Krzysztof SZCZYPIORSKI, Ryszard KOSSOWSKI**

In God we trust, all others we monitor
motto NSA (*National Security Agency*) –
Narodowej Agencji Bezpieczeństwa USA

Trendy w ochronie informacji

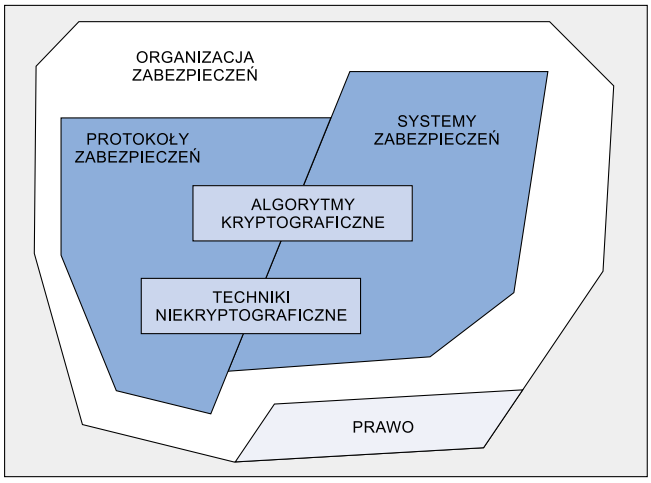
Celem artykułu jest przybliżenie – z perspektywy telekomunikacyjnej – zagadnień związanych z ochroną informacji. Ochrona taka nie jest potrzebna, jeśli nie ma zagrożenia. Trudno jednak wyobrazić sobie to, aby w obecnym świecie, wymieniającym informacje w kanałach publicznych, zagrożenie to nie występowało. W pierwszej części artykułu przedstawiono, składający się z sześciu komponentów (obszarów), model współczesnej ochrony informacji, a następnie omówiono wybrane trendy związane z poszczególnymi jego obszarami.

* **Instytut Telekomunikacji Politechniki Warszawskiej,**
e-mail: K.Szczypiorski@tele.pw.edu.pl
R. Kossowski@tele.pw.edu.pl

MODEL WSPÓŁCZESNEJ OCHRONY INFORMACJI

Ochronę informacji można opisać przez zdefiniowanie modelu określającego tę dyscyplinę nauki i techniki (rys. 1). Przedstawiony w artykule model składa się z **sześciu komponentów (obszarów)**. Są to:

- **algorytmy kryptograficzne**, czyli oparte na kryptografii szyfry, funkcje skrótu, algorytmy podpisu cyfrowego;
- **techniki niekryptograficzne**, czyli metody nie wywodzące się wprost z kryptografii – niekiedy bez wsparcia ze strony kryptografii nie stanowią w istocie żadnego zabezpieczenia; przykła-



Rys. 1. Model współczesnej ochrony informacji

dami technik niekryptograficznych są: parametry zależne od czasu (*Time Variant Parametrs*), techniki biometryczne (analiza kształtu dłoni, tęczówki, barwy głosu);

- **protokoły zabezpieczeń**, które **realizują** wybrane **usługi bezpieczeństwa** – protokoły mogą korzystać z algorytmów kryptograficznych lub technik niekryptograficznych; przykładami są protokoły uwierzytelnienia lub protokoły dzielenia sekretów;
- **systemy zabezpieczeń,** czyli rozbudowane aplikacje lub realizacje sprzętowe wybranych usług ochrony informacji – w szczególnym przypadku wykorzystują one wybrane protokoły zabezpieczeń, np. systemy realizujące wirtualne sieci prywatne (protokoły uwierzytelnienia, poufności i integralności); niekiedy systemy zabezpieczeń wykorzystują wyłącznie techniki niekryptograficzne zapewniania ochrony informacji, np. ściany przeciwogniowe (*firewall*) i mechanizm filtrowania pakietów na podstawie list kontroli dostępu;
- **organizacja zabezpieczeń**, czyli zarządzanie zabezpieczeniami w systemach informacyjnych, poczynając od oceny ryzyka, projektu zabezpieczeń, przez jego wdrażanie i eksploatację;
- **prawo**, czyli kwestie legislacyjne, które oddziaływują na postać (w tym jakość) zabezpieczeń.

Algorytmy kryptograficzne

Rozwój algorytmów kryptograficznych na świecie charakteryzuje się dwoma pozornie sprzecznymi nurtami. Pierwszy nurt to olbrzymi i kaskadowy rozwój kryptoanalizy z wykorzystaniem technik obliczeń rozproszonych, drugi – to tendencja zapobiegająca negatywnym skutkom kryptoanalizy – ujawnione zapotrzebowanie i realizacja technik kryptograficznych godnych przeciwnika.

