_tv_why_im_scared_to_turn_this_thing_on_and_youd_be_too*.

[23] Zgłoszenie rezygnacji (ang. *opt out*) oznacza, że przedsiębiorstwo wpisuje użytkowników na jakąś listę, ale pozwala im się wycofać pod pewnymi warunkami. Przykładowo automatycznie wprowadza użytkownika do programu zbierania danych, lecz pozwala mu „zgłosić rezygnację", jeżeli zmieni on pewne ustawienia swojego konta albo wyśle podpisany formularz. Mechanizm „zgłaszania uczestnictwa" (ang. *opt in*) działa odwrotnie: trzeba wyraźnie poprosić o to, żeby zostać wpisanym na listę.

(ang. *end-user license agreement* — EULA), towarzyszącą każdemu instalowanemu programowi i każdej usłudze internetowej[24]? Zawiera ona sformułowania, które w zasadzie pozwalają dostawcy robić, co mu się żywnie podoba. Jedynym sposobem na zmianę tego stanu rzeczy jest wybieranie przedstawicieli, którzy uregulują prawnie tego rodzaju działalność.

Unia Europejska poczyniła duże kroki we właściwym kierunku, wprowadzając rozporządzenie o ochronie danych osobowych (RODO), które odnosi się do większości albo nawet wszystkich poruszonych przeze mnie problemów. Tymczasem w USA faktycznie *znosi się regulacje* dotyczące gromadzenia danych na skalę przemysłową. Pozostaje kwestią przyszłości, czy skandale wywołane przez Equifax, Facebooka i Cambridge Analytica w końcu odwrócą tę tendencję i przyczynią się do wprowadzenia zdroworozsądkowych przepisów.

Komu można zaufać?

Komu zatem *można* zaufać w dzisiejszych czasach? To jest istotne, fundamentalne pytanie i jako społeczeństwo powinniśmy je zadawać o wiele częściej niż dotychczas. Niestety, nie ma na nie łatwej odpowiedzi. Jeżeli się nad nim dokładniej zastanowić, szybko zyskuje ono głęboki wymiar filozoficzny. Moim jednak zadaniem jest upraszczanie problemów, zatem spojrzyjmy na to z praktycznego punktu widzenia.

Przede wszystkim trzeba ustalić, co rozumiemy przez *zaufanie*. Pogwałcenie tej zasady nie sprowadza się do celowej próby spowodowania szkody. Podmioty świadczące usługi i prowadzące działalność marketingową przez internet na pewno nie chcą zaszkodzić swoim klientom przez masowe gromadzenie i sprzedawanie „anonimowych" danych osobowych. W istocie mogłyby dowodzić (i w rzeczy samej tak robią), że pomagają użytkownikom, ponieważ starają się dopasować prezentowane reklamy do ich indywidualnych zainteresowań. Dzięki temu wzrasta prawdopodobieństwo, że odbiorca rzeczywiście będzie chciał się dowiadywać o towarach i usługach będących w ofercie. Ponieważ dopasowane reklamy są wyżej cenione przez handlowców, można zarobić więcej pieniędzy na pojedynczej reklamie, dzięki czemu (teoretycznie) mniejsza ilość reklam wystarczy do uzyskania takiego samego przychodu. Według owych firm taka sytuacja przynosi korzyść wszystkim uczestnikom. Oczywiście można poświęcić część swojej prywatności w zamian za darmowe treści i usługi internetowe. Niemniej trzeba zdawać sobie sprawę, w jaki sposób się za nie płaci, a także wiedzieć, że nasze dane prawdopodobnie są odsprzedawane innym podmiotom, które mogą kierować się całkiem odmiennymi intencjami.

Koniec końców trzeba samemu ocenić motywację osoby, firmy bądź instytucji oferującej daną poradę lub usługę. W wielu przypadkach należy się po prostu zastanowić, w jaki sposób zarabiają pieniądze. Czy płacimy uczciwą cenę za to, co otrzymujemy? Jeżeli nie płacimy nic albo cena jest nazbyt atrakcyjna, to powinniśmy się dobrze zastanowić nad obdarzeniem oferenta zaufaniem. Wiele „bezpłatnych" serwisów internetowych zarabia na zamieszczaniu reklam i na prowizji, którą dostają za każde kliknięcie przez użytkowników odsyłaczy do innych witryn. Uzyskują też dochód z odsprzedawania uzyskanych informacji zainteresowanym podmiotom, na co prawdopodobnie użytkownik wyraża zgodę w trakcie abonowania usługi i co zostało opisane zawiłym językiem gdzieś w środku umowy licencyjnej. Niestety, jak już powiedzieliśmy, wiadomo również o tym, że uczciwa cena za usługę nie zawsze pozwala zaufać usługodawcy, ale przynajmniej zwiększa nasze szanse.

