MOŻLIWOŚCI TECHNOLOGICZNE POZYSKIWANIA I MODYFIKACJI INFORMACJI W SIECIACH TELEKOMUNIKACYJNYCH I TELEINFORMATYCZNYCH

Zdzisław Drzycimski

POTRZEBY PRZECIWDZIAŁAŃ
Potrzeby technologiczne

W niniejszym opracowaniu przedstawiono wybrane możliwości techniczne w zakresie: pozyskiwania informacji, modyfikowania informacji i uniemożliwienia przekazywania informacji w sieciach telekomunikacyjnych i teleinformatycznych. Znajomość takich technik może być przydatna, z jednej strony, do ich bezpośredniego wykorzystania, z drugiej, do opracowania metod zabezpieczeń przed takimi działaniami.

WSTĘP

Sieci TK (telekomunikacyjne) i TI (informatyczne) działają z wykorzystaniem ogólnoświatowych standardów. Przyjęcie standardowych rozwiązań jest z wielu względów bardzo korzystne, wręcz konieczne, biorąc pod uwagę możliwości rozwoju sieci i usług. Obecnie stosowane systemy TK i TI są niezawodne, dzięki wysokiemu poziomowi zastosowanych technologii, redundancji łączy i wyposażeń oraz automatycznym rozwiązaniom sterowania i zarządzania systemami. Można stwierdzić, że w zakresie świadczenia usług komunikacyjnych istniejące systemy są bezpieczne dla operatorów, ponieważ mogą oni w sposób niezawodny dostarczać swoim klientom różnorodne usługi. W dostarczaniu klientom usług na wysokim poziomie niebagatelne znaczenie mają scentralizowane systemy zarządzania.

W komunikacji między klientami przekazywana informacja może być stosunkowo łatwo podsłuchana lub zmodyfikowana. Łatwość przeprowadzenia takich działań wynika, przede wszystkim, z braku jakichkolwiek zabezpieczeń w sieciach TK. W sieciach TI sytuacja jest nieco inna, istnieją możliwości zabezpieczania informacji, które z reguły nie wymagają przekazywania ich w czasie rzeczywistym. Do zabezpieczenia przekazywanej informacji stosuje się metody szyfrowania połączeń (sesji) [1] użytkownik – użytkownik, dzięki temu informacja pozyskana przez osoby trzecie jest niezrozumiała (przynajmniej przez jakiś czas).

Na potwierdzenie tezy, że sieci TK i TI są niebezpieczne, zostaną przedstawione możliwości technologiczne pozyskiwania, modyfikowania i uniemożliwiania przekazywania informacji.

TECHNIKI DOSTĘPU DO MEDIÓW TRANSMISYJNYCH

Media transmisyjne w TK i TI w zasadzie są identyczne. Najczęściej stosuje się media miedziane, światłowodowe i radiowe. Istnieją różne techniki „wyłowienia" sygnału transmitowanego w poszczególnych mediach. Ze światłowodu część mocy sygnału może być wyprowadzona na zewnątrz [2, 3] (do innego włókna) z wykorzystaniem sprzęgacza optycznego. Fizyczny dostęp do „gołego" włókna jest możliwy zarówno na stacji, jak i na pewnych odcinkach trasy optycznej. Można wyróżnić dwie metody związane ze stosowaniem sprzęgaczy optycznych. Pierwsza z nich polega na rozłączeniu lub przecięciu światłowodu i wprowadzeniu sprzęgacza. Sytuacja taka zostanie odnotowana przez operatora, niestety przez użytkownika raczej nie, ponieważ zadziała automatyczne przełączenie dokonywane z reguły w czasie mniejszym od 50 ms [9]. Druga metoda jest pozbawiona tej wady (konieczności rozłączenia), ponieważ w tym wypadku stosuje się sprzęgacze, w których sygnał jest pozyskiwany dzięki wyciekowi sygnału z przegięcia włókna o małym promieniu, straty mocy na przegięciu są mniejsze od 1% [3]. Tak pozyskany sygnał może być wprowadzony do odpowiedniego interfejsu odbiorczego. Wybór odpowiedniego odbiornika (urządzenia sieciowego lub analizatora) jest możliwy przy znajomości technologii oraz standardu transmitowanego sygnału. Jeżeli jest on nieznany, łatwo można go określić, stosując dostępną aparaturę diagnostyczno-pomiarową. Ze zdekodowanego sygnału można pozyskać nie tylko informacje przekazywane przez użytkowników sieci, lecz również dotyczące jej konfiguracji.