Biorąc pod uwagę konstrukcję szyfrów, warto wspomnieć o bardzo istotnej zmianie w architekturze najnowszego systemu kryptograficznego – Rijndael [1], następcy algorytmu **DES** (*Data Encryption Standard*) [2]. Dotychczas w technikach kryptografii symetrycznej z zasady wykorzystywano tzw. schematy Feistela. Do konkursu na następcę algorytmu DES – czyli **AES** (*Advanced Encryption Standard*) – zgłoszono wiele nowych algorytmów, których działanie jest oparte na schematach Feistela. Wygrał jednak kandydat o algorytmie całkowicie odmiennym, opartym na tych samych zasadach, jakie są wykorzystywane w kryptosystemach klucza publicznego. Warto zaznaczyć, że systemy klucza publicznego wykorzystują bardzo zaawansowane narzędzia matematyczne, np. systemy oparte na krzywych eliptycznych, które są naukowymi skromnymi sąsiadami dowodu Wielkiego Twierdzenia Fermata. Algorytm Rijndael jest szyfrem symetrycznym, w którym używa się kluczy o długości 128, 192 lub 256 bitów. Wspomniane długości klucza powinny gwarantować bezpieczeństwo przez okres co najmniej najbliższych paru dekad. Dla porównania: algorytm DES używa klucza o efektywnej długości 56 bitów, a algorytm 3DES – 112 bitów. Wraz z pojawieniem się nowego algorytmu symetrycznego, amerykański instytut NIST (*National Institute of Standards and Technology*) uaktualnił algorytm funkcji skrótu **SHA** (*Secure Hash Algorithm*), proponując nowe algorytmy o symbolach **SHA-256**, **SHA-384**, **SHA-512** [3]. Wymienione w symbolach liczby są długościami skrótów generowanych przez te algorytmy. Długości skrótów są dobrane do długości bloków szyfrowania algorytmu Rijndael z uwzględnieniem ataku typu dzień urodzin[1)], stąd długość skrótów jest dwa razy większa. W dziedzinie podpisów cyfrowych nie pojawiły się ostatnio nowe propozycje, wydaje się, że algorytm **DSA** (*Digital Signature Algorithm*) o długości 160 bitów wciąż jest bezpieczny.

Techniki niekryptograficzne

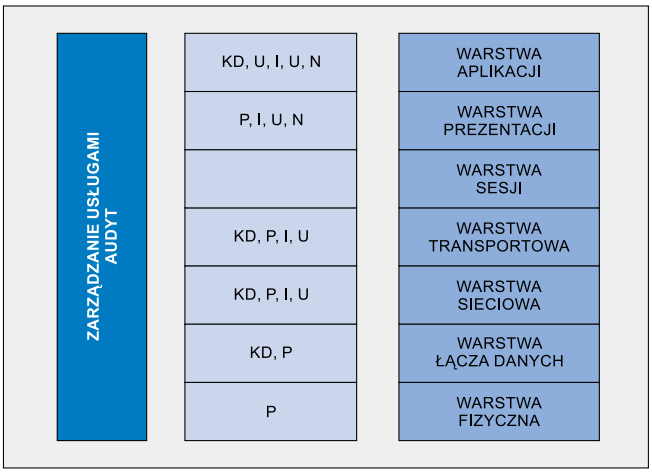
Wśród technik niekryptograficznych warto wspomnieć o trendach związanych z wykorzystaniem technik biometrycznych [4]. Techniki biometryczne służą uwierzytelnieniu ludzi, a źródłem informacji uwierzytelniających mogą być m.in. linie papilarne, kształt dłoni, wzór siatkówki lub tęczówki, kształt twarzy, cechy pisma ręcznego (w tym podpisu), cechy głosu. Zintensyfikowana praca nad wyłonieniem formuł matematycznych opisujących poszczególne cechy biometryczne daje w rezultacie coraz skuteczniejsze systemy uwierzytelnienia, których dokładność (poziom błędu) jest obecnie na poziomie ułamków procenta. Biometryczne źródło uwierzytelnienia ma od kilkudziesięciu do kilkuset cech, które są poddawane analizie. Przykładowo system uwierzytelniający na podstawie kształtu dłoni opiera się na ok. 100 cechach charakterystycznych, takich jak szerokość i grubość dłoni czy długość i grubość palców.

Coraz częściej spotyka się rozwiązania hybrydowe, w których poza wykorzystywaniem kilku źródeł uwierzytelnienia (np. kształtu dłoni i wzoru tęczówki), jest np. także brane pod uwagę miejsce pobytu uwierzytelniającego się człowieka, na podstawie jego osobistego odbiornika systemu lokalizacji **GPS** (*Global Positioning System*). Przewiduje się, że masowe wykorzystanie technik biometrycznych umożliwi lepszą interakcję użytkowników z systemami teleinformacyjnymi, a także usunie bariery związane z zapamiętaniem przez nich wielu kodów PIN i haseł, posiadaniem kluczy do domu czy do samochodu.

Protokoły zabezpieczeń

Mimo że lokalizacja usług ochrony informacji jest możliwa we wszystkich warstwach sieci (rys. 2), w sieciach przewodowych nie ma wyraźnego trendu w zakresie implementowania usług ochrony informacji wraz z protokołami komunikacyjnymi. W sieciach bezprzewodowych – w dwóch najniższych ich warstwach – jest implementowana poufność danych przez mechanizm szyfrowania. Stosowane są przeważnie szyfry symetryczne pseudostrumieniowe (np. **RC4**) o niezbyt długim kluczu, np. 64 bity, często celowo osłabianym np. do 40 bitów. Zapewniana na tym poziomie ochrona, w połączeniu z niektórymi metodami transmisji (np. techniki z widmem rozproszonym, takie jak **FHSS –** *Frequency-Hopping Spread Spectrum*, **DSSS –** *Direct Sequence Spread Spectrum*), zabezpiecza raczej przed przypadkowym

