WYMAGANIA TECHNOLOGICZNE W ODNIESIENIU DO SYSTEMÓW TELEKOMUNIKACYJNYCH I TELEINFORMATYCZNYCH W OBSZARZE SIŁ ZBROJNYCH

Robert Goniacz

WYMAGANIA TECHNOLOGICZNE
Obszar sił zbrojnych

Najważniejsze problemy poruszane w referacie dotyczą następujących zagadnień:

- *Wymagania technologiczne stawiane wojskowym systemom teleinformatycznym(TI) i telekomunikacyjnym (TK).*
- *Analiza wymagań technologicznych stawianych wojskowym systemom TI i TK w aspekcie funkcjonowania w obszarze państwa.*
- *Wymagania technologiczne stawiane wojskowym systemom TI i TK w aspekcie współpracy w ramach NATO i współpracy międzynarodowej.*

Współczesne wojskowe systemy telekomunikacyjne i teleinformatyczne muszą bezwzględnie charakteryzować się wysokim poziomem niezawodności i zapewnić użytkownikom odpowiedni poziom bezpieczeństwa. Ze względu na charakter informacji wymienianych pomiędzy użytkownikami systemów wojskowych rzadko mają one klauzulę poufności „jawne". Informacje tego typu mogą być, po uprzednim zaaprobowaniu, przesyłane za pomocą sieci publicznych – dotyczy to również informacji wymienianych w ramach współpracy państw NATO.

Przez pojęcie sieci publicznych należy tu rozumieć obecnie najczęściej używany Internet i usługi wykorzystujące stos protokołów TCP/

IP (e-mail, ftp, VoIP, portale WWW itp.). W odniesieniu do takiego sposobu wykorzystania sieci publicznych i rodzaju przesyłanych w nich informacji, sposobów i zasad zapewnienia poufności i integralności danych oraz zapewnienia odpowiedniego poziomu jakości usług (*Quality of Service*) reguły obowiązujące w tego typu sieciach wojskowych nie różnią się od stosowanych w sieciach publicznych, korporacyjnych, akademickich itp. Rozwiązania technologiczne przyjęte do stworzenia infrastruktury komunikacyjnej, modele logiczne powiązań pomiędzy elementami sieci oraz rodzaj zastosowanych zabezpieczeń nie różnią się od już opisanych.

Ze względu na to, że informacje przesyłane w sieciach wojskowych zazwyczaj mają klauzulę poufności wyższą niż „jawne", sposoby zabezpieczeń w opisanych systemach są niewystarczające. Jednym ze sposobów podniesienia poziomu bezpieczeństwa jest budowa autonomicznej i odseparowanej od innych sieci infrastruktury TI lub TK. Możliwe jest to, podobnie jak w innych służbach, poprzez dzierżawienie od operatorów telekomunikacyjnych wydzielonej linii lub budowę własnej infrastruktury. Podjęcie działań mających na celu przejęcie informacji przesyłanych w tych sieciach jest jednak w dalszym ciągu możliwe, ich pozyskanie nie jest jednak łatwe. Wymagałoby bowiem, w pierwszej kolejności, wiedzy o fizycznej budowie systemu lub ingerencji osób od wewnątrz. Technologie wykorzystywane do budowy takich systemów zasadniczo nie różnią się niczym od tych stosowanych w rozwiązaniach cywilnych (sieci rozległe, infrastruktura oparta na sieciach transmisyjnych SDH lub ATM). Elementem zabezpieczającym przed przechwyceniem informacji tworzonych w elementach takich sieci jest elektromagnetyczna separacja urządzeń (jednostki centralne, monitory komputerowe, drukarki, elementy sieciowe itp.). W dzisiejszych rozwiązaniach dopuszcza się stosowanie urządzeń zaprojektowanych specjalnie do tego celu, tzw. urządzeń o obniżonym poziomie emisji elektromagnetycznej lub specjalnych komór ekranujących, obniżających emisję urządzeń komercyjnych (przez to pojęcie należy rozumieć urządzenia powszechnie stosowane w rozwiązaniach cywilnych i dostępne dla każdego użytkownika).

