ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1997
Seria: INFORMATYKA z. 32 Nr kol. 1356

Andrzej BARCZAK, Lesław MACHERZYŃSKI, Piotr WOLSKI, Tadeusz SZUSZKIEWICZ
Wyższa Szkoła Oficerska Wojsk Łączności
Krzysztof SILICKI
Naukowa i Akademicka Sieć Komputerowa NASK

PROBLEMY OCHRONY INFORMACJI W SIECIACH KOMPUTEROWYCH

Streszczenie. W referacie omówiono dwa zagadnienia mające istotny wpływ na bezpieczeństwo sieci. Pierwsze dotyczy funkcjonowania zespołu reagującego na zdarzenia zagrażające bezpiecznemu funkcjonowaniu sieci, drugie zaś obejmuje istotę autentyzacji i autoryzacji z wykorzystaniem zasady „jednokrotnego hasła".

INFORMATION SECURITY PROBLEMS IN COMPUTER NETWORKS

Abstract. In this article two main aspects of network Security are covered. First deals with security system which is to react on dangerous situations, and second explains the rules of autentization and authorization with the help of „one use command".

1. Wprowadzenie

Powszechne staje się przekonanie, że jedną z istotnych barier dalszego rozwoju i wykorzystania sieci jest problematyka bezpieczeństwa. Coraz większy problem stanowi zarządzanie sieciami i coraz wyraźniej widziana jest potrzeba standaryzacji zarządzania. Potrzeba sieci chronionych wzrasta zwłaszcza w obszarze biznesu, co warunkuje ich sens użytkowania (elektroniczny podpis, pieniądz, autentyzacja nadawcy i odbiorcy, wiarygodność i nienaruszalność danych, wreszcie poufność i prywatność).

Rozważając bezpieczeństwo sieci, ma się zwykle na uwadze następujące aspekty:

- sprawność techniczną i wydajność sieci;
- wierność przekazu;
- autentyzację odbiorcy i nadawcy;
- nienaruszalność struktury sieci, zwłaszcza zbiorów konfiguracyjnych i bazy danych związanych z użytkowaniem i wykorzystaniem sieci;
- dodatkowo, o ile przesyłane dane mają charakter klasyfikowany, potrzeba dodatkowej ochrony tych danych, zwykle poprzez metody kryptografii;
- nawet w wypadku danych nieklasyfikowanych istnienie problemu prywatności.

Szczególnie wyraźnie widać te aspekty w sieci Internet.

Sieć Internet posiada specyficzne właściwości, które w dość oczywisty sposób wpływają na problematykę bezpieczeństwa w tej sieci. Jest to sieć o globalnym zasięgu, której prapoczątki sięgające sieci ARPA i założenia przyjęte przez budowniczych Internetu wyznaczyły kierunki rozwoju, gdzie bezpieczeństwo pracy w sieci jest raczej problemem stałej troski niż zasadą wpisaną w Internet. Sieć Internet charakteryzuje się między innymi tym, że:

- nie ma właściciela,
- nie posiada centralnej kontroli,
- nie istnieje centralny autorytet mogący coś narzucić społeczności Internetu,
- brak jest standardowej, zaakceptowanej przez wszystkich polityki (np. bezpieczeństwa),
- brak jest międzynarodowego prawodawstwa w dziedzinie przestępstw komputerowych.

Problematyka streszczona powyżej jest coraz bardziej istotna w kontekście przyszłości Internetu, która rysuje się w postaci wzrostu zainteresowania tą siecią ze strony tzw. użytkowników nietradycyjnych (a więc spoza szeroko pojętego środowiska uczelnianego). Zainteresowanie tą siecią użytkowników komercyjnych, bankowości, administracji i innych wymusza profesjonalizację sieci i wzrost zainteresowania problematyką bezpieczeństwa traktowaną coraz częściej jako być albo nie być Internetu. Ma to szczególny wydźwięk także w kontekście zainteresowania Internetem rozmaitych grup anarchizacyjnych czy przestępczych.

