ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1993

Seria: INFORMATYKA z. 24 Nr kol. 1222

Andrzej GRZYWAK

BEZPIECZEŃSTWO W SYSTEMACH ROZPROSZONYCH

Streszczenie. Bezpieczeństwo systemów rozproszonych to bezpieczna eksploatacja sieci komputerowych różnego rodzaju zintegrowanych ze sobą. Problem bezpieczeństwa systemu rozproszonego wymaga rozwiązania szeregu składowych czynników, takich jak:

- kontrola dostępu do zasobów z uwzględnieniem uprawnień,
- sprawdzenie autentyczności użytkowników sieci,
- ustalenie rejonów zaufania,
- wprowadzenie kryptografii do systemów przekazywania informacji,
- rozwiązanie problemu dystrybucji klucza,
- identyfikacja użytkownika systemu

Artykuł przedstawia zasadnicze koncepcje realizujące bezpieczne systemy rozproszone.

SECURITY IN DISTRIBUTED SYSTEMS

Summary. Distributed system security is presented in the context of a general model of computing. A central role in distributed system security playes: cryptographic techniques access controls autentication. The future direction of distributed system security will be determined largely by standards.

SÉCURITÉ DANS LES SYSTEMES DISTRIBUES

Résumé. La sécurité des systèmes distribués est présenté dans le contexte du modèle de calcul général. La plus grande rôle, dans la sécurité des systèmes jouent: la technique cryptographique d'accès aux systèmes, contrôle des régions de confiance et l'identification des usagers. L'avenir de la sécurité dans les systemes sera déterminée par standardisation.

1. Wprowadzenie

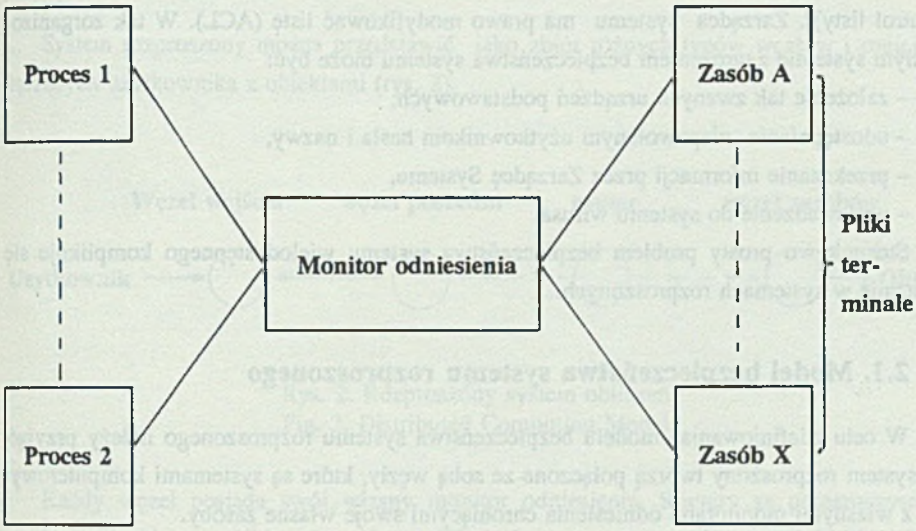
Stosowanie systemów rozproszonych, których działanie oparte jest na sieciach komputerowych różnego typu, wymaga w przeważającej liczbie przypadków rozwiązania problemu bezpieczeństwa pracy sieci. Bezpieczeństwo pracy sieci, to przede wszystkim ochrona zasobów rozproszonych i ochrona przekazywania informacji w sieci. Bezpieczeństwo sieci komputerowej można przyrównać w najogólniejszy sposób do bezpieczeństwa systemu operacyjnego.