[1)] tzw. birthday/square root attack – aby znaleźć dwie dowolne wiadomości, dające ten sam skrót, średnio wystarczy przeszukać przestrzeń o wielkości $2^{d/2}$, gdzie d to długość skrótu



Rys. 2. Potencjalna możliwość realizacji usług ochrony informacji w warstwach sieci. Oznaczenia: Kd – kontrola dostępu, P – poufność, I – integralność danych, U – uwierzytelnienie, N – niezaprzeczalność

podsłuchem, nie chroni zaś przed zaawansowanym atakiem na tego typu systemy. Niektóre z najpopularniejszych protokołów bezpieczeństwa używanych w sieciach bezprzewodowych, np. **WEP** (*Wired Equivalent Privacy*) wprowadzony wraz ze standardem IEEE 802.11, były obarczone błędami w konstrukcji, w szczególności niedbałym doborem wartości inicjujących szyfry, użyciem cyklicznego kodu nadmiarowego typu **CRC-32** do zapewnienia usługi integralności [5]. Oprócz poufności w sieciach bezprzewodowych jest także realizowane uwierzytelnienie poszczególnych stacji (np. terminali i punktów dostępowych), głównie za pomocą technik symetrycznych ze wspólnym tajnym kluczem, połączonych z mechanizmem wyzwanie-odpowiedź. Natomiast w systemach telefonii komórkowej 2. generacji (**GSM**) oprócz poufności w kanale radiowym jest realizowane uwierzytelnienie abonenta w sieci i poufność jego lokalizacji ([6]). System 3. generacji **UMTS** odziedziczył architekturę zabezpieczeń po GSM, jednak wzmocniono część mechanizmów oraz rozszerzono obszar ich działania [7].

Najpopularniejsze protokoły sieci danych, takie jak **ATM**, Frame Relay, **MPLS**, nie zapewniają żadnych usług ochrony informacji. W szczególności protokół MPLS jest często mylnie traktowany jako bezpieczna sieć, chociaż poziom bezpieczeństwa MPLS nie wyróżnia się na tle innych sieci danych (por. [19]). Jest to świadoma polityka twórców protokołów sieci danych, zgodnie z którą oferowanie kryptograficznego bezpieczeństwa nie jest zadaniem sieci – odpowiedzialni są za to jej użytkownicy.

W wyższych warstwach sieci usługi ochrony informacji są opcjonalne i w praktyce przeznaczone do rozwiązań dla sieci **TCP/IP**, które dominują przy organizacji sieci zarówno rozległych, jak i lokalnych (intranety). W latach 70. XX wieku, projektanci stosu protokołów TCP/IP nie zakładali, że ktoś chce ukraść informacje, gdyż tworzyli sieć, która umożliwia dzielenie się wiedzą. Podobnie twórcy systemów operacyjnych, takich jak Unix, nie mieli motywacji do wdrażania zabezpieczeń. Zakładano bowiem, że każdy użytkownik pragnie, by system działał. To podejście, słuszne 30 lat temu, w dobie obecnej powszechności sieci TCP/IP jest często określane „rujnującym dziedzictwem".

Trendy związane z zabezpieczeniem stosu TCP/IP (por. [8]) podążają dwiema wyraźnymi drogami: **pierwsza droga** w warstwie sieciowej polega na zastąpieniu protokołu **IPv4** przez protokół **IPv6** lub uzupełnieniu IPv4 przez protokół **IPsec** [9]. Ujednolicone dla IPsec i IPv6 mechanizmy bezpieczeństwa to:

- *Authentication Header* (**AH**) [10] – nagłówek uwierzytelniający, zapewniający integralność i uwierzytelnienie,
- *IP Encapsulating Security Payload* (**ESP**) [11] – bezpieczna koperta, zapewniająca poufność i zależnie – od użytego algorytmu oraz trybu – także integralność i uwierzytelnienie.

Uwierzytelniona dystrybucja klucza kryptograficznego jest realizowana za pomocą protokołu **IKE –** *Internet Key Exchange* [12].

Druga droga polega na dodaniu do warstwy transportowej protokołu realizującego poufność, integralność i uwierzytelnienie, zwanego TLS (*Transport Layer Security* – [13]), którego wcześniejsze wersje były znane pod nazwą **SSL** (*Secure Sockets Layer*). Bezpieczeństwo realizowane za pomocą protokołu TLS ogranicza się do aplikacji wykorzystujących protokół **TCP** (m.in. **HTTP**, **FTP**, **SMTP**, **POP3**). Jednak z wyjątkiem zmiany wywołań do warstwy transportowej protokół TLS nie zmienia architektury aplikacji. Został on zaadaptowany jako warstwa zabezpieczeń dla środowiska **WAP** (**WTLS –** *Wireless Transport Layer Security*).