2. Ataki na komputery w sieci

Na rozmaitych słabościach Internetu żerują tzw. włamywacze do sieciowych systemów komputerowych. Niektórzy robią to dla zabawy (rodzaj gry intelektualnej), inni prowadzą destrukcję w imieniu własnym lub na zlecenie (anarchiści, przestępcy, nihiliści) - istnieje też działalność wywiadowcza na tym polu. Typowy atak wpisuje się w następujący scenariusz:

- zlokalizowanie systemu do zaatakowania,
- zdobycie dostępu do konta legalnego użytkownika systemu

- brak haseł lub łamanie łatwych haseł
- podsłuchane hasła (sniffery),

- wykorzystanie dziur w konfiguracji i w oprogramowaniu systemowym w celu wejścia na konto uprzywilejowane,
- zatarcie śladów działalności (usunięcie zapisów z pamiętników - auditing records),
- przeprowadzenie nieuprawnionych działań,
- zainstalowanie „konia trojańskiego" dla aktualnego i przyszłego wykorzystania,
- ataki na inne komputery w sieci lokalnej.

Intruzi atakujący systemy komputerowe znajdujące się w sieci częstokroć posługują się kilkoma złamanymi wcześniej kontami na różnych maszynach logując się kolejno z jednego na drugie. Utrudnia to śledzenie miejsca, z którego tak naprawdę przeprowadzony był atak.

Ataki na systemy komputerowe dokonywane poprzez sieć mają wieloletnią historię. Przez lata zmienił się, ich profil i natężenie. Jednakże sposoby włamywania się stosowane przed laty są także wykorzystywane dziś - stale powiększa się arsenał środków, jakie są wykorzystywane przez intruzów w celu nieautoryzowanego dostępu do systemów.

3. Zespoły reagujące na zdarzenia

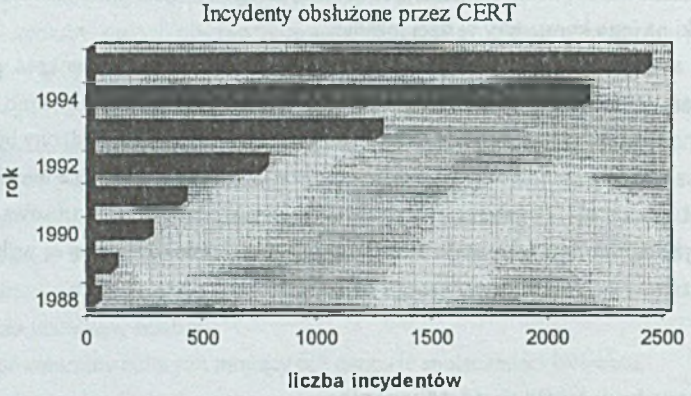
W tak potencjalnie niebezpiecznym środowisku, gdzie liczba incydentów naruszających bezpieczeństwo sieci stale rośnie (a potwierdzają to dane zbierane przez organizacje zajmujące się tym zagadnieniem), zaczęły powstawać zespoły, które w zorganizowany sposób reagują (głównie od strony technicznej) na sygnały o wystąpieniu zdarzenia. Pierwszym sformowanym centrum zatrudniającym ludzi dedykowanych do reagowania na pojawiające się w Internecie zagrożenia jest działający od roku 1988 CERT Coordination Center zlokalizowany w Carnegie Mellon University. Sformowanie CERT/CC nastąpiło bezpośrednio po osławionym incydencie 'internet worm' - który zablokował na kilkanaście godzin wiele komputerów dołączonych w 1988 roku do sieci.

Jako misję strategiczną CERT/CC przyjął:

- stworzenie wiarygodnego i niezawodnego dwudziestoczterogodzinnego punktu kontaktowego dla zgłaszania niebezpieczeństw w sieci,
- zapewnienie komunikacji pomiędzy ekspertami pracującymi nad rozwiązywaniem określonych problemów z dziedziny bezpieczeństwa,
- stworzenie centralnego miejsca identyfikowania i niwelowania problemów wynikających z niedopracowania systemów komputerowych,
- działanie w dziedzinie badań nad poprawieniem bezpieczeństwa w istniejących systemach,

- działanie w kierunku propagowania wiedzy w celu zwiększenia świadomości o problemach bezpieczeństwa wśród szerokiej rzeszy użytkowników Internetu.