Ingerencja w tor światłowodowy może być zauważona i zarejestrowana przez operatora, gdy dokonano przerwania włókna światłowodowego. Jeśli w tor zostaje włączony dowolny sprzęgacz optyczny, to po stronie odbiorczej maleje moc dostarczana do odbiornika. Jest to spadek rzędu od 0,1 do 2 dB. Warto pamiętać, że trasy optyczne są projektowane z pewnym zapasem energetycznym i spadek mocy tego rzędu nie spowoduje generacji informacji o zdarzeniu, alarmu czy pojawienia się błędów transmisyjnych, chyba że konstruktorzy systemów przewidzą taką możliwość w oprogramowaniu urządzenia. Większość urządzeń umożliwia monitorowanie wartości odbiorczej mocy sygnału z poziomu systemu zarządzania. Jej zmiany w małym zakresie nie generują alarmów.

Należy zaznaczyć, że zdecydowana większość systemów optycznych pracuje w pełnym dupleksie z wykorzystaniem dwu włókien. Często wystarczy monitorowanie jednego toru, aby uzyskać informacje o korespondencji i jej treści między użytkownikami.

Informacje przesyłane w światłowodzie mogą być zmodyfikowane z wykorzystaniem logicznego systemu *back-to-back* i wiąże się to z ingerencją w tor optyczny, podobnie jak w wypadku klasycznego sprzęgacza optycznego. Po takim zabiegu fizycznym modyfikacja informacji w pewnym uogólnieniu może odbywać się na dwa sposoby: „udawanie" użytkowników końcowych lub wprowadzenie użytkownika dodatkowego. Oprócz łatwości, z jaką można pozyskać informacje z toru światłowodowego, należy zwrócić uwagę na bardzo dużą ilość informacji oraz różnorodność jej źródeł i typów.

W wypadku tzw. mediów miedzianych mamy do czynienia z mniejszą ilością informacji. Nie można stwierdzić, że technika ingerencji w tego rodzaju medium jest łatwiejsza. Zależy to od trybu transmisji sygnałów cyfrowych (w wypadku sygnałów analogowych sytuacja jest o wiele prostsza). W dwutorowowym trybie transmisji, jeśli sygnał jest monitorowany z wykorzystaniem fizycznego dołączenia się do toru interfejsem o wysokiej impedancji, sytuacja jest bardzo prosta. Ta sama metoda w wypadku jednotorowego trybu transmisji jest bardziej złożona i skomplikowana. Podobne jest, gdy do nasłuchu stosuje się zjawisko indukowania sygnału w sąsiednich torach. Metoda wykorzystująca przenik w torach miedzianych nie zawsze znajduje zastosowanie, w większości wypadków jest ona bardzo skomplikowana, wyjątek stanowi telefonia analogowa. Mnogość technolo-

gii i standardów wymaga indywidualnego podejścia do zagadnienia, ich opis byłby zbyt obszerny.

Istnieją systemy, w których monitorowanie torów miedzianych jest możliwe jedynie poprzez włączenie w tor dodatkowego urządzenia. Ingerencja taka powinna być odnotowana przez operatorów sieci. Włączenie dodatkowego urządzenia w tor umożliwia zarówno nasłuchiwanie informacji, jak i jej modyfikację z zastosowaniem technik, których zasada działania jest taka sama jak zasada wykorzystywana w technikach światłowodowych.