Na poziomie aplikacji kwestie związane z bezpieczeństwem, nawet jeżeli nie są dobrze realizowane, są najlepiej rozumiane przez twórców systemów. W szczególności dużą rolę odgrywa zrealizowanie naturalnej dla człowieka usługi **prywatności.** Prywatność jest najczęściej realizowana przez poufność i uwierzytelnienie (systemy bezpiecznej poczty elektronicznej **PEM –** *Privacy Enhancement for Internet Electronic Mail* i **PGP –** *Pretty Good Privacy*). Niekiedy prywatność jest osiągana przez zapewnienie **anonimowości**. W tym celu przeważnie wdraża się systemy anonimowego surfowania po Internecie i systemy anonimowego przesyłania wiadomości. W przypadku **WWW** systemy anonimowego surfowania usuwają informacje ułatwiające ustalenie tożsamości nadawcy, takie jak: adres źródłowy IP, nazwa **DNS** maszyny źródłowej, rodzaj przeglądarki i nazwa systemu operacyjnego. Dodatkowo mogą filtrować tzw. *cookies* [14] – parametry (zmienne i wartości) wymieniane przez przeglądarkę i serwer WWW, z jednej strony niwelujące w protokole HTTP bezstanowość, z drugiej umożliwiające śledzenie poczynań i preferencji użytkowników.

Pod koniec lat 90. XX wieku katalizatorem zmian w obrębie Internetu i bezpieczeństwa stały się protokoły handlu elektronicznego (*e-commerce*). Mimo że niewielka ich liczba została wdrożona (kilka z ok. 70 uznanych propozycji – por. [15]), nastąpił wzrost zainteresowania klasycznymi algorytmami kryptograficznymi, w tym przede wszystkim podpisem cyfrowym. Celem budowy elektronicznych protokołów płatności jest wdrożenie rozwiązań odpowiadających rzeczywistym środkom płatności, takim jak czeki, karty płatnicze, gotówka. Przy niektórych kwotach okazuje się, że zabezpieczenie transakcji przekracza jej wartość, stąd też proponuje się metody tańsze (np. bez każdorazowej autoryzacji, bez zaawansowanej kryptografii), ale obarczone większym ryzykiem fałszerstwa. Przykładem tego typu protokołów są mikropłatności.

Spore obietnice wiąże się z płatnościami w środowisku abonentów telefonii ruchomej (*m-commerce*). Powiązanie wirtualnego elektronicznego portfela czy portmonetki z kartą **SIM** lub zapamiętanie klucza prywatnego abonenta (moduł **WIM** – *Wireless Identity Module* w protokole WAP) gwarantuje bezpieczeństwo płatności. Znane są przynajmniej dwie strony transakcji – abonent oraz organizacja finansowa współpracująca z operatorem.

Dotychczas większość światowych systemów handlu elektronicznego w segmencie **B2C** (*business to client*) opiera się na kartach płatniczych. Karty płatnicze są obarczone dużym ryzykiem nadużyć – znajomość numeru aktywnej karty i daty jej ważności jest równoznaczna z możliwością finalizacji zakupów w Internecie. Proste zabiegi utrudniające proceder posługiwania się cudzym numerem karty, takie jak wykorzystywanie jednorazowych numerów kart płatniczych, nie są szeroko implementowane. Także zastosowanie szyfrowanej transmisji pomiędzy klientem a internetowym sprzedawcą, np. za pomocą protokołu **TLS/SSL**, nie chroni przed kradzieżą numeru karty i daty jej ważności z serwera, na którym te dane są przechowywane. Alterna-

tywne rozwiązania do transakcji opartych na kartach, takie jak np. **SET** (*Secure Electronic Transactions* – [16]), wykorzystujące kryptografię asymetryczną i ideę podwójnego podpisu, nie znalazły zastosowania ze względu na koszty implementacji i utrzymania takiego systemu.

Patrząc na telekomunikację w sposób klasyczny – jako model komunikacyjny dwóch podmiotów – i mając świadomość, że ochrona informacji zapewnia dla tego modelu dobre metody, warto wspomnieć o trendach związanych z komunikacją grupową (por. [17]). W komunikacji grupowej wciąż brakuje ujednoliconego systemu zarządzania kluczami kryptograficznymi, a wyzwanie stojące przed ochroną informacji nie jest bagatelne: nowi członkowie grupy nie powinni mieć dostępu do informacji wymienianych w grupie przed ich przybyciem, natomiast członkowie, którzy odeszli, nie powinni mieć dostępu do danych aktualnie transmitowanych. Dodatkowo postawione wyzwanie komplikuje fakt, że dystrybucja klucza kryptograficznego nie powinna być kosztowna z punktu widzenia zasobów sieciowych i obliczeniowych. Także niejednorodność grup komunikacyjnych: dynamizm w przyłączaniu i odłączaniu członków, parametry jakościowe usług, wielkość grupy, liczba podmiotów nadających – utrudniają sformułowanie zadowalających propozycji. Większość rozwiązań związanych z dystrybucją klucza kryptograficznego w komunikacji grupowej opiera się na drzewach binarnych – członkowie grupy dzielą zestaw kluczy, wynikający z ich położenia w drzewie.