Pomimo zapewnienia separacji od innych sieci i zabezpieczenia urządzeń końcowych najczęściej dla zapewnienia poufności i integralności informacji stosuje się dodatkowe elementy w postaci urządzeń kryptograficznych, mających na celu utajnienie informacji w warstwie łącza danych (ze względu na charakter tego opracowania szczegóły dotyczące samych urządzeń, konfiguracji i zasady działania nie będą tutaj opisane).

Dodatkowym i niezbędnym elementem jest natomiast system odpowiedniego szkolenia i doboru kadr, zarówno po stronie użytkownika sieci telekomunikacyjnej i (lub) operatora telekomunikacyjnego świadczącego usługi. Do pracy przy urządzeniach sieciowych i kryptograficznych mogą być dopuszczone wyłącznie osoby posiadające certyfikaty bezpieczeństwa wydane przez uprawnione do tego służby.

Koszty utrzymania systemów bazujących na wymienionych rozwiązaniach są duże. Przede wszystkim, wysokie nakłady przeznacza się na infrastrukturę transportową (dzierżawienie osobnych linii), utrzymanie własnego personelu technicznego. Z tego powodu oraz ze względu na fakt, że obecnie elementy sieci IP oferują QoS wymagane przez usługi stosowane w sieciach wojskowych, coraz częściej jako sieć transportową wykorzystuje się Internet.

Zabezpieczenia informacji w sieci Internet stosowane powszechnie w rozwiązaniach cywilnych nie są niestety akceptowane dla zastosowań wojskowych – zarówno krajowych, jak i wykorzystywanych w NATO – ze względu na małą moc kryptograficzną zastosowanych algorytmów. Rozwiązaniem dopuszczonym do zastosowań wojskowych jest wykorzystanie urządzeń typu „Spiec", umożliwiających budowę prywatnych sieci wirtualnych (*Virtual Private Network* – VPN) lub zapewniających bezpieczną komunikację pomiędzy pojedynczymi elementami (*end-to-end*). Urządzenia te spełniają standardy opracowane przez Internet Engineering Task Force (IETF) i zapewniają poufność, integralność oraz autentyfikację informacji przesyłanych przez publiczną sieć IP. Szczegóły protokołów, na których jest oparty IPsec, są opisane w [1] i [2].

Typowe urządzenia zaaprobowane do użytku w sieciach NATO posiadają następujące cechy: algorytmy szyfrowania zaakceptowane przez NATO, interfejs Ethernet 10 Mbit, bezpieczeństwo dla 500 lub 900 datagramów IP na sekundę, do 1000 bezpiecznych połączeń, praca w sieci złożonej z maksymalnie 1000 takich urządzeń, scentralizowane zarządzanie i kontrola, kompatybilność elektromagnetyczna spełniająca normy AMSG 720B.

Z punktu widzenia zastosowań w krajowych systemach wojskowych, urządzenia od dostawców zewnętrznych mogą być użyte tylko dla sieci o klauzuli poufności do poziomu „zastrzeżone" włącznie. Sieci o klauzuli „tajne" wymagają urządzeń, w których są stosowane m.in. bezpieczne na-

rodowe algorytmy kryptograficzne (wymagania dla sieci o klauzuli „tajne" dotyczą również komponentów danego urządzenia). Tak wysokie wymagania wynikają m.in. z faktu, że potencjalnie przechwycone informacje muszą pozostać tajne przez następne 50 lat.

Zaletami takiego sposobu zabezpieczeń jest bezspornie dostępność sieci opartych na IP (głównie Internet), natomiast tam, gdzie ich nie ma, łatwość realizacji za pomocą dostępnych środków łączności (łącza radiowe, radioliniowe, satelitarne, przewodowe).

Bezpieczna współpraca pomiędzy elementami narodowych systemów państw NATO z reguły polega na wymianie informacji (danych) z wykorzystaniem wspólnie opracowywanych i budowanych elementów stanowiących bezpieczny interfejs (lub *gateway*) wymiany danych. Prace standaryzacyjne prowadzone obecnie dotyczą m.in. opracowywania rozszerzeń do istniejących publicznych standardów bezpiecznej wymiany dokumentów XML (*eXtensible Markup Language*), m.in. urządzeń typu XML *firewall*, rozszerzeń do protokołów stosowanych do wymiany dokumentów XML, rozszerzeń protokołów dostępu do serwerów aplikacji.