W ostatnich kilkunastu latach w komunikacji powszechnie wykorzystuje się technikę radiową (mikrofalową). Dotyczy to wszystkich obszarów sieci TK i TI, począwszy od sieci dostępowych, skończywszy na sieciach szkieletowych. Technika ta jest wykorzystywana w systemach telefonii mobilnej, radiodostępie, systemach radioliniowych, bluetooth, WLAN (ang. *Wireless Local Area Network*) czy WiMax (ang. *Wireless Max*). Na temat bezpieczeństwa trzech ostatnich systemów istnieje dużo opracowań, jest to bardzo aktualne i ważne zagadnienie. W tym artykule skupiono się bardziej na pozostałych systemach.

Pozyskanie sygnału w postaci mikrofal jest bardzo proste i wynika z łatwości dostępu do medium; jedynym utrudnieniem jest dystans. Dostęp do informacji w systemach telefonii mobilnej i radiodostępowych, zawartej w pozyskanym sygnale, zależy od zastosowanych technologii – generacji systemu. Sposób pozyskiwania może być bardzo prosty, wystarczy zwykła aparatura krótkofalarska, lub niesłychanie skomplikowany, jak w wypadku systemów nowszych generacji, w których zastosowano nowoczesne metody szyfrowania [13,14]. Omawiane systemy działają w obszarze dostępowym. Należy uwzględnić fakt, że między użytkownikami na dużym odcinku informacja jest przekazywana środkami naziemnymi (stacjonarnymi), w których nie wykorzystuje się szyfrowania.

Do transmisji wykorzystuje się standardowe interfejsy, agregujące od kilkudziesięciu do kilkudziesięciu tysięcy użytkowników. Przykładami takich interfejsów może być Abis, DSS-1 (ang. *Digital Subscriber Signaling No.1*) czy V5.2 [4, 5, 6, 7, 8].

Inaczej należy podejść do zagadnień bezpieczeństwa informacji w systemach radioliniowych. Tu ilość informacji w niektórych wypadkach może być

porównywalna do ilości informacji transmitowanej z wykorzystaniem klasycznej techniki światłowodowej TDM (ang. *Time Domain Multiplexing*) bez WDM (ang. *Wave Domain Multiplexing*). Dodatkowo nie jest konieczny fizyczny dostęp do drogi transmisyjnej. Nasłuch informacji przekazywanej z wykorzystaniem systemów radioliniowych jest prosty; wystarczy dysponować odpowiednią (ogólnie dostępną) aparaturą, np. diagnostyczno-pomiarową. O wiele bardziej skomplikowana jest modyfikacja informacji przekazywanej drogą radiową.

PRZYKŁADOWA REALIZACJA DOSTĘPU DO KORESPONDENCJI

Jako przykład łatwości dostępu do informacji wybrano interfejs V5.2. Wybierając go, kierowano się wieloma powodami, między innymi takimi, jak: popularność interfejsu w sieciach TK, pewne podobieństwa w architekturze sieciowej oraz stosowanych protokołach do innych interfejsów, np. V5.1, ISDN (ang. *Integrated Services Digital Network*) czy GSM (ang. *Global System for Mobile Communication*), niezależnością od rozwiązań po stronie użytkownika (cyfrowe, analogowe, przewodowe czy bezprzewodowe).