Artykuł niniejszy ma na celu zdefiniowanie pojęć i metod związanych z bezpieczeństwem systemów rozproszonych, dokonanie analizy metod stosowanych w celu poprawienia bezpieczeństwa oraz ustalenie wytycznych w celu rozwiązania tego aktualnego problemu dla rozwoju zastosowań. Należy zwrócić uwagę na fakt, że w kraju stosuje się już obecnie systemy rozproszone, które są wyposażone w "silne" mechanizmy zapewniające bezpieczeństwo. Do tej kategorii systemów można zaliczyć np.sieć typu INTERNET, której INTERNET gałąź rządowa, czy też militarna jest niedostępna dla większości krajowych użytkowników.

2. Definicja pojęć związanych z bezpieczeństwem sieci

Tak zwany model bezpieczeństwa w systemach rozproszonych musi być ściśle powiązany z ogólnym modelem obliczeń. Należy założyć, że model obliczeń obejmuje wiele aplikacji uruchamianych "on line" przez wielu użytkowników, realizację pewnych procesów w tle oraz pracę wsadową niektórych MC system.

Koncepcja bezpieczeństwa systemu rozproszonego nawiązuje do rozwiązanego wcześniej problemu bezpieczeństwa systemu wielodostępnego (multi-user). System wielodostępny (rys. 1) w zakresie bezpieczeństwa opiera swoje działanie na tak zwanym monitorze odniesienia, którym jest jednostka centralna, system operacyjny i tak zwany program zaufania.



Rys. 1. System wielodostępny
Fig. 1. Standalone System Model

Monitor odniesienia realizuje szereg funkcji, takich jak:
- sterowanie pracą zbioru zasobów,
- uruchamianie dostępu do zasobów (plików, terminali, urządzeń wejścia/wyjścia),
- wykonywanie tak zwanej strategii bezpieczeństwa.

Praca monitora odniesienia zakłada, że procesy nie mają do siebie zaufania. System bezpieczeństwa wymaga zdefiniowania strategii bezpieczeństwa, która wiąże się przede wszystkiem ze strategią przyznawania dostępu do zasobów. Strategia bezpieczeństwa wymaga:

1) przyznania zasobom unikatowych nazw,
2) sprawdzenia przez monitor odniesienia autentyczności nazw,
3) przyznania użytkownikom (procesora) nazw i haseł.

Nazwa użytkownika i prawidłowe hasło tworzą symbol indentyfikacyjny (ID).

Monitor odniesienia porozumiewa się z użytkownikiem i tworzy dla niego tak zwaną ścieżkę zaufania łączącą użytkownika z zasobami.

Kontrola dostępu w systemach tego rodzaju musi zawierać definiowanie praw dostępu do wykonania różnych operacji (*czytaj, pisz, modyfikuj* itp.).

Obiekt jest związany z listą nazw procesów, które mają do niego dostęp [ACL (access kontrol listy)]. Zarządca systemu ma prawo modyfikować listę (ACL). W tak zorganizowanym systemie zagrożeniem bezpieczeństwa systemu może być:

- założenie tak zwanych urządzeń podstawowych,
- udostępnienie niepowołanym użytkownikom hasła i nazwy,
- przekazanie informacji przez Zarządcę Systemu,
- wprowadzenie do systemu wirusa.

Stosunkowo prosty problem bezpieczeństwa systemu wielodostępnego komplikuje się znacznie w systemach rozproszonych.

2.1. Model bezpieczeństwa systemu rozproszonego

W celu zdefiniowania modelu bezpieczeństwa systemu rozproszonego należy przyjąć, że system rozproszony tworzą połączone ze sobą węzły, które są systemami komputerowymi z własnymi monitorami odniesienia chroniącymi swoje własne zasoby.

Węzłowy monitor odniesienia jest odpowiedzialny wyłącznie za "bezpieczeństwo" węzła i realizuje tak zwaną węzłową strategię bezpieczeństwa. Najważniejszą różnicę pomiędzy bezpieczeństwem systemu rozproszonego a wolnostojącego stanowi mechanizm, którego używa monitor odniesienia, aby ustanowić zaufanie odwzorowania pomiędzy lokalnymi i odległymi nazwami procesów.