Systemy zabezpieczeń

Szeroko stosowanym sieciowym systemem ochrony informacji jest ***firewall* (ściana przeciwogniowa)** – por. [8]. W najprostszej postaci ten system jest filtrem, odrzucającym pakiety nadchodzące z określonych lokalizacji, a także odrzucającym niepoprawne jednostki danych. *Firewall* realizuje usługę kontroli dostępu, a także na podstawie generowanych logów umożliwia audyt. System ten, mimo że najczęściej spotykany w sieciach TCP/IP, jest dostępny także dla sieci danych, takich jak np. ATM. Oprócz warstwy sieciowej i transportowej ściany przeciwogniowe mogą działać na poziomie protokołów warstwy aplikacji, służąc jako system pośredniczący. Najczęściej ściany przeciwogniowe są umieszczane na styku sieci lokalnej z siecią rozległą lub w newralgicznych miejscach sieci lokalnej. Zauważalnym trendem jest dedykowanie funkcji ściany przeciwogniowej maszynie użytkownika (tzw. osobiste ściany przeciwogniowe) przez użycie specjalistycznego oprogramowania. Rozwiązanie to cieszy się dużą popularnością wśród klientów *dial-up* (abonentów „dodzwaniających się" do sieci), którzy w większości przypadków otrzymując przy negocjacji połączenia publiczny adres IP nie są skutecznie chronieni przez dostawcę usług internetowych.

Kolejnym ważnym systemem zabezpieczeń jest **system wykrywania włamań** (*intrusion detection system*) – por. [8]. Jest to system wykrywający zachowania niezgodne z przyjętą definicją poprawnego zachowania się lub ewidentne naruszenie bezpieczeństwa systemu. Metody ataków na sieci ulegają ewolucji i podstawowym problemem we wdrażaniu tego systemu jest wiedza o tych atakach. Systemy wykrywania włamań mogą informacje o atakach wymieniać między sobą w postaci wzorców nadużyć, mogą też próbować rozpoznać odmienne zachowania czyli anomalie. Źródłem wiedzy o zdarzeniach dla systemu wykrywania włamań może być każda z warstw sieciowych, w szczególności sieciowa, transportowa i aplikacji, a także system operacyjny maszyn.

Systemy zarządzania nadużyciami (*fraud management system*) przeznaczone dla operatorów telekomunikacyjnych mają wiele wspólnych elementów z systemami wykrywania włamań. Celem wdrażania takich systemów jest ograniczenie nadużyć dokonywanych przez abonentów albo nieuczciwy personel. Nadużycia te mogą objawiać się w postaci niezapłaconych rachunków lub innych metod darmowego korzystania z zasobów operatorskich. Systemy zarządzania nadużyciami często działają na podstawie informacji billingowych, co jest zarówno pewnym ograniczeniem czasowym (opóźnienie w dostępie do informacji billingowej), jak i ograniczeniem wiarygodności tych systemów do rzetelności systemu billingowego. Systemy zarządzania nadużyciami mogą czerpać informacje o aktywności bezpośrednio z systemów sygnalizacyjnych, np. **SS7** (por. [18]). Implementacja takich systemów wymaga zakupu kosztownych monitorów sieciowych, jednak poprawne umiejscowienie ich przy węzłach związanych z usługami, z którymi wiążą się największe nadużycia (połączenia międzynarodowe, usługi *premium-rate*), zapewnia wysoką skuteczność.

Wracając jednak do sieci danych, trzeba stwierdzić, że poważnym zagrożeniem jest **złośliwe oprogramowanie** (*malware*), takie jak wirusy, konie trojańskie, robaki. Jest ono przede wszystkim przekazywane za pomocą poczty elektronicznej, w postaci załączników z programami wykonywalnymi albo plikami zawierającymi skrypty użytkownika – tzw. makra. Czasem jest zakażone pirackie oprogramowanie dystrybuowane w sieci Internet. Często funkcję systemu zwalczającego złośliwe oprogramowanie przejmuje ściana przeciwogniowa. Podobnie jak systemy wykrywania włamań, systemy zwalczające złośliwe oprogramowanie gromadzą sygnatury wirusów, robaków i koni trojańskich. Mogą one także na podobieństwo systemu immunologicznego istoty żywej, reagować na nieznane oprogramowanie, chroniąc przed nowymi, nieudokumentowanymi zakażeniami.

Wykrywanie włamań oraz złośliwego oprogramowania komplikuje przesyłanie danych w formie zaszyfrowanej. Systemy wykrywające włamania, wirusy, konie trojańskie i robaki przeprowadzają analizę semantyczną, która bez odszyfrowania danych jest bezwartościowa. Z tego powodu zauważalnym trendem jest integracja kryptosystemów szyfrujących ze wspomnianymi systemami wykrywania włamań i złośliwego oprogramowania. W tym miejscu warto wspomnieć, że większość współczesnych kryptosystemów, realizujących poufność przez szyfrowanie, implementuje kompresję danych. Procesu kompresji dokonuje się wyłącznie przed zaszyfrowaniem danych, gdyż kompresja zaszyfrowanego strumienia danych jest nieefektywna.

Często kryptograficzna ochrona informacji jest stosowana do rozwiązań dotyczących **wirtualnych sieci prywatnych** (**VPN** – *Virtual Private Network*). W sieciach TCP/IP najczęściej jest do tego używany wspomniany już protokół IPsec. Dopiero uzupełnienie o IPsec znanych rozwiązań VPN-owych, takich jak **PPTP** (*Point-to-Point Tunnelling Protocol* – [20]), **L2TP** (*Layer Two Tunneling Protocol* – [21]) gwarantuje prywatność w rozumieniu ochrony informacji. Także w systemach MPLS-VPN poufność jest najczęściej uzyskiwana przez protokół IPsec.