Oprócz przeprowadzenia „analizy pieniężnej" należy się zastanowić nad innymi motywami i zadać głębsze pytania. Czy w najlepszym interesie własnym danego usługodawcy leży otwartość, uczciwość i przejrzystość wobec odbiorców? A może zyska on więcej, jeżeli będzie mącił w głowach, zwodził i zastraszał? Zastanówmy się nad tym przez chwilę. Przed nadejściem internetu i powstaniem CNN większość ludzi czerpała wiedzę o świecie z prasy i wieczornych dzienników telewizyjnych. W „dawnych czasach" (30 – 40 lat temu) twórcy serwisów informacyjnych nie mieli przysparzać dochodów, tylko świadczyć usługi publiczne (co nie wynikało z dobroci ich serca, lecz z przepisów prawa, w myśl których przydzielano licencje nadawcze pod różnymi warunkami związanymi z „interesem ogółu"). Jednakże w następnych latach, kiedy wskaźniki

[24] Na temat tych umów i zbierania danych o nas wszystkich nakręcono znakomity film dokumentalny pt. *Terms and Conditions May Apply*.

oglądalności i wpływy z reklam stały się głównym motorem telewizji, programy informacyjne nabrały charakteru rozrywkowego[25]. Głównym celem przestała być edukacja lub informacja, a stało się nim przyciągnięcie (i utrzymanie) odbiorców. Suche fakty nie przykują niczyjej uwagi. „Czy wieczorny dziennik naprawdę was zabije? Szokująca odpowiedź! Oglądajcie dzisiaj o dwudziestej trzeciej!". Im więcej sensacji, tym lepiej.

Podsumowanie

- Bezpieczeństwo cybernetyczne jest analogiczne do fizycznego. Aby naprawdę się zabezpieczyć, trzeba poznać możliwości i motywy przeciwnika, jak również własne słabe punkty. Należy też mieć kilka linii obrony, a nie tylko jedną.
- Bezpieczeństwo nigdy nie jest absolutne i zawsze wybiera się rozwiązania kompromisowe. Całkowite zabezpieczenie się poskutkowałoby bankructwem, więc trzeba zadbać o rozsądną równowagę.
- Zapoznałeś się z najważniejszymi pojęciami z dziedziny informatyki i bezpieczeństwa cybernetycznego. Jeżeli czegoś zapomnisz, sięgnij do słowniczka na końcu książki.
- Szyfrowanie to wspaniała metoda zabezpieczania danych, zarówno na dysku twardym, jak i w ich podróży przez internet.
- Największe zagrożenia dotyczą dzisiaj naszej prywatności. Korporacje i maklerzy danych gromadzą mnóstwo informacji o użytkownikach bez ścisłej kontroli. Informacje te wręcz proszą się o nadużycie, wykradzenie przez włamywaczy lub zawłaszczenie przez zachłanne agencje.

[25] W oryginale *infotainment*, co oznacza połączenie informacji (ang. *information*) z rozrywką (ang. *entertainment*) — *przyp. tłum.*

Lista kontrolna

Pora na praktykę!

Wskazówka 2.1. Poznaj samego siebie

Powinniśmy jeszcze zanotować kilka ważnych informacji, które zawsze powinieneś mieć pod ręką. Będą Ci potrzebne do wyboru ścieżki postępowania na listach kontrolnych. Zapisz sobie poniższe dane:

- Jakiego rodzaju komputer posiadasz — biurkowy czy przenośny? Komputer biurkowy (stacjonarny) jest stale podłączony do gniazda sieci elektrycznej, przenośny natomiast ma wbudowany akumulator, czyli własne źródło zasilania w energię elektryczną.
- Jaki system operacyjny (ang. *operating system* — OS) działa na Twoim komputerze? Ta książka dotyczy nowoczesnych wersji dwóch najpopularniejszych systemów: Microsoft Windows i Apple macOS (dawniej zwany OS X). Aby szybko sprawdzić typ i wersję swojego systemu, można po prostu skorzystać z poniższej strony internetowej (w języku angielskim):

  http://whatsmyos.com/

- U góry strony pojawi się możliwie najtrafniejsze rozpoznanie typu i wersji Twojego systemu operacyjnego. Na stronie widnieją również objaśnienia, jak można uzyskać te ważne informacje „ręcznie". Przykładowe wersje Windows to 7, 8, 8.1 i 10. Wersje Mac OS noszą oznaczenia liczbowe i nazwę własną, np. Sierra (10.12) i High Sierra (10.13). W starszych komputerach macintosh można spotkać Mac OS X 10.11 (El Capitan) albo 10.10 (Yosemite). Jeżeli nie posiadasz żadnej z nich, to znaczy, że Twój system jest przestarzały i możesz mieć kłopoty z wdrożeniem niektórych zaleceń podanych w tej książce; inne jednak pozostaną użyteczne.

Wskazówka 2.2. Dowiedz się, co oni wiedzą

Starałem się pokazać, ile danych jest gromadzonych na nasz temat, wątpię jednak, czy naprawdę uświadamiamy sobie skalę tego zjawiska. Czy wiesz o tym, że wiele popularnych serwisów pozwala użytkownikowi pobrać wszystkie zebrane o nim informacje? Tyle że niejednokrotnie są to jedynie surowe dane, a nie wszystko to, co udało się z nich *otrzymać*. W takim zestawieniu brakuje też informacji, które mogą pochodzić z innych źródeł. Niemniej zapoznanie się z tymi danymi pozwala przejrzeć na oczy, więc gorąco zachęcam, żeby pobrać ich maksymalną ilość i dokładnie je przeanalizować.