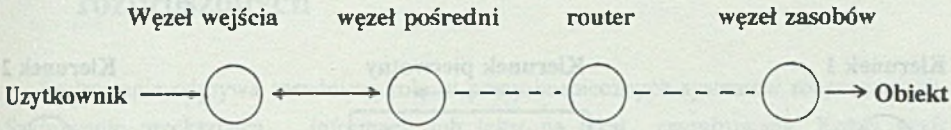
W systemie rozproszonym można założyć, że tak zwany "kierownik", którym jest każda jednostka aktywna, może generować żądania dostępu do innego kierownika. Każdy kierownik ma zdefiniowane swoje własne prawa.

Rozpatrując rodzaje węzłów występujących w systemie rozproszonym można wyróżnić tak zwane"węzły przyjazne". Węzłami przyjaznymi nazywamy węzły realizujące tę samą strategię bezpieczeństwa. Węzły przyjazne udostępniają sobie na żądanie pliki. Węzły tego samego typu tworzą regiony zaufania. W sieci może być, oczywiście, wiele różnych regionów zaufania, co wiąże się z różnymi strategiami bezpieczeństwa.

W celu zdefiniowania bezpieczeństwa sieci przyjmuje się, że informacja, którą transmitują węzły, może "wędrować" po całej sieci (system w pełni połączony). Jeżeli informacja ta nie jest zaszyfrowana, to każdy może ją w sieci "przeczytać". Każdy węzeł może odebrać każdą informację z innego węzła i żaden czynnik zewnętrzny nie może temu zapobiec. Jeżeli odległy węzeł otrzyma informację, to nie ma on innej możliwości, jak tylko zaufać tej informacji. Z tego powodu węzeł, który przesyła informację, musi zwrotnie otrzymać z węzła odległego potwierdzenie, że jest on węzłem zaufania. Wynika stąd wymaganie, że informacje związane z żądaniami dostępu muszą być sprawdzane przez węzeł. Zaufanie do innych węzłów musi być oparte na zrozumiałym modelu zaufania.

2.2. Model obliczeń w systemie rozproszonym

System rozproszony można przedstawić jako zbiór różnych typów węzłów i routerów łączących użytkownika z obiektami (rys. 2).



Rys. 2. Rozproszony system obliczeń
Fig. 2. Distributed Computing Model

Każdy węzeł posiada swój własny monitor odniesienia. Routery są przezroczyste z punktu widzenia strategii bezpieczeństwa. Węzły i routery tworzą tak zwaną kaskadę działania.

Dla dowolnej kaskady działania można przyjąć następujące założenia:

- użytkownik współpracuje tylko z jednym węzłem,
- węzeł wejścia współpracuje z węzłem pośrednim,
- węzeł zasobów współpracuje z jednym węzłem pośrednim,
- węzeł zasobów odbiera żądania dostępu do zasobów węzła pośredniego,
- router nie interpretuje ani nie modyfikuje informacji,
- węzły, które nie współdziałają ze sobą, są tak zwanymi węzłami nieosiągalnymi.

Dla przyjętych założeń można zdefiniować zależności zaufania między elementami systemu rozproszonego:

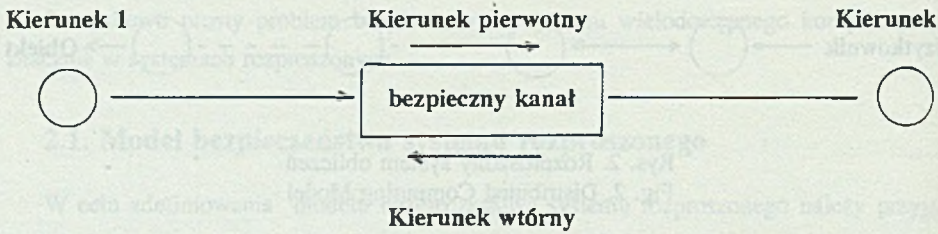
1. Węzeł wejścia sprawdza autentyczność użytkownika.
2. Użytkownik sprawdza autentyczność węzła.
3. Węzeł wejścia sprawdza autentyczność węzła pośredniego.
5. Węzeł zasobów sprawdza prawo dostępu do zasobów.
6. Komunikacja zabezpiecza przed zniekształceniami transmisji

3. Zagrożenia w systemach rozproszonych

W systemach rozproszonych należy rozwiązać zarówno problem bezpieczeństwa usług, jak i problem bezpieczeństwa informacji.