W roku 1995 CERT/CC otrzymał 32 tysiące listów pocztą elektroniczną i prawie 3,5 tysiąca zgłoszeń za pomocą gorącej linii telefonicznej. Obsłużono 2412 incydentów (od początku działalności - ponad 7 000). Ponad 12 000 lokalizacji na całym świecie było dotkniętych incydentami.



Rys. 1. Diagram wzrostu incydentów obsłużonych przez CERT
Fig. 1. Incidences served by CERT

Z rocznego raportu CERT/CC wynika, że najgroźniejszymi klasami ataków w roku 1995 były:

- IP spoofing (w przeciągu kilku letnich tygodni miało miejsce ponad 170 ataków tego typu, które w większości przypadków skończyły się udanymi włamaniami),
- NFS (ataki poprzez słabości Network File System rozwinęły się w roku 1995 - pojawiły się wśród intruzów programy, które automatyzują ataki tego typu),
- Skanowanie sieci,
- Sniffery (podsłuchiwanie pakietów w celu wyłapywania haseł za pomocą instalowanych przez intruzów pakietów),
- Ataki poprzez sendmail.

Pod koniec roku nasiliły się ataki m.in. na sieci dostarczycieli usług, co zaowocowało wydaniem przez CERT generalnego ostrzeżenia o niebezpieczeństwie.

Jednym z ważniejszych przejawów działalności CERT/CC jest wydawanie tzw. „advisory", czyli tematycznych publikacji elektronicznych dotyczących pojawiających się zagrożeń. Zawierają one opis problemu, niebezpieczeństwa, potencjalne skutki dla różnych systemów operacyjnych oraz środki zaradcze.

W ciągu lat powstało na świecie wiele zespołów reagujących na zdarzenia naruszające bezpieczeństwo sieci. CERT/CC nadal jest centralnym miejscem i organizacją o światowym zasięgu, jednakże wiele krajów posiada własne centra, np. DFN-CERT w Niemczech, CERT-IT we Włoszech i wiele innych. Niektóre zespoły powstały przy „branżowych" centrach jak chociażby CIAC (Computer Incident Advisory Capability) działający z ramienia amerykańskiego Departamentu Energii.

Poszczególne IRTy (IRT: Incident Response Team) współpracują ze sobą w celu wymiany doświadczeń, ostrzeżeń itp., gdyż wiele z powstających zdarzeń naruszających bezpieczeństwo ma charakter rozległy czy wręcz międzynarodowy. Powstało także forum zrzeszające zespoły tego typu o nazwie: FIRST, czyli Forum of Incident Response and Security Teams.

4. Przygotowanie i reakcja

Zgodnie z zaleceniami bezpieczeństwa każda organizacja (sieć) powinna wypracować sobie model, który wyraża się w czynnościach takich jak:

- zidentyfikowanie dostępnych zasobów,
- stworzenie programu bezpieczeństwa,
- zaplanowanie systemu reagującego.

Intruzi są bowiem przygotowani i zorganizowani. Wykorzystują wszelkie dostępne media jak:

- modemy,
- pocztę elektroniczną
- BBS-y,
- serwery FTP,
- konferencje.

Nie każdą organizację stać jednak na utrzymywanie zespołu, który zawodowo będzie zajmował się obsługą zdarzeń naruszających bezpieczeństwo czy też w ogóle będzie na bieżąco z zagrożeniami. Jednakże jest celowe, aby powstawały zespoły w ramach tych organizacji, które mogą nieść pomoc innym w celu skoordynowania całości problemu bezpieczeństwa w danym kraju czy rejonie.

5. Cele sformowania zespołu reagującego na zdarzenia

Wśród głównych misji, jakie przyjmują powstające zespoły, można wymienić:

- wsparcie dla scentralizowanego, skoordynowanego i stałego reagowania,
- szybkie i efektywne reagowanie i pomoc dla „poszkodowanych",
- techniczne wsparcie dla potrzebujących oraz rozpropagowywanie wiedzy z dziedziny network security.

6. Formalne umocowanie zespołu

Jednym z istotnych obszarów, które decydują w ogóle o możliwości spełnienia funkcji IRT (Incident Response Team), jest strona formalna. Zespół bowiem musi mieć instytucjonalną organizację - nie może być zawieszony w próżni. Przedsięwzięcie wymaga także desygnowania określonego budżetu m.in. na:

- organizację struktury (personel, pomieszczenie, wyposażenie),
- utrzymanie ciągłe.