Organizacja zabezpieczeń

W organizacji zabezpieczeń warto rozważyć dwa aspekty: **zarządzanie bezpieczeństwem** oraz **bezpieczeństwo zarządzania**. **Zarządzanie bezpieczeństwem** to od strony technicznej **zarządzanie usługami i mechanizmami ochrony informacji**. Jest ono realizowane przez dostarczanie informacji zarządzania do usług i mechanizmów, jak i zbieranie oraz przechowywanie informacji o tych usługach i mechanizmach. Od strony organizacyjnej jest to proces projektowania, implementacji, oceny i eksploatacji zabezpieczeń. Dobór właściwych metod technicznych, jak i organizacyjnych, wymaga przeprowadzenia analizy ryzyka jako analizy **zagrożeń**, **podatności (słabych punktów)** i **następstw**. Ponieważ zarządzanie bezpieczeństwem powinno być procesem, a nie jednorazowym aktem, często mówi się o zarządzaniu ryzykiem (por. [22], [23]). Propozycja odpowiednich za-

bezpieczeń dla systemu jest często przedstawiana w dokumencie określanym **polityką bezpieczeństwa**.

Bezpieczeństwo zarządzania, w ujęciu zbliżonym do sieci zarządzania telekomunikacją **TMN** (*Telecommunications Management Network*) jest realizacją polityki bezpieczeństwa w zakresie zarządzania konfiguracją, wydajnością, uszkodzeniami, rozliczeniami, jak i samym jej bezpieczeństwem. Dla operatorów telekomunikacyjnych istotne jest **bezpieczeństwo systemu zarządzania,** które traktuje się jako atrybut systemu, związany z implementacją mechanizmów zapewniających: poufność, integralność, dostępność, rozliczalność i niezawodność. Dany stan bezpieczeństwa systemu zarządzania osiąga się przez zarządzanie bezpieczeństwem.

Popularna w ciągu kilku ostatnich lat, nie tylko dzięki **ustawie o podpisie elektronicznym**, stała się **infrastruktura klucza publicznego** (**PKI** – *Public Key Infrastructure*). Stanowi ona platformę, która umożliwia tworzenie usług wykorzystujących certyfikaty klucza publicznego. Certyfikaty te są zbiorami danych, które zawierają: informacje o właścicielu certyfikatu, materiał klucza publicznego, datę ważności certyfikatu – całość potwierdzoną podpisem urzędu wystawiającego certyfikat, tj. urzędu ds. certyfikacji. Certyfikaty mogą być wystawiane nie tylko ludziom, ale także maszynom, stąd też istnieje możliwość wzajemnego certyfikowania urzędów. W ten sposób powstaje między urzędami łańcuch zaufania, dzięki któremu certyfikat wydany przez jeden urząd może być zweryfikowany przez odtworzenie ścieżki certyfikacji do drugiego urzędu, którego certyfikat jest znany dla sprawdzającego podmiotu.

Podstawowy problem w infrastrukturze klucza publicznego to wiarygodność certyfikatu. Przy wystawianiu certyfikatu wyróżnia się urząd ds. rejestracji, który jest odpowiedzialny za uwierzytelnienie podmiotu ubiegającego się o certyfikat – poprawne określenie tożsamości wnioskującego. Różnica w polityce rejestracji w różnych systemach może doprowadzić do istnienia certyfikatów o różnej „jakości". Infrastruktura klucza publicznego od strony technicznej jest dobrze zdefiniowana – określa ją Zalecenie X. 509 [24], które – wraz ze standardami PKCS#10 [25], PKCS#7 [26] oraz protokołem **LDAP** (*Lightweight Directory Access Protocol* – [27]) – jest rozwiązaniem powszechnie implementowanym. Przeważnie użytkownicy infrastruktury klucza publicznego mają możliwość przeprowadzenia podstawowych procesów, takich jak: generacja pary kluczy (prywatny i publiczny), poufna wymiana klucza (dystrybucja lub uzgodnienie klucza), generacja podpisu cyfrowego, weryfikacja podpisu cyfrowego. Na podstawie infrastruktury klucza publicznego istnieje możliwość tworzenia złożonych usług, takich jak: cyfrowy notariusz, system potwierdzonej dostawy wiadomości, system dystrybucji biletów i wielu innych.

Dotychczas większość rozwiązań wykorzystujących algorytmy klucza publicznego zaprojektowano tak, aby współpracowały z infrastrukturą klucza publicznego. Są to m.in.: **TLS/SSL**, **S/MIME** (*Secure/Multipurpose Internet Mail Extensions*), **SET** (*Secure Electronic Transactions*), **PEM** (*Privacy Enhancement for Internet Electronic Mail*). Pewne nadzieje wiąże się z bezprzewodową infrastrukturą klucza publicznego, tzw. *Wireless PKI* (**W-PKI**), dzięki której będzie możliwość dostępu do usług opartych na certyfikatach z poziomu telefonu komórkowego.