Usługi bezpieczeństwa wiążą się z każdą warstwą modelu OSI/ISO. Definiuje się je jako określone właściwości realizowanych funkcji.

Podstawowym problemem w realizacji bezpiecznych usług jest autentyfikacja. Usługa ta pozwala autentyfikującemu kierownikowi zlokalizować bezpieczny kanał do autetyfikowanego kierownika. Proces autentyfikacji jest realizowany dwustronnie.



Rys. 3. Usługa autentyfikacji
Fig. 3. Authentyfication service

Bezpieczny kanał może być kanałem fizycznym lub wirtualnym. Musi on spełniać warunek poufności i integralności usług. Poufność usług oznacza , że informacja jest nieczytelna dla nieautoryzowanych. Integracja usług bezpiecznego kanału oznacza, że informacja jest zabezpieczona przed zniekształceniem.

W rozproszonych systemach zagrożeniem bezpieczeństwa jest:

- pasywne podłączenie się tak zwanego "napastnika", który może odbierać informację,
- aktywne podłączenie się "napastnika", który może odczytywać i modyfikować informację.

Mechanizmami wywołującymi zagrożenia są:

- zmiana tożsamości użytkownika,
- nadużycie przydzielonych nazw i uprawnień,
- instalacja wirusa w oprogramowaniu sieci,
- penetracje w systemie operacyjnym.

Należy zwrócić uwagę na fakt, że pasywne podłączenie do sieci stwarza możliwość obserwacji pracy systemu rozproszonego. Na podstawie obserwacji "napastnik" może wiele wydedukować. Istnieją tak zwane techniki obrony przed dedukcją.

Zagrożeniem w sieci może być również przeciążenie serwera plików tak, że nie potrafi on zareagować na prawowite żądanie.

4. Zastosowanie kryptografii w systemach rozproszonych

Szyfrowanie odgrywa zasadniczą rolę w pracy bezpiecznych systemów rozproszonych. Szyfrowanie przekształca informacje lub tekst na tekst zaszyfrowany. Każdy szyfr posiada określone cechy, które można dostosować do realizowanych w systemie rozproszonym aplikacji.

Algorytmy szyfrowania i deszyfrowania są powszechnie znane. Utajniony jest tak zwany klucz. Znane i stosowane są dwa typy algorytmów kryptograficznych:

- algorytmy symetrycznego klucza,
- algorytmy asymetrycznego klucza.

W algorytmie symetrycznego klucza ten sam klucz (k) używany jest do szyfrowania (E) i deszyfrowania (D). Oznaczając informację pierwotną przez (M), a informację zaszyfrowaną przez M', można zapisać:

$$M' = Ek(M)$$

$$M = Dk(M')$$

Dobry algorytm szyfrowania musi mieć tę cechę, że znajomość M', D i E nie może doprowadzić do śladów klucza k i M. Dla informacji reprezentowanej przez ciąg liczb binarnych wymieniona cecha algorytmu oznacza, że zmiana jednego bitu M daje niemożliwą do przewidzenia zmianę wszystkich bitów M'. Każdy bit M' może przyjąć wartość "0" lub "1" z prawdopodobieństwem 50%. Algorytm tajnego klucza może być użyty do zachowania poufności i integralności.

Jeżeli użytkownicy "A" i "B" są jedynymi, którzy dzielą tajny klucz, to "A" może przyjąć, że wiadomość (M), którą zaszyfrowano kluczem (k) może przyjąć tylko (B). (B) może ustalić, że odebrana wiadomość (M') została zaszyfrowana przez (A).

Bezpieczeństwo algorytmu szyfrowania jest funkcją liczby możliwych do zastosowania kluczy (klucz o określonej długości).

Algorytmy symetrycznego klucza są stosowane do transmisji plików. Tak zwany Data Energyption Standard zakłada, że klucz ma 64 bity (algorytm typu DES).