W Polsce problematyka bezpieczeństwa sieci komputerowych stała się również wrażliwym i docenianym problemem. Przykładem tego może być powołanie w 1996 roku, przez operatora Naukowej Akademickiej Sieci Komputerowej, zespołu CERT-NASK.

7. Specyfika bezpieczeństwa sieci komputerowych

Jednym z kluczowych aspektów zapewnienia bezpieczeństwa w sieciach rozległych jest właściwa autentyzacja i autoryzacja użytkowników.

Autentyzacja kładzie główny nacisk na identyfikację użytkownika. Autoryzacja to realizacja ustalonych przez administratora sieci zasad udostępniania zasobów użytkownika. Ochrona danych w sieciach rozległych ma swoją specyfikę. Skuteczne rozwiązanie problemu ochrony danych w sieciach rozległych wymaga zastosowania zarówno autentyzacji, jak i autoryzacji w sposób ściśle ze sobą powiązany.

W porównaniu do metod identyfikacji użytkownika w sieciach lokalnych skuteczne i efektywne metody w sieciach rozległych muszą być odporne na aktywne i pasywne metody ataku na liniach transmisyjnych (podsłuch i symulacja pracy użytkownika i /lub serwera). W świetle powyższego wiele tradycyjnych metod jest nie w pełni adekwatnych (np. identyfikacja za pomocą obrazu siatkówki, odcisku palca, wzorca podpisu).

Wszystkie wyżej wymienione metody są z natury statyczne (przechwycenie informacji w linii i symulacja pracy może prowadzić do skutecznego ataku). Metody powyższe są drogie i na dziś nie do zastosowania na skalę masową, choć mogą służyć jako środek dodatkowy pod warunkiem przykrycia kryptograficznego również o cechach zawierających dynamiczną zmianę klucza.

Metody identyfikacji w sieciach rozległych musi charakteryzować dynamika, to znaczy realizacja zasady „Jednokrotnego Hasła". Chodzi o to, że nie może być skuteczne złamanie ochrony w wyniku działań pasywnych, a następnie aktywnych na łączach telekomunikacyjnych. Zapewnienie każdemu użytkownikowi unikalnych haseł wykorzystywanych jednokrotnie jest administracyjnie, organizacyjnie i technicznie nie do przyjęcia. Dynamika systemów identyfikacji i autentyzacji zapewniona może być w dwojaki sposób: z generatora bazowego w systemie autentyzacji (Challange-responze) lub w oparciu o naturalny element zmiennej, jakim jest czas (rys. 2).