Niemal zawsze przygotowany do pobrania zostanie duży plik typu *.zip*, czyli skompresowane archiwum pewnej liczby plików i katalogów. Po ściągnięciu takiego pliku można dwukrotnie go kliknąć, a wówczas powinien rozwinąć swoją zawartość.

Google

1. W przeglądarce internetowej otwórz stronę *https://takeout.google.com/settings/takeout*.
2. Po zalogowaniu się na swoim koncie ujrzysz dziesiątki usług Google'a. Pozostawiłbym zaznaczone wszystkie pozycje, może z wyjątkiem *Poczty* (*Gmail*); masz już wszystkie swoje wiadomości, więc nie potrzebujesz pobierać ich raz jeszcze.
3. Przewiń na sam dół i kliknij *Dalej*.
4. Tutaj ustawienia standardowe powinny być odpowiednie, więc tylko kliknij *Utwórz archiwum*.

Facebook

1. Po zalogowaniu się w witrynie Facebooka wybierz *Ustawienia*.
2. Kliknij *Twoje informacje na Facebooku* u dołu w dziale *Ogólne*.
3. Wybierz *Pobieranie Twoich informacji*, a na kolejnej stronie — *Utwórz plik*.

Twitter

1. W witrynie Twittera wybierz *Ustawienia i prywatność*.
2. Kliknij *Informacje o Tobie* na Twitterze, a następnie przycisk *Uzyskaj swoje dane*.

LinkedIn

1. Kliknij ikonę *Ja* u góry na stronie głównej LinkedIn.
2. Wybierz pozycję *Ustawienia i prywatność*.
3. Kliknij *Prywatność* u góry strony.
4. W części *W jaki sposób LinkedIn wykorzystuje Twoje dane* kliknij *Zmień* obok *Pobierz swoje dane*.
5. Nastąpi przekierowanie na stronę, na której można wybrać dane do pobrania.

Apple

1. Zaloguj się na stronie Apple'a *Dane i prywatność* pod adresem *https://privacy.apple.com/?r=1&language=PL-PL*.
2. Pod *Pobierz kopię swoich danych* kliknij *Zaczynamy*.
3. Wybierz dane, które chcesz pobrać. Możesz pominąć te pozycje, które już masz, np. pocztę.
4. Wybierz wielkość porcji danych, czyli maksymalny rozmiar każdego pobieranego pliku.
5. Gdy pliki zostaną przygotowane, otrzymasz powiadomienie pocztą elektroniczną.

Skorowidz

F

G

H

I

J

K

L

Ł

M

N

O

Z

Nie musisz być informatykiem, by pamiętać o bezpieczeństwie!

Internet jest obecny w większości obszarów naszego życia. To już nie tylko korzystanie ze stron internetowych, ale także bankowość, zakupy w sieci czy podtrzymywanie relacji z rodziną i ze znajomymi. Oznacza to, że niemal cały czas Twoje bezpieczeństwo, pieniądze i prywatność są narażone na ataki. Aby skutecznie chronić siebie i swoich bliskich, musisz zdobyć pewne minimum wiedzy. Nie sposób obronić się przed naprawdę zdeterminowanym hakerem, ale ochrona przed pospolitymi włamaniami czy masową inwigilacją jest jak najbardziej możliwa, i to z wykorzystaniem prostych narzędzi. Trzeba tylko wiedzieć, jak się do tego zabrać!

To przystępny i kompleksowy przewodnik po zagadnieniach bezpieczeństwa, skierowany do osób, które nie znają się na komputerach i informatyce. Kwestie cyberbezpieczeństwa przedstawiono tu krok po kroku, z minimalnym użyciem specjalistycznego języka. Opisano dziesiątki całkiem prostych sposobów pozwalających każdemu zabezpieczyć swoje urządzenia i dane. Książka została napisana tak, aby maksymalnie uprościć zarządzanie Twoim bezpieczeństwem w sieci. W każdym rozdziale znalazła się kompletna lista kontrolna ze szczegółowymi instrukcjami i rysunkami.

Najważniejsze zagadnienia:

- zarządzanie hasłami dostępu
- blokowanie inwigilacji i śledzenia w internecie
- bezpieczne korzystanie z bankowości, ze sklepów i z serwisów społecznościowych
- bezpieczeństwo smartfona, tabletu i domowej sieci
- ochrona dzieci korzystających z internetu

Carey Parker — jest pasjonatem komputerów, elektrotechniki i programowania. Ma ponad dwudziestoletnie doświadczenie jako programista. Zainspirowany przez Edwarda Snowdena, głębiej zainteresował się sprawami prywatności, masowej inwigilacji i cyberbezpieczeństwa. Jest głęboko przekonany, że każdy, kto korzysta z nowych technologii, może zadbać o swoje cyberbezpieczeństwo. Dzielenie się wiedzą z ludźmi, którzy nie są inżynierami, stało się jego misją.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

ISBN 978-83-283-5569-9
9 788328 355699

Cena: 49,00 zł
Apress