Interfejs V5.2 jest stosowany pomiędzy LE (ang. *Local Exchange*) a AN (ang. *Access Network bądź Access Node*), gdzie stykiem dla tego interfejsu są trakty E1 [8]. Pomiędzy LE a AN stosuje się niezależny przezroczysty system teletransmisyjny [9]. Pozyskany (opisanymi metodami) sygnał z medium transmisyjnego musi być podany na zgodny z nim odbiornik odpowiedniej aparatury. Mogą to być analizatory lub demultipleksery pomiarowe czy krotnice (jedynie ich strona odbiorcza) o przepływności zgodnej z pozyskanym sygnałem. Ze względu na zaawansowane funkcje monitorujące lepsze efekty uzyskuje się, stosując aparaturę diagnostyczno-pomiarową. Określenie przepływności bądź technologii transportowej jest bardzo proste, można do tego wykorzystać powszechnie stosowaną aparaturę, taką jak oscyloskopy lub analizatory widma, czy po prostu konfigurując parametry odbiornika, aż do ustąpienia w nim alarmu LOS (ang. *Loss of Signal*). Kolejną czynnością jest określenie ścieżek cyfrowych do których, zostały odwzorowane trakty E1. W przypadku popularnych systemów SDH (ang. *Synchronous Digital Hierarchy*) [10] jest to stosunkowo proste, dzięki powszechnemu stosowaniu funkcji trasowania w nagłówkach

POH (ang. *Path Overhead*) ścieżek wirtualnych. Po określeniu ścieżek cyfrowych sygnały E1 w liczbie od 1 do 16 (z reguły jest ich co najwyżej kilka) powinny być podane do odbiornika testera protokołów. Po ustaleniu kanału sygnalizacyjnego (zgodnie z [8] jest to szczelina 16. pierwszego traktu E1) należy włączyć monitorowanie warstwy trzeciej. W przypadku usług PSTN (ang. *Public Switched Telephone Network*) wystarczy monitorować jedynie dwa z pięciu protokołów, mianowicie PSTN i BCC (ang. *Bearer Capability Channel*) [11], w przypadku zaś usług ISDN – tylko BCC wraz z włączoną funkcją kopertowania dla wybranego adresu portu logicznego ISDN. Ustalenie adresu logicznego dla usług PSTN i ISDN jest stosunkowo proste (nieopisane w tej pracy). Dzięki takim rozwiązaniom jest możliwe monitorowanie sygnalizacji związanej nie tylko z realizacją usług komunikacyjnych, lecz także z próbą ich realizacji. Ostatnią czynnością jest dołączenie rejestratora korespondencji (np. rejestratora rozmów) równolegle z analizatorem protokołów do traktów E1 oraz sprzęgnięcie tych urządzeń odpowiednim interfejsem, np. popularnym RS232C z jednoczesnym wykorzystaniem obsługi funkcji TRAP [12] w analizatorze.

MOŻLIWOŚCI OPERATORÓW

Opisane rozwiązania dotyczyły możliwości dostępu do informacji przez osoby trzecie. Operatorzy sieci TK czy TI raczej by ich nie stosowali, ponieważ mają wiele innych możliwości. Obecnie technologia stosowana w sieciach pozwala na dostęp w mieście C do informacji przekazywanej z miasta A do B. Pozostając przy problematyce dotyczącej operatorów sieci, należy rozważyć rolę zdalnego zarządzania w kontekście bezpieczeństwa informacji. W ostatnich latach scentralizowano zarządzanie nie tylko sieci, ale i usług. Taka sytuacja na pewno prowadzi do obniżenia kosztów eksploatacji sieci, pozwala równocześnie na koordynację różnych działań w sieci i jest to szczególnie przydatne w monitorowaniu błędów i anomalii. Niestety sieć zarządzania siecią i usługami stanowi dodatkowy element wymagający ochrony. Technologie stosowane do budowy sieci zarządzania stanowią hybrydę różnych rozwiązań – od wykorzystania kanałów sieci zarządzanej po budowę dodatkowych sieci wyłącznie do zarządzania. Rozwiązania te cechuje mnogość zastosowanych protokołów komunikacyjnych i routingowych; dodatkowo stosuje się wiele interfejsów i adapterów, w tym programowych, mających na celu integrację zarządzania usługami. Taki stan sprzyja pojawieniu się

luk, wpływających na bezpieczeństwo informacji transportowanej przez zarządzaną sieć.