8. Kierunki rozwiązań

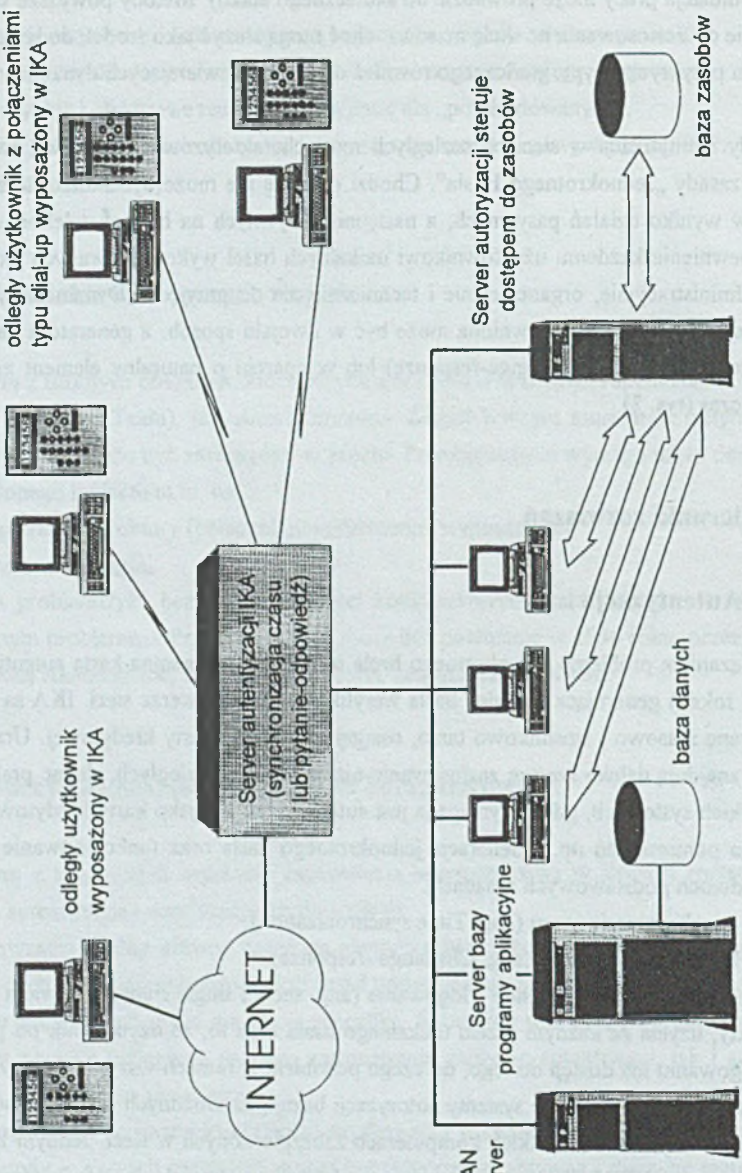
8.1. Autentyzacja

Rozwiązaniem problemu jednokrotnego hasła może być inteligentna karta autentyzacyjna IKA (ang. token) generująca unikalne hasła weryfikowane na serwerze sieci. IKA są obecnie produkowane masowo i stosunkowo tanio, osiągając wielkość karty kredytowej. Urządzenia typu IKA znajdują daleko szersze zastosowanie niż w sieciach rozległych, służąc praktycznie we wszystkich systemach, gdzie wymagana jest autentyzacja (np. jako karty kredytowe, klucz dostępu do pomieszczeń itp.). Generacja jednokrotnego hasła oraz funkcjonowanie IKA są oparte na dwóch podstawowych zasadach:

1. Synchronizacja czasu (ang. Time synchronization),
2. Pytanie - odpowiedź (ang. Challange -responze).

Bezpieczny jednokrotny dostęp - logowanie (ang. secure single sign-on) zawiera w sobie dwa aspekty; użycia za każdym razem unikalnego hasła oraz to, że użytkownik po pojedynczym zalogowaniu ma dostęp do tego, do czego powinien, w ramach wszystkich przyznanych zasobów w całej sieci. Ogólnie systemy autoryzacji bazują na złożonych pakietach softwarowych, instalowanych na wszystkich komputerach zabezpieczonych w sieci. Jednym z najbardziej znanych jest KERBEROS sprzedawany w różnych wariantach. Podstawowym problemem jest dostosowanie procedur logowania do poszczególnych platform softwarowych.

To oznacza, że poszczególne węzły sieci muszą się wzajemnie autentyzować bezpiecznymi metodami w sposób dynamiczny.



Rys. 2. Ogólny schemat autentyzacji i autoryzacji
Fig. 2. The general idea of authentication and authentization

IKA generują hasło przekazywane do systemu weryfikacji punktów dostępu do sieci. Serwer autentyzacji weryfikuje hasło umożliwiając logowanie użytkownika. Serwerem autentyzacji może być wydzielone urządzenie - router, dedykowany komputer pod systemem UNIX lub innej platformy pakiet softwarowy na serwerze, bądź inaczej, zwykle w zależności od tego, ilu użytkowników ma obejmować system. Szczegóły realizacji mechanizmów autentyzacji zależą od producenta. Najbardziej popularna technika to opracowana przez Security Dynamic synchronizacja czasowa. Przykładami są: KERBEROS, IBM-owski NetSP, ICL Lan Manager.