We współcześnie projektowanych systemach wojskowych należy brać pod uwagę możliwości współpracy systemów (lub elementów systemów) w zakresie wymiany informacji opartej na architekturze SOA (*Service Oriented Architecture*). Obecnie trwają prace standaryzacyjne, w ramach państw członkowskich NATO, dotyczące bezpiecznej wymiany informacji pomiędzy domenami o różnej klauzuli bezpieczeństwa. Polegają one przede wszystkim na dogłębnej analizie istniejących i obowiązujących standardów wymiany informacji, stosowanych w sieciach IP, wyszukaniu słabości tych rozwiązań i opracowaniu rozszerzeń, których implementacja zapewni możliwość ich stosowania w sieciach wojskowych NATO. Wyniki prac w postaci referencji i zaleceń są udostępniane zainteresowanym krajom członkowskim.

Warto tu wspomnieć o współczesnych mobilnych sieciach wojskowych. Zazwyczaj to one są kojarzone z zadaniami, jakie wykonują obecnie siły zbrojne, a nie wojskowe sieci stacjonarne. Ze względu na specyficzne wymagania (niezawodność, mobilność, rodzaj świadczonych usług, bezpieczeństwo, wykorzystane środki transmisyjne) wojskowe systemy mobilne TI/TK należą do najbardziej zaawansowanych technologicznie.

W rozwiązaniach krajowych są wykorzystywane m.in. technologie ATM – sieć szkieletowa z gwarantowanym poziomem jakości usług, ISDN, nowoczesne środki radioliniowo-przewodowe (światłowodowe), nowoczesne metody zarządzania elementami sieci, sprzętowa kryptografia. Posiadają one interfejsy do współpracy z zewnętrznymi systemami TI/TK i mogą być również wykorzystywane jako sieci transportowe. Realizacja nowych usług w tych sieciach wymagałaby tylko implementacji nowych aplikacji (programów komputerowych) bądź zastosowania odpowiednich urządzeń, które wykorzystują sieci IP. Cała infrastruktura transportowa jest zapewniona przez sieć.

PODSUMOWANIE

Na podstawie zagadnień poruszonych w tym artykule można wysnuć wniosek, że istnieje konieczność dogłębnej analizy bezpieczeństwa komponentów w procesie planowania i budowy wojskowych systemów TI.

Dzisiejsze rozwiązania technologiczne umożliwiają wykorzystanie publicznej infrastruktury telekomunikacyjnej jako platformy transportowej, w odróżnieniu od sieci i systemów autonomicznych. Z jednej strony, umożliwia to łatwiejszy dostęp do informacji, z drugiej natomiast, implikuje konieczność zwrócenia szczególnej uwagi na aspekty bezpieczeństwa informacji wymienianych pomiędzy elementami (użytkownikami) sieci oraz samych elementów ją tworzących.

W procesie planowania bezpiecznych sieci wojskowych zachodzi konieczność dostosowania ich do istniejących standardów bezpieczeństwa lub współtworzenia i implementacji nowych, w ramach współpracy państw NATO. Rozwiązaniami, które najczęściej są wykorzystywane w elementach sieci przeznaczonych do pracy na obszarze kraju oraz w elementach wydzielonych do współpracy międzynarodowej, są implementacje istniejących standardów oraz rozwiązania polegające na modyfikacjach części standardu w celu zwiększenia bezpieczeństwa. Implementacja takich interfejsów zapewnia nie tylko niezależność od systemów innych krajów, lecz także jest technologicznym potwierdzeniem gotowości do współpracy i podniesieniem prestiżu.

Jedną z najbardziej „obiecujących" propozycji w zakresie bezpieczeństwa w sieciach wojskowych i wykorzystujących publiczną infrastrukturę transportową jest stosowanie urządzeń tunelujących ruch typu IPsec i wykorzystujących narodowe rozwiązania kryptograficzne.

Literatura

[1] *RFC 2401, Security Architecture for the Internet Protocol.*

[2] *RFC 2402, IP Authentication Header.*