Tak zwana kryptografia oparta na algorytmach asymetrycznych ma uprościć problem bezpiecznego dostarczenia klucza.

Dla algorytmów asymetrycznych każdy użytkownik posiada klucz ogólny (pk) oraz klucz prywatny (sk). Istnieje ścisła relacja pomiędzy (pk) a (sk). Relacja ta oznacza, że wiadomość zaszyfrowana za pomocą (pk) może być rozszyfrowana przy użyciu klucza (sk).

$$M' = Epk(M)$$

$$M = Dsk(M')$$

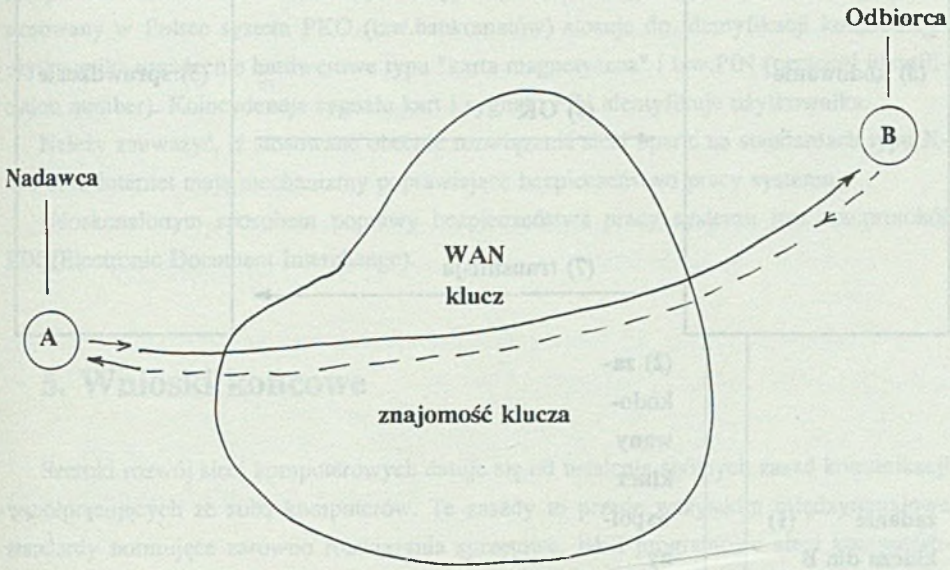
W sieciach komputerowych stosuje się szyfrowanie dwoma sposobami:
- szyfrowanie periodyczne (serial encryption),
- szyfrowanie pakietowe (packet encryption)

Szyfrowanie periodyczne ogranicza się do warstwy fizycznej i warstwy danych, gdzie informacja jest "przenoszona" jako strumień bitów i tam, gdzie istnieje pojęcie *wiadomości*. Transmisja pakietów lub datagramów szyfrowania dotyczy określonej jednostki "wiadomości". Istnieje wówczas niezależność logiczna jednego pakietu od drugiego, co umożliwia stosowanie efektywniejszych metod szyfrowania. Przy szyfrowaniu pakietowym część nagłówka jest nieszyfrowana. Wynika to z faktu, że węzły sieci muszą identyfikować np. adresy w celu realizacji połączeń.

Zasady szyfrowania są ujęte w tak zwanych *protokołach szyfrujących*, które są dołączane do istniejących architektur logicznych sieci. Z szyfrowaniem jest związana tzw.*ochrona powtórna* (replay protection). Ochrona ta ma zapewnić niemożność powtórnej transmisji przy wymianie przez napastnika zaszyfrowanej informacji. W celu "zwalczania" powtórzeń nadawca wysyła między pakietami kolejne liczby (tzw.wybielanie pakietów). Ten typ ochrony jest implementowany zwykle w łączach danych.

W celu autentyfikacji nadawcy stosuje się protokoły oparte na zasadzie "znajomości" klucza (konwersacja potwierdzająca znajomość tajnego klucza).