Synchronizacja czasowa polega na algorytmie i kluczu 64-bitowym do generowania liczby losowej co minutę, przy czym czas może być zmieniany przez administratora sieci. Każdy użytkownik ma przydzielony unikalny Klucz pamiętany w IKA, jak i w bazie danych serwera autentyzacji. W czasie próby logowania użytkownik podaje 4-cyfrowy osobisty numer identyfikacyjny (ang. PIN), a następnie 6-cyfrową liczbę wygenerowaną przez IKA. PIN określa serwerowi, jakiego tajnego klucza użyć. Serwer znajduje odpowiedni klucz, wykonuje algorytm i sprawdza, czy otrzymana (wygenerowana) liczba jest taka sama, jak podana przez użytkownika (rys. 3). W wypadku zgodności następuje logowanie.

Pytanie - odpowiedź jest innym schematem bazującym na algorytmach szyfracji. Gdy użytkownik próbuje się logować, serwer autentyzacji wysyła liczbę losową. IKA szyfruje tę liczbę przy użyciu tajnego klucza użytkownika i wysyła z powrotem do serwera autentyzacji. Identyczny algorytm jest wykonywany na serwerze, a rezultaty porównywane (rys. 4).

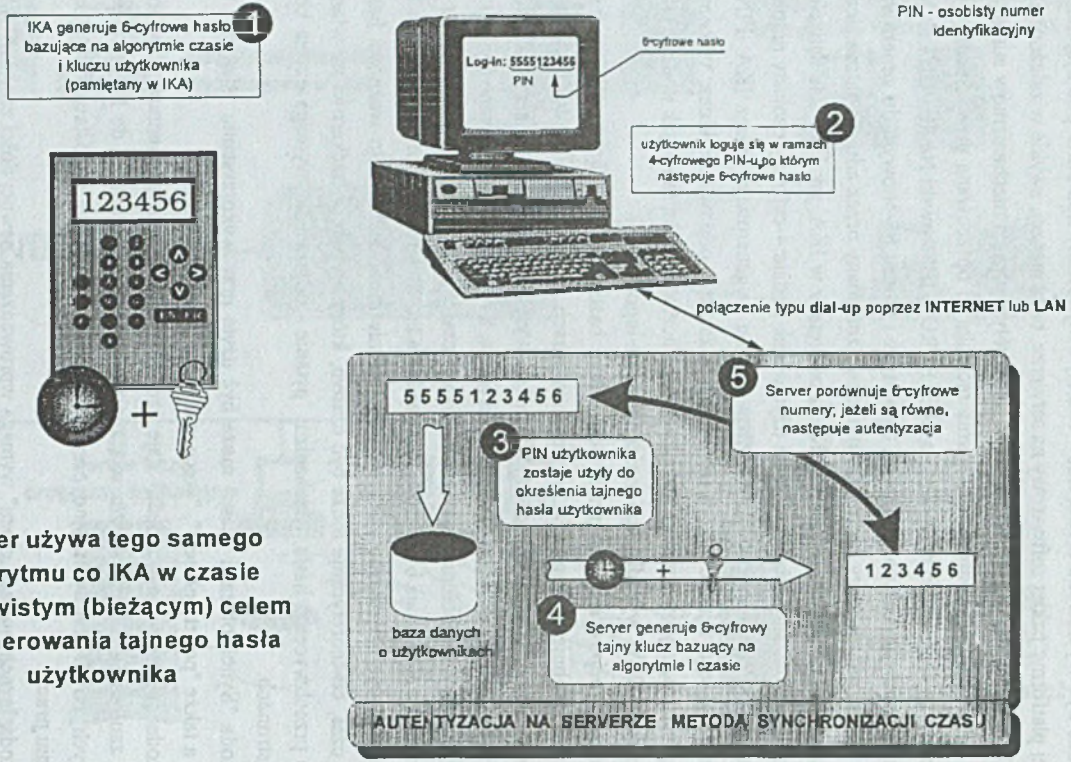
Podstawowym problemem w synchronizacji czasowej jest synchronizacja czasu na IKA, zwłaszcza o ile IKA mają być używane przez kilka lat. Stosowana może być metoda kompensacji powstających rozbieżności czasu. Zastrzeżenie może budzić fakt ważności hasła przez pewien czas, co teoretycznie może być czasem, który wystarczy hackerowi na włamanie do sieci po przechwyceniu hasła. Mechanizm "pytanie - odpowiedź" wymaga użycia komputera po obu stronach.

Metoda "Synchronizacji czasu" może być użyta przy wykorzystaniu "ślepych" terminali Faxów, a także "poczty głosem", "voice mail" - spr. konta w banku.