Prawo

Przyspieszona rywalizacja włamujących się do przekazywanych informacji i je chroniących jest ściśle związana z zagrożeniami, a te z przestępstwami. Ponieważ zagrożenia są pod względem jakościowym zupełnie nowe, a pod względem ilościowym bez porównania większe od tych „klasycznych" (światowy rozgłos związany z robakiem *Love Letter,* znanym także pod nazwą: *I love You*), nie należy dziwić się, że istnieje konieczność rozpatrywania tego problemu w aspekcie prawnym. W wielu krajach pojawienie się wirusów komputerowych powodujących duże straty przedsiębiorstw wywołało próby reinterpretacji dotychczasowych paragrafów prawa, tak aby nimi objąć i te przestępstwa. Istotniejszym jednak problemem jest fakt, że nowoczesne przestępstwa teleinformacyjne zaczęły mieć charakter transgraniczny. Jeśli do tego dodać możliwości wykorzystania najnowszych systemów kryptograficznych „nie do złamania" przez świat przestępczy (mafie o zasięgu światowym, kartele przemytnicze i narkotykowe), to problem prawny z jednej strony wydaje się nie do uregulowania, z drugiej wszakże strony uczciwi użytkownicy nowoczesnej telekomunikacji muszą próbować jakoś rozwiązać ten problem. Przynajmniej w tym aspekcie „globalizacja" może napawać otuchą.

Wydaje się, że w dniu dzisiejszym stan bezpieczeństwa wymiany informacji w skali naszego kraju nie jest zbytnio opóźniony w porównaniu np. ze stanem bezpieczeństwa wymiany informacji w USA. Trzy dokumenty zatwierdzone w ostatnich 5 latach, mianowicie: **ustawa o ochronie danych osobowych** [28], **ustawa o ochronie informacji niejawnej** [29] oraz **ustawa o podpisie elektronicznym** [30] mogą budzić nadzieję, że sytuacja nie będzie się pogarszać.

Ustawa o ochronie danych osobowych z punktu widzenia ochrony informacji jest w zasadzie tylko granicą wyznaczającą, co na temat konkretnej osoby można udostępnić publicznie, a jaki zbiór danych podlega już ściśle określonej kontroli dostępu. Granica ta jest oczywiście bardzo kontrowersyjna i może ulegać zmianom. Bezpośrednio ustawa może wpływać na politykę bezpieczeństwa, w szczególności w zakresie dysponowania danymi personalnymi, w danej instytucji, a ta może definiować konieczność użycia konkretnych rozwiązań w zakresie zabezpieczeń dostępu do baz danych personalnych.

Ukazanie się **ustawy o ochronie informacji niejawnych** było bardzo istotnym krokiem w kierunku przystosowania systemów ochrony informacji do warunków demokratycznych. Stara ustawa o tajemnicy była przystosowana do centralnego, apodyktycznego zarządzania bezpieczeństwem. Charakteryzowała się tym, że po prostu wszystko było tajne (nawet zapasy cukru w hurtowni stanowiły tajemnicę strategiczną). Osoba mająca uprawnienia dostępu do spraw tajnych nie mogła wiedzieć, co naprawdę jest tajne. Obecna ustawa wyraźnie wylicza, co ma być chronione oraz wymienia obowiązki osoby, mającej dostęp do chronionych informacji. Inna rzecz, że z punktu widzenia ochrony informacji stara ustawa była lepsza.

Ustawa o podpisie elektronicznym jest w zasadzie ustawą o certyfikacie podpisu elektronicznego. Warto tutaj przyjrzeć się analogii z podpisem klasycznym. Sam ręczny podpis, z punktu widzenia formalnego, nie ma żadnej wartości, jeśli nie można go zweryfikować. Do weryfikacji zaś służy certyfikat tego podpisu, jakim jest w Rzeczypospolitej Polskiej tzw. dowód osobisty. Dowód ten musi być dobrze zabezpieczony przed możliwością podrobienia, musi zawierać ściśle określone dane dotyczące zarówno właściciela, jak i instytucji wydającej dokument, musi zapewniać związanie go z właścicielem w jednoznaczny sposób (zdjęcie, cechy szczególne) oraz dawać możliwość sprawdzenia zgodności podpisu ze wzorcem zawartym w dowodzie. Wydawanie dowodu osobistego jest związane z koniecznością weryfikacji tożsamości – trzeba zgłosić się osobiście i w sposób jednoznaczny wykazać swoją tożsamość. Przy odbiorze dokumentu trzeba koniecznie złożyć swój podpis. Wszystkie te wymagania mają ścisły odpowiednik w certyfikacie podpisu elektronicznego. Różnice zaś wynikają z faktu, że operacje związane z posługiwaniem się dowodem osobistym odbywają się w konkretnym miejscu fizycznym i czasie, zaś posługiwanie się certyfikatem podpisu elektronicznego odbywa się w przestrzeni wirtualnej i bliżej nie określonym czasie.