Protokół zaufanych wyjść ma potwierdzić fakt, że łączność nawiązano z właściwą stacją, a nie z tzw.oszustem.



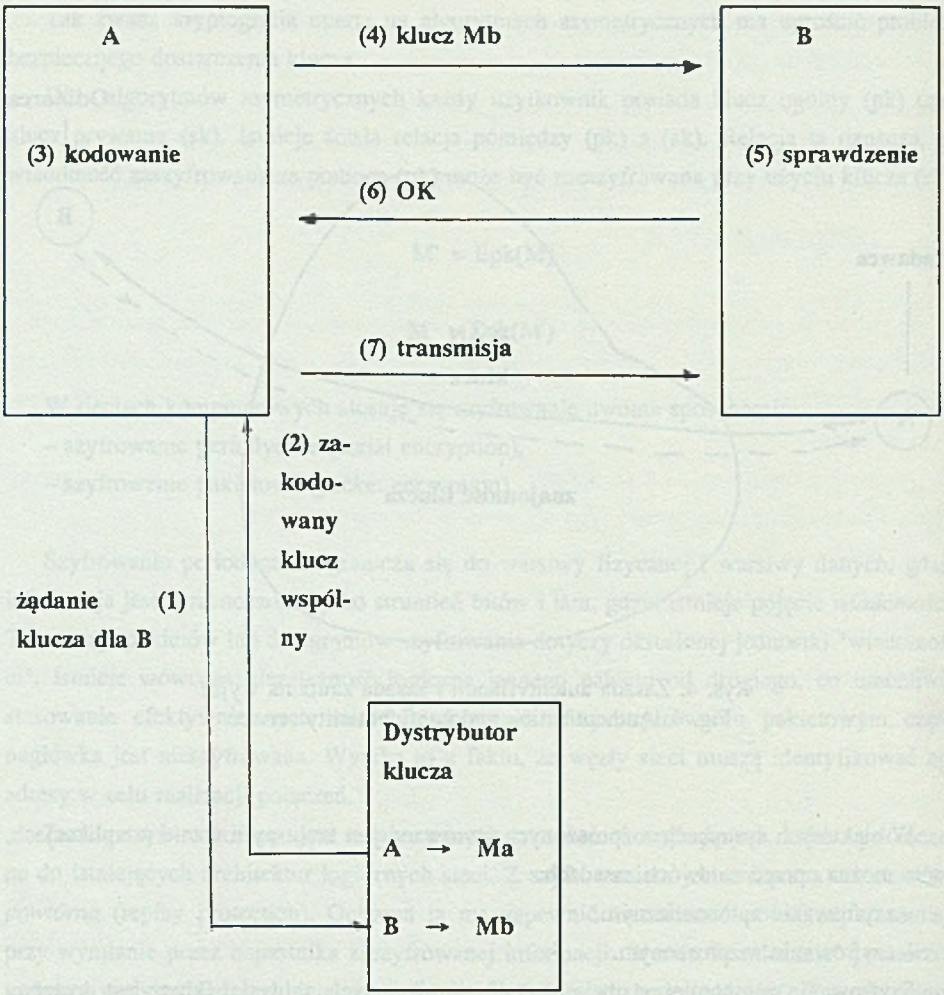
Rys. 4. Zasada autentyfikacji i zasada zaufania wyjść
Fig. 4. Authentication and confidentiality service

W niektórych systemach rozproszonych stosowane jest tzw. szyfrowanie w aplikacjach, które można oprzeć na dwóch zasadach:

- szyfrowaniu autonomicznym,
- szyfrowaniu rozproszonym.

Szyfrowanie autonomiczne obejmuje tylko zapis danych na dysku (klucz jest dostępny tylko w określonym systemie), natomiast szyfrowanie rozproszone obejmuje szyfrowanie tekstów i dystrybucję klucza. Dystrybucja klucza stanowi zaś istotny element bezpieczeństwa pracy rozproszonego systemu.