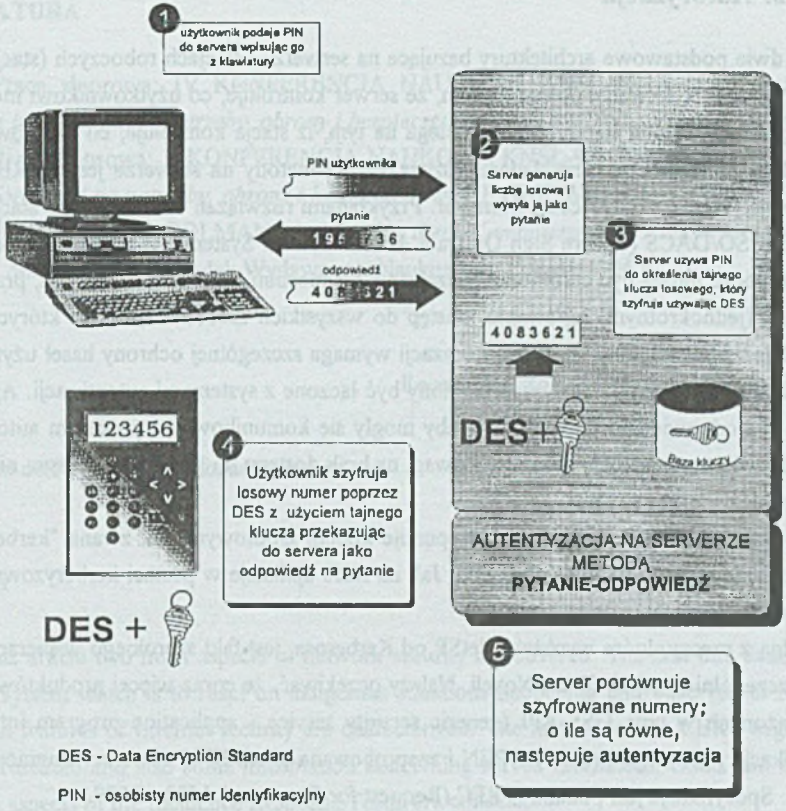
Metoda "pytanie - odpowiedź" daje szersze możliwości implementacji. Np. może być w pełni zautomatyzowana poprzez włączenie odpowiednich urządzeń do PC w miejsce stacji dyskowych, co też jest dyskusyjne, ponieważ użytkownicy mogą je zostawiać w stacji po zakończeniu pracy.

Metoda "synchronizacji czasu" wymaga wprowadzenia pewnej ilości znaków, zaś metoda "pytanie - odpowiedź" jest jednak bardziej uciążliwa, ponieważ użytkownik musi podać do IKA, np. w przypadku łączy "dial up", liczbę losową, a potem rezultat szyfracji, a niekiedy musi się ponownie logować do serwera.

Nawet w przypadku softwarowych IKA, programów wykonywanych na PC-cie lub laptopie, jest wiele opinii, że proces logowania jest zbyt wolny i zbyt uciążliwy.



Rys. 3. Autentyzacja metodą synchronizacji czasu
Fig. 3. Time synchronization based authentization method



Rys. 4. Autentyzacja metodą pytanie odpowiedź
Fig. 4. Challenge response based authentization method

Problem stanowi także połączenie serwerów komunikacyjnych z serwerem autentyzacji. Metoda "pytanie - odpowiedź" umożliwia zwykle samodzielne konfigurowanie IKA. Jest to oczywiście dodatkowa praca, ale wtedy tylko administrator, poza użytkownikiem, ma dostęp do klucza. Metody inicjalizacji IKA są różne w zależności od dostawcy, niekiedy np. Security-Dynamic inicjacja jest fabryczna. Problemem jest także wymiana baterii w IKA. Synchronizacja bazy i IKA w przypadku dużej sieci stanowi problem - bywa kosztowna. Z drugiej strony stosowanie tego typu mechanizmów w małych sieciach jest niecelowe. Zwykle przyjmuje się jako granicę sieć powyżej 500 stanowisk (użytkowników).