MOŻLIWOŚCI DOSTAWCÓW SPRZĘTU

Jeszcze inny problem stanowi potencjalna możliwość dostępu do informacji przez producentów sprzętu sieciowego. Nie można wykluczyć, że producenci sprzętu dostarczonego do eksploatacji nie zapewnili sobie możliwości zewnętrznej ingerencji w sprzęt, np. w postaci wirtualnego użytkownika sieci czy agenta zarządzającego. Dostęp do sprzętu może być realizowany z wykorzystaniem sieci, w której on pracuje lub z wykorzystaniem niezależnych technik komunikacji.

PODSUMOWANIE I WNIOSKI

Sieci i systemy TI wkraczają w wiele dziedzin życia, w tym do przemysłu. Przykładem świadczącym o roli zabezpieczeń może być sieć energetyczna, gdzie mocą steruje się zdalnie i na bieżąco. Nie trudno wyobrazić sobie konsekwencji ingerencji w taką sieć.

Naszkicowane w tym referacie możliwości technologiczne stanowią jedynie podzbiór potencjalnych zagrożeń. Dla podanych przykładów można opracować i przedstawić technologiczne metody przeciwdziałania im. Niemniej na tym etapie można stwierdzić, że powinny one iść w parze z rozwiązaniami systemowo-proceduralnymi.

Biorąc pod uwagę obecnie stosowane rozwiązania technologiczne w sieciach TK oraz uwzględniając konwergencję wielu usług (w tym transportowych) realizowanych przez sieci TI z wykorzystaniem np. technologii IP (ang. *Internet Protocol*), najkorzystniejszą metodą zabezpieczeń informacji jest metoda użytkownik – użytkownik. Zawansowane techniki szyfrowania powinny być zastosowane nie tylko w urządzeniu abonenckim, lecz w każdym dowolnym urządzeniu brzegowym sieci, np. w centrali PABX (ang. *Private Branch Exchange*).

Literatura

[1] Łukasik Z., *Teoria informacji i bezpieczeństwa transmisji,* Politechnika Radomska 2000.

[2] *Norscan Instruments Limited: Fiber Optic Intrusion Detection Systems,* 2003.

[3] *Info Guard: Risks and Dangers of Fiber Optic Cables,* 2004.

[4] Hołubowicz W., Płuciennik P., *Cyfrowe systemy telefonii komórkowej,* Wyd. 3, Poznań 1998.

[5] *ETSI Specification ETS 300 125, Integrated Services Digital Network (ISDN) – User- Network Interface Data Link Layer Specification,* 1993.

[6] *ITU-T Recommendation Q.931: Digital Subscriber Signaling System No.1 (DSS 1) – ISDN User- Network Interface Layer 3 Specification for Basic Call Control ,* Helsinki 1998.

[7] Kościelnik D., *ISDN cyfrowe sieci zintegrowane usługowo,* Wydawnictwo Komunikacji i Łączności, Warszawa 2001.

[8] *ETSI Specification ETS 300 347, V5.2 Interface Specification for the Support of Access Networks,* 1996.

[9] Kula S., *Systemy teletransmisyjne,* Wydawnictwo Komunikacji i Łączności, Warszawa 2005.

[10] *ITU-T Recommendation G.707: Network Node Interface for the Synchronous Digital Hierarchy (SDH),* Geneva 1996.

[11] Gillespie A., *Access Networks- Technology and V5 Interfacing, Artech House. Inc,* Boston – Lodyn 1997.

[12] *Tektronix, Test Measurement and Monitoring Products Catalog 2003,* Copyright by Tektronix Inc., 2002.

[13] Haykin S., *Systemy telekomunikacyjne,* Wydawnictwo Komunikacji i Łączności, Warszawa 1998.

[14] Killen H., *Transmisja cyfrowa w systemach światłowodowych i satelitarnych,* Wydawnictwo Komunikacji i Łączności, Warszawa 1992.