Klucz można rozprowadzać "ręcznie" lub "automatycznie". Ręczne rozprowadzanie klucza może doprowadzić do przekazania go w niepowołane ręce. Z tego też powodu stosuje się obecnie metody automatycznego rozprowadzania klucza przez tzw. *ośrodek dystrybucji klucza* (Key Distribution Center) (rys. 5).



Rys. 5. System dystrybucji klucza
Fig. 5. Online key distribution

Przedstawiony system dystrybucji klucza jest oparty na omówionej zasadzie konwersacji. System ten umożliwia wprowadzenie zasady periodycznej zmiany klucza.

System dystrybucji klucza przedstawiony na rys. 5 pracuje na zasadzie tzw. słownika kluczy ogólnodostępnych. Stosowanie klucza umożliwia zarówno szyfrowanie, jak i identyfikowanie użytkownika sieci. Systemy te wymagają jednak zaufanego odwzorowania nazw użytkowników i ich ogólnego klucza.

W bezpiecznych systemach rozproszonych stosuje się, poza omówionymi mechanizmami, jeszcze tak zwane *mechanizmy identyfikacji konkretnego użytkownika*. Na przykład stosowany w Polsce system PKO (tzw.bankomatów) stosuje do identyfikacji konkretnego użytkownika urządzenie hardwerowe typu "karta magnetyczna" i tzw.PIN (personal identification number). Koincydencja sygnału kart i sygnału PIN identyfikuje użytkownika.

Należy zauważyć, iż stosowane obecnie rozwiązania sieci oparte na standardach typu X-400 oraz Internet mają mechanizmy poprawiające bezpieczeństwo pracy systemu.

Udoskonalonym sposobem poprawy bezpieczeństwa pracy systemu jest tzw.protokół EDI (Electronic Document Interchange).

5. Wnioski końcowe

Szeroki rozwój sieci komputerowych datuje się od ustalenia spójnych zasad komunikacji współpracujących ze sobą komputerów. Te zasady to przede wszystkim międzynarodowe standardy normujące zarówno rozwiązania sprzętowe, jak i programowe sieci komputerowych.

Rozwiązanie problemu bezpieczeństwa pracy systemów rozproszonych jest bez wątpienia zagadnieniem znacznie bardziej złożonym. Jak wynika z rozważań przedstawionych w artykule, bezpieczny system rozproszony musi uwzględniać takie czynniki, jak:

- kontrolę dostępu do zasobów z uwzględnieniem uprawnień,
- sprawdzenie autentyczności użytkowników sieci,
- ustalenie regionów zaufania,
- wprowadzenie kryptografii do systemów przekazywania informacji,
- rozwiązanie problemów dystrybucji klucza,
- identyfikację użytkownika systemu (identyfikacja osoby).

Wszystkie wymienione problemy wymagają również pewnych prac standaryzacyjnych, które umożliwią szerokie stosowanie bezpiecznych systemów rozproszonych w różnych aplikacjach.

LITERATURA

[1] Rozproszone systemy mikrokomputerowe, t.VI (Projekt Badawczy "Grant" PB-401/3/91), Materiały Instytutu Informatyki Pol.Śląskiej, Gliwice 1993.

[2] Recent Technical Developments in Telecommunications, Paul Levaux, North-Holland, 1992

[3] American National Standards Institute (ANSI) Data Encryption Algorithm X3.92

[4] Internetional Standards Organization Information processing Systems – Open System Interconnection Basic Reference Model-Part 2 Security Architecture ISO IS7498-2, 1988

[5] Okamato E., Tanaka K.: Key Distribution SystemBased on Identification Information, IEEE Journal 7(4)481-485, May 1989

Recenzent: Prof. dr inż. Stefan Węgrzyn

Wpłynęło do redakcji: 20 września 1993 r.

Abstract

This paper is a tutorial on the state of the art in the architecture, design and implementation of secure distributed systems. Distributed system computeing model is presented in which all information, whether in transit between and systems or resident within an end system, is equivalently protected under a unified architecture. Since cryptography is a basic mechanism used to implement many of security mechanisms for distributed systems, considerable space is devoted to a discussion of enecryption technology. Security is usually added to systems and protocols.