Na zakończenie warto wspomnieć **ustawę o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym** [31] oraz rozporządzenie w sprawie rodzajów broni i amunicji oraz wykaz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, na których wytwarzanie lub obrót jest wymagana koncesja [32]. W punkcie wspomnianego rozporządzenia „WT XI. Wyroby i technologie związane z ochroną informacji niejawnych" systemy kryptograficzne są zaliczone do wyrobów militarnych, jeśli dla systemów symetrycznych klucz jest dłuższy od 64 bitów, dla systemów asymetrycznych opartych na faktoryzacji ma on ponad 512 bitów, dla opartych na logarytmie dyskretnym – dłuższy niż 512 bitów oraz na logarytmie dyskretnym na krzywych eliptycznych – dłuższy niż 112 bitów. Rozporządzenie nie dotyczy algorytmów realizujących podpis elektroniczny bez usługi poufności. Wydaje się, że te dokumenty w istotny sposób zmieniają naszą rzeczywistość, chociaż trudno dzisiaj powiedzieć, jaką ukształtują przyszłość.

LITERATURA

[1] NIST FIPS PUB 191 – *Advenced Encryption Standard (AES)*. National Institute of Standards and Technology, U. S. Department of Commerce, November 26, 2001
[2] NIST FIPS PUB 186 – *Digital Signature Standard*. National Institute of Standards and Technology, U. S. Department of Commerce, May 18, 1994
[3] NIST FIPS PUB 180-1 – *Secure Hash Standard (SHS)*. National Institute of Standards and Technology, U. S. Department of Commerce, April 17, 1995
[4] Gałach A.: *Systemy biometryczne*. IT Security Magazine, nr 2, 2001
[5] Borisov N., Goldberg I., Wagner D.: *Intercepting Mobile Communications: The Insecurity of 802.11.* Proceedings of the Seventh Annual International Conference on Mobile Computing And Networking, July 16–21, 2001
[6] Shaefer G., Festag A., Karl H.: *Current Approaches to Authentication in Wireless and Mobile Communications Network.* Technical Report (TKN-01-002), Technical University Berlin, March 2001
[7] 3rd Generation Partnership Project – *Security Architecture (Release 4)* – 3GPP TS 33.102 V4.3.0, December 2001
[8] Kijewski P., Szczypiorski K.: *Bezpieczeństwo w sieciach TCP/IP*. Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne, nr 5-6,2001
[9] Kent S., Atkinson R.: *Security Architecture for the Internet Protocol*. RFC 2401, November 1998
[10] Kent S., Atkinson R.: *IP Authentication Header*. RFC 2402, November 1998
[11] Kent S., Atkinson R.: *IP Encapsulating Security Payload*. RFC 2406, November 1998
[12] Harkins D., Carrel D.: *The Internet Key Exchange (IKE).* RFC 2409, November 1998
[13] Dierks T., Allen C.: *The TLS – Protocol Version 1.0.* RFC 2246, January 1999
[14] Kristol D., Montulli L.: *HTTP State Management Mechanism,* RFC 2109, February 1997
[15] Weber R.: *Chablis – Market Analysis of Digital Payment Systems*. Technical Report (TUM-I9819), Muenchen University of Technology, August 1999
[16] SET Secure Electronic Transaction LLC (SETco): *The SET Standard Book 1 Business Description* – http: //www. setco. org/, May 1997
[17] Canetti R., Garay J., Itkis G. i in.: *A taxonomy of multicast security issues and efficient constructions*. Proceedings of the Infocom'99, New York, NY, March 1999
[18] ITU-T Q. 752, *Specifications of Signalling System No. 7 – Signalling System No. 7 management – Monitoring and measurements for Signalling System No. 7 networks*, 1998
[19] MierCom: *Cisco MPLS based VPNs: Equivalent to the security of Frame Relay and ATM.* Whitepaper, March 2001
[20] Hamzeh K., Pall G., Verthein W. i in.: *Point-to-Point Tunnelling Protocol (PPTP)*. RFC 2637, July 1999
[21] Townsley W., Valencia A., Rubens A. i in.: *Layer Two Tunneling Protocol „L2TP".* RFC 2661, August 1999
[22] ISO/IEC 17799: 2000 – *Information technology – Code of practice for information security management – 2000*
[23] PN-I-13335-1: *Technika informatyczna: Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*, Polski Komitet Normalizacyjny, 1999
[24] ITU-T X. 509, *OSI – The Directory – Part 8: Authentication Framework*, Revision 3
[25] Nystrom M., Kaliski B.: *PKCS #10: Certification Request Syntax Specification Version 1.7.* RFC 2986, November 2000
[26] Public-Key Cryptography Standards – *PKCS #7 – Cryptographic Message Syntax Standard,* RSA Security Inc., May 1997
[27] Wahl M., Howes T., Kille S.: *Lightweight Directory Access Protocol (v3)*. RFC 2251, December 1997
[28] *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.* Dz. U. 1997 nr 133 poz. 883 wraz z późniejszymi zmianami
[29] *Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.* Dz. U. 1999 nr 11 poz. 95 wraz z późniejszymi zmianami
[30] *Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym.* Dz. U. 2001 nr 130 poz. 1450
[31] *Ustawa z dnia 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym.* Dz. U. 2001 nr 67 poz. 679
[32] *Rozporządzenie Rady Ministrów z dnia 3 grudnia 2001 r. w sprawie rodzajów broni i amunicji oraz wykazu wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym, na których wytwarzanie lub obrót jest wymagana koncesja.* Dz. U. 2001 nr 145 poz. 1625

Artykuł recenzowany

(Artykuł nadesłano do red. – marzec 2002)