8.2. Autoryzacja

Są dwie podstawowe architektury bazujące na serwerze i stacjach roboczych (stacji roboczej). Metoda na serwerze polega na tym, że serwer kontroluje, co użytkownikowi może być udostępnione. Metoda stacji roboczej polega na tym, iż stacja kontroluje, co użytkownikowi może być udostępnione. Przykładami rozwiązań dla metody na serwerze jest KERBEROS, IBM-owski NetSP i ICL Access Manager. Przykładami rozwiązań dla metody na stacji roboczej jest SSO/DACS (Secure Sign On/Data Access Control System). W tym przypadku same stacje robocze muszą być chronione. Niezależnie od sposobu rozwiązań celem jest, przy pojedynczym (jednokrotnym) logowaniu, dostęp do wszystkich zasobów sieci, do których użytkownik jest upoważniony. System autoryzacji wymaga szczególnej ochrony haseł użytkownika. Dlatego też systemy autoryzacji powinny być łączone z systemami autentyzacji. Aplikacje muszą być odpowiednio dostosowane, aby mogły się komunikować z procesem autoryzacji. W większości stosowanych aplikacji, z uwagi na brak dostępu do kodu źródłowego, nie da się tego zrobić.

Dla kerberosa, o ile użytkownik dysponuje kodem źródłowym, tak zwana "kerberyzacja aplikacji" nie stanowi na ogół problemu. Jak na razie aplikacje w postaci kerberyzowanej nie są jeszcze powszechnie dostępne.

Jedną z rzeczy, która wyróżnia NetSP od Kerberosa, jest fakt szerokiego wspierania aplikacji szczególnie pod NetWare Novell. Należy oczekiwać, że coraz więcej produktów będzie wyposażonych w tzw. GSS-API (generic security service - application program interface), specyfikację rozwiniętą przez X-OPEN i zaaprobowaną przez IETF (Internet Engineeri Task Force). Specyfikacja jest podana w RFC (Request for Comment) 1503 - 1509.

Należy podkreślić, że wszelkie rozwiązania techniczne są tylko fragmentem odpowiednio prowadzonej polityki ochrony, która musi obejmować: aspekty prawne, softwarowo-hardwarowe, administracyjne, zasady eksploatacji, regulaminy pracy, szkolenia itp. tak, jak to np. zakłada program bezpieczeństwa sieci NASK.

Stosowane metody ochrony w sieciach powinny podlegać procesowi weryfikacji i formalnej autentyzacji w odniesieniu do takich zagadnień jak: moc kryptograficzna algorytmów i kluczy oraz systemów operacyjnych komputerów. Zagadnienia te są stosunkowo proste i znajdują konkretne rozwiązania (np. DES i norma C2).

W praktyce najtrudniejsze wydaje się zastosowanie analogicznego postępowania w odniesieniu do procesu wdrożenia i eksploatacji oraz postępowania w przypadkach szczególnych. Dla skutecznej ochrony danych w sieciach rozległych nie wystarcza sam fakt weryfikacji produktów.

LITERATURA

1. Praca zbiorowa: IV KONFERENCJA NAUKOWA KNSŁ-95, *Systemy łączności i informatyki na potrzeby obrony i bezpieczeństwa RP*. WSOWŁ, Zegrze 1995 r.
2. Praca zbiorowa: V KONFERENCJA NAUKOWA KNSŁ-96, *Systemy łączności i informatyki na potrzeby obrony i bezpieczeństwa RP*. WSOWŁ, Zegrze 1996 r.
3. Praca zbiorowa: POLMAN'96, *Miejskie Sieci Komputerowe w Nauce, Gospodarce i Administracji*. Ośrodek Wydawnictw Naukowych, Poznań 1996 r.

Recenzent: Prof. dr hab. inż. Andrzej Grynak

Wpłynęło do Redakcji 21 listopada 1996 r.

Abstract

In this article two main aspects of network security are covered. The first one deals with security system which is to react on dangerous situations happening and observed in reality. The main features of Internet security are characterized. The mission of the CERT organization is presented and also some information concerning served incidences. Goals and organizational aspects of the Incidence Response Team are considered.

The second part of the article explains the rules of authentication and authorization with the help of „one use command" There are two main methods: time synchronization and challenge response. Presented ideas of authentication and authorization is a part of NASK